

FUJITSU Software

openUTM V7.0

Programming Applications with KDCS for COBOL, C and C++

User Guide

November 2019

Comments... Suggestions... Corrections...

The User Documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to: bs2000services@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2015

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2015.

Copyright and Trademarks

Copyright © 2019 Fujitsu Technology Solutions GmbH.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Table of Contents

- Programming Applications with KDCS for COBOL, C and C++** 10
- 1 Preface** 11
 - 1.1 Summary of contents and target group** 13
 - 1.2 Summary of contents of the openUTM documentation** 14
 - 1.2.1 openUTM documentation 15
 - 1.2.2 Documentation for the openSEAS product environment 18
 - 1.2.3 Readme files 19
 - 1.3 Changes in openUTM V7.0** 20
 - 1.3.1 New server functions 21
 - 1.3.2 Discontinued server functions 25
 - 1.3.3 New client functions 26
 - 1.3.4 New functions for openUTM WinAdmin 27
 - 1.3.5 New functions for openUTM WebAdmin 28
 - 1.4 Notational conventions** 29
- 2 Structure and use of UTM programs** 31
 - 2.1 The openUTM service concept** 34
 - 2.2 Structure of a program unit** 37
 - 2.2.1 Program framework 38
 - 2.2.2 Structure of a dialog program unit 40
 - 2.2.3 Reentrant capability of program units 42
 - 2.3 Structuring services** 43
 - 2.3.1 Multi-step services 44
 - 2.3.2 Multiple program units in one processing step 47
 - 2.3.3 Multiple processing steps in a single program unit 49
 - 2.3.4 Subprogram calls from program units 50
 - 2.3.5 Chaining services 51
 - 2.3.6 Stacking services 52
 - 2.4 Message Queuing (asynchronous processing)** 53
 - 2.4.1 Dead Letter Queue 54
 - 2.4.2 Messages to UTM-controlled queues 55
 - 2.4.2.1 Output jobs 56
 - 2.4.2.2 Background jobs 57
 - 2.4.2.3 MQ calls of the KDCS interface 58
 - 2.4.2.4 Structure of an asynchronous service 59
 - 2.4.2.5 Redelivery with background jobs 66
 - 2.4.3 Messages to service-controlled queues 67
 - 2.4.3.1 USER queues 68

2.4.3.2 TAC queues	69
2.4.3.3 Temporary queues	70
2.4.3.4 MQ calls of the KDCS interface	71
2.4.3.5 Lifetime of queues and queue messages	72
2.4.3.6 Deleting USER and TAC queues by means of programmed administration	73
2.4.3.7 Examples	74
2.5 KDCS storage areas in openUTM	81
2.5.1 Standard primary working area (SPAB)	85
2.5.2 Communication area (KB)	87
2.5.3 Local secondary storage area (LSSB)	89
2.5.4 Global secondary storage area (GSSB)	90
2.5.5 Terminal-specific long-term storage area (TLS)	91
2.5.6 User-specific long-term storage area (ULS)	92
2.5.7 User log file	93
2.5.8 Other areas	94
2.5.9 Action with locked storage areas (TLS, ULS and GSSB)	95
2.6 Programming error routines	96
2.7 Message segments	97
2.8 Communication partners of a UTM application	99
2.9 Output to printers	100
2.9.1 Hardcopy mode with openUTM on BS2000 systems	101
2.9.2 Print jobs	102
2.10 Support for ID card readers on BS2000 systems	104
2.10.1 Signing on to the application via ID card reader (BS2000 systems)	105
2.10.2 Data input via ID card (BS2000 systems)	106
3 Interaction with databases	107
3.1 UTM transaction and DB transaction	109
3.2 Programming ESQL program units	111
3.3 Error processing with connected databases	112
4 Screen functions	113
4.1 Use of formats in openUTM on BS2000 systems	114
4.1.1 Screen output functions in format mode (BS2000 systems)	116
4.1.2 Starting services using basic formats (BS2000 systems)	117
4.1.3 Using partial formats (BS2000 systems)	118
4.1.3.1 Output formatting with partial formats (BS2000 systems)	119
4.1.3.2 Input formatting with partial formats (BS2000 systems)	120
4.1.4 Message flow for formatted messages (BS2000 systems)	121
4.1.5 Outputs on printers in format mode (BS2000 systems)	122
4.2 Controlling the output in line mode (BS2000 systems)	123
4.3 Output on printers in line mode	125

4.4 Screen restart	126
4.5 Format names for message exchange with UPIC clients	127
5 Program structure in distributed processing	128
5.1 Addressing remote services	129
5.2 Distributed dialogs	131
5.2.1 Controlling communication in the program	132
5.2.2 Error handling by the program unit	133
5.2.2.1 Programmed rollback	134
5.2.2.2 Error handling after service restart	137
5.2.3 Load distribution using LPAP bundles	139
5.3 Distributed dialogs via LU6.1	140
5.3.1 Programming aids	141
5.3.2 Programming rules and recommendations	143
5.3.3 Existing program units as LU6.1 job receivers	151
5.3.4 Example: distributed dialog via LU6.1	152
5.4 Distributed dialogs via OSI TP	156
5.4.1 Functional units	157
5.4.2 Programming aids	159
5.4.3 Programming rules for dialogs without the functional unit commit	164
5.4.4 Programming rules with the functional unit commit	165
5.4.5 Programming rules for communications with BeanConnect	168
5.4.6 Particularities of rollback and restart	169
5.4.7 Using existing program units for OSI TP communication	171
5.4.8 Particularities with heterogeneous coupling	173
5.4.9 Examples: distributed dialogs via OSI TP	174
5.4.9.1 One job receiver	175
5.4.9.2 Multiple job receivers	185
5.4.9.3 More complex dialog trees	187
5.4.9.4 Using CTRL AB to terminate a job receiver	193
5.5 UTM-controlled queues in distributed processing	194
5.5.1 Job submitter side	195
5.5.2 Job receiver side	196
5.6 Service-controlled queues in distributed processing	197
6 Program structure in communication with transport system applications	198
6.1 Communication with TS applications of the type APPLI	199
6.2 Communication with socket USP applications	200
6.2.1 Input messages for openUTM	201
6.2.2 Output messages of openUTM	202
6.2.3 Structure of the USP header	203
7 KDCS calls	205
7.1 Complete overview of KDCS calls	206

7.2 Comments on the description of the KDCS calls	209
7.3 APRO Address job-receiving service	210
7.4 CTRL Control OSI TP Dialog	219
7.5 DADM Administer message queues	224
7.6 DGET Read a message from a service-controlled queue	235
7.7 DPUT Generate time-driven asynchronous messages	245
7.7.1 DPUT call without job complex	246
7.7.2 DPUT call in a job complex	258
7.8 FGET Receive asynchronous message	265
7.9 FPUT Generating asynchronous messages	270
7.10 GTDA Read from TLS	279
7.11 INFO Request information	282
7.11.1 INFO CK call	293
7.12 INIT Initialize program unit	296
7.13 LPUT Write to log file	320
7.14 MCOM Define job complex	323
7.15 MGET Receive dialog message	327
7.16 MPUT Send dialog message	341
7.17 PADM Administer printouts and printers	352
7.18 PEND Terminate program unit	360
7.19 PGWT Set wait point in program without terminating program unit	372
7.20 PTDA Write to TLS	382
7.21 QCRE Create temporary queue	385
7.22 QREL Delete temporary queue	389
7.23 RSET Roll back transaction	392
7.24 SGET Read from secondary storage area	395
7.25 SIGN Control sign-on and sign-off, check authorization data, change passwords	400
7.25.1 SIGN CL - Change locale of user ID (BS2000 systems)	413
7.26 SPUT Write to secondary storage area	416
7.27 SREL Delete secondary storage area	422
7.28 UNLK Unlock TLS, ULS or GSSB	426
8 Program interface UTM-HTTP	430
8.1 Overview of all UTM-HTTP functions	431
8.1.1 Function kcHttpGetHeaderByIndex	433
8.1.2 Function kcHttpGetHeaderByName	435
8.1.3 Function kcHttpGetHeaderCount	437
8.1.4 Function kcHttpGetMethod	438
8.1.5 Function kcHttpGetMputMsg	439
8.1.6 Function kcHttpGetPath	440

8.1.7 Function kcHttpGetQuery	441
8.1.8 Function kcHttpGetRc2String	442
8.1.9 Function kcHttpGetReqMsgBody	443
8.1.10 Function kcHttpGetScheme	444
8.1.11 Function kcHttpGetVersion	445
8.1.12 Function kcHttpPercentDecode	446
8.1.13 Function kcHttpPutHeader	448
8.1.14 Function kcHttpPutMgetMsg	450
8.1.15 Function kcHttpPutRspMsgBody	451
8.1.16 Function kcHttpPutStatus	452
8.2 Addressing TAC	454
8.3 Evaluation of the HTTP Header of an HTTP request	455
8.4 Setting the HTTP Header of an HTTP Response	457
8.5 Specifics of communicating with HTTP clients	460
8.6 Behaviour in error situations	461
9 Event functions	462
9.1 Event exits	464
9.1.1 Event exit INPUT	465
9.1.2 Event exit HTTP	473
9.1.3 Event exit START	477
9.1.4 Event exit SHUT	479
9.1.5 Event exit VORGANG	480
9.1.6 Event exit FORMAT (BS2000 systems)	482
9.2 User-specific error handling (Unix and Linux systems)	490
9.3 STXIT routines (BS2000 systems)	492
9.4 Event handling in ILCS programs (BS2000 systems)	493
9.5 Event services	495
9.5.1 Dialog service BADTACS	496
9.5.2 Asynchronous service MSGTAC	497
9.5.3 The SIGNON service	499
9.5.3.1 Programming notes	500
9.5.3.2 Sign-on service for terminals	501
9.5.3.3 Sign-on service for UPIC clients or transport system applications	504
10 Additional information for C/C++	507
10.1 Program structure for C/C++ program units	508
10.1.1 C/C++ program units as subroutines	509
10.1.2 Parameters of a C/C++ program unit	510
10.1.3 Declaring data	511
10.1.3.1 Communication area	512
10.1.3.2 Standard primary working area	513
10.1.3.3 Other data areas (AREAs)	514

10.1.4	Data structures for C/C++ program units	518
10.1.5	Command section of a C/C++ program unit	520
10.1.6	C/C++ macro interface	521
10.1.7	Event exits	526
10.1.8	Programming the KDCS error handling routines	527
10.1.9	Programming user-specific error handling (Unix and Linux systems)	528
10.1.9.1	User signal routines (Unix and Linux systems)	529
10.1.9.2	Exchanging the utmwork process (Unix and Linux systems)	531
10.1.9.3	Creating a UTM dump (Unix and Linux systems)	532
10.1.10	Modifying KDCS attributes (BS2000 systems)	533
10.1.11	Platform-specific characteristics on BS2000 systems	534
10.1.12	Platform-specific characteristics on Unix and Linux systems	536
10.1.13	Platform-specific characteristics on Windows systems	537
10.2	Programming examples in C/C++	538
10.2.1	Examples of individual KDCS calls	539
10.2.2	Example of a complete C program unit	543
10.2.3	Example: INPUT exit (BS2000 systems)	544
10.2.4	Example: MSGTAC event service	547
10.2.5	Example of a complete UTM application on BS2000 systems	551
11	Additional information for COBOL	567
11.1	Structure of COBOL program units	568
11.1.1	COBOL program units as subroutines	569
11.1.2	Data structures for COBOL program units	573
11.1.3	KDCS calls in COBOL program units	576
11.1.4	Programming user-specific error handling (Unix and Linux systems)	578
11.1.4.1	User signal routines (Unix and Linux systems)	579
11.1.4.2	Exchanging the utmwork process (Unix and Linux systems)	581
11.1.4.3	Creating a UTM dump (Unix and Linux systems)	582
11.1.5	Platform-specific features on BS2000 systems	583
11.1.6	Platform-specific features on Unix and Linux systems	586
11.1.7	Platform-specific features on Windows systems	589
11.2	Programming examples in COBOL	591
11.2.1	Examples of individual KDCS calls	592
11.2.2	Example of an INPUT exit (BS2000 systems)	599
11.2.3	Example of an asynchronous MSGTAC program unit	601
11.2.4	Example of a complete UTM application on BS2000 systems	605
12	Appendix	617
12.1	Overview of all KDCS calls	618
12.2	Different field names for C/C++ and COBOL	627
12.3	ASCII-EBCDIC code conversion	632
12.3.1	BS2000 systems	633

12.3.2 Unix, Linux and Windows systems	634
12.3.2.1 Modifying the code conversion tables on Unix and Linux systems	635
12.3.2.2 Modifying the code conversion tables on Windows systems	636
13 Glossary	637
14 Abbreviations	670
15 Related publications	675

Programming Applications with KDCS for COBOL, C and C++

1 Preface

The IT infrastructure of today's companies as the heart and engine of the business must meet the requirements of the digital age. At the same time, it has to cope with increased amounts of data as well as with stricter requirements from the environment, e.g. compliance requirements. It must also be possible to integrate additional applications at short notice. And all this under the aspect of guaranteed security.

Thus, essential requirements for a modern IT infrastructure consist of, among others

- Flexibility and almost limitless scalability also for future requirements
- high robustness with highest availability
- absolute safety in all respects
- Adaptability to individual needs
- Causing low costs

To meet these challenges, Fujitsu offers an extensive portfolio of innovative enterprise hardware, software, and support services within the environment of our enterprise mainframe platforms, and is therefore your

- Reliable service provider, giving you longterm, flexible, and innovative support in running your company's mainframe-based core applications
- Ideal partner for working together to meet the requirements of digital transformation
- Longterm partner, by reason of continuous adjustment of modern interfaces required by a modern IT landscape with all its requirements.

With openUTM, Fujitsu provides you a thoroughly tried-and-tested solution from the middleware area.

openUTM is a high-end platform for transaction processing that offers a runtime environment that meets all these requirements of modern, business-critical applications, because openUTM combines all the standards and advantages of transaction monitor middleware platforms and message queuing systems:

- consistency of data and processing
- high availability of the applications
- high throughput even when there are large numbers of users (i.e. highly scalable)
- flexibility as regards changes to and adaptation of the IT system

A UTM application on Unix, Linux and Windows systems can be run as a standalone UTM application or sumultaneously on several different computers as a UTM cluster application.

openUTM forms part of the comprehensive **openSEAS** offering. In conjunction with the Oracle Fusion middleware, openSEAS delivers all the functions required for application innovation and modern application development. Innovative products use the sophisticated technology of openUTM in the context of the **openSEAS** product offering:

- BeanConnect is an adapter that conforms to the Java EE Connector Architecture (JCA) and supports standardized connection of UTM applications to Java EE application servers. This makes it possible to integrate tried-and-tested legacy applications in new business processes.
- Existing UTM applications can be migrated to the Web without modification. The UTM-HTTP interface and the WebTransactions product, are two openSEAS alternatives that allows proven host applications to be used flexibly in new business processes and modern application scenarios.



The products BeanConnect and WebTransactions are briefly presented in the performance overview. There are separate manuals for these products.

i Wherever the term Linux system or Linux platform is used in the following, then this should be understood to mean a Linux distribution such as SUSE or Red Hat.

Wherever the term Windows system or Windows platform is in the following, this should be understood to mean all the variants of Windows under which openUTM runs.

Wherever the term Unix system or Unix platform is used in the following, then this should be understood to mean a Unix-based operating system such as Solaris or HP-UX.

1.1 Summary of contents and target group

The openUTM manual „Programming Applications with KDCS“ is intended for anyone who wants to use the KDCS programming interface or the UTM-HTTP programming interface to program UTM applications.

The vast majority of the information presented in this manual is operating system-independent, i.e. it applies to both Unix, Linux and Windows systems, as well as to BS2000 systems. In addition, descriptions of platform-specific features are also provided. Any such platform-specific information is clearly indicated by means of markings in the margins. As a result you can, if you so desire, write applications that can run on Unix and Linux systems, Windows systems and BS2000 systems. The form of presentation used throughout this manual will also simplify matters if you are wanting to port existing UTM(BS2000) applications to Unix systems, Linux systems or Windows systems, or vice versa.

The chapters in this manual can be subdivided into three blocks:

- Chapter "[Structure and use of UTM programs](#)" to "[Program structure in communication with transport system applications](#)" contain introductory information. They explain basic concepts, such as the way program units are structured into processing step modules, message queuing functionality and distributed processing in their respective contexts.
- Chapters "[KDCS calls](#)" to "[Event functions](#)" provide reference materials in which you can look things up. Chapter "[KDCS calls](#)" lists the KDCS calls in alphabetical order, chapter "[UTM-HTTP calls](#)" lists the functions of UTM-HTTP programming interface and chapter [8 \(Event functions\)](#) lists the event functions.
- Chapters "[Additional information for C/C++](#)" and "[Additional information for COBOL](#)" contain programming language-specific information - chapter "[Additional information for C/C++](#)" for C/C++, and chapter "[Additional information for COBOL](#)" for COBOL.

The appendix includes a series of tables which provide overviews of the entries that must be made in the parameter area for the individual KDCS calls, for example, or of the values returned to the communication area.

The detailed reference section at the back of the manual – including a glossary, abbreviations, a list of related publications and a keyword index – is intended to help you get the most out of this manual.

i Wherever the term Unix system is used in the following, then this should be understood to mean a Unix-based operating system such as Solaris or HP-UX.

Wherever the term Linux system is used in the following, then this should be understood to mean a Linux distribution such as SUSE or Red Hat.

Wherever the term Windows system or Windows platform is used below, this should be understood to mean all the variants of Windows under which openUTM runs.

1.2 Summary of contents of the openUTM documentation

This section provides an overview of the manuals in the openUTM suite and of the various related products.

1.2.1 openUTM documentation

The openUTM documentation consists of manuals, the online help for the graphical administration workstation openUTM WinAdmin and the graphical administration tool WebAdmin as well as release notes.

There are manuals and release notes that are valid for all platforms, as well as manuals and release notes that are valid for BS2000 systems and for Unix, Linux and Windows systems.

All the manuals are available on the internet at <https://bs2manuals.ts.fujitsu.com>. For the BS2000 platform, you will also find the manuals on the Softbook DVD.

The following sections provide a task-oriented overview of the openUTM V7.0 documentation.

You will find a complete list of documentation for openUTM in the chapter on related publications at the back of the manual.

Introduction and overview

The **Concepts and Functions** manual gives a coherent overview of the essential functions, features and areas of application of openUTM. It contains all the information required to plan a UTM operation and to design a UTM application. The manual explains what openUTM is, how it is used, and how it is integrated in the BS2000, Unix, Linux and Windows based platforms.

Programming

- You will require the **Programming Applications with KDCS for COBOL, C and C++** manual to create server applications via the KDCS interface or UTM-HTTP programming interface. This manual describes the KDCS interface as used for COBOL, C and C++. This interface provides the basic functions of the universal transaction monitor, as well as the calls for distributed processing. The manual also describes interaction with databases. The UTM-HTTP programming interface provides functions that may be used for communication with HTTP clients.
- You will require the **Creating Applications with X/Open Interfaces** manual if you want to use the X/Open interface. This manual contains descriptions of the openUTM-specific extensions to the X/Open program interfaces TX, CPI-C and XATMI as well as notes on configuring and operating UTM applications which use X/Open interfaces. In addition, you will require the X/Open-CAE specification for the corresponding X/Open interface.
- If you want to interchange data on the basis of XML, you will need the document entitled openUTM **XML for openUTM**. This describes the C and COBOL calls required to work with XML documents.
- For BS2000 systems there is supplementary documentation on the programming languages Assembler, Fortran, Pascal-XT and PL/1.

Configuration

The **Generating Applications** manual is available to you for defining configurations. This describes for both standalone UTM applications and UTM cluster applications on Unix, Linux and Windows systems how to use the UTM tool KDCDEF to

- define the configuration
- generate the KDCFILE
- and generate the UTM cluster files for UTM cluster applications

In addition, it also shows you how to transfer important administration and user data to a new KDCFILE using the KDCUPD tool. You do this, for example, when moving to a new openUTM version or after changes have been made to the configuration. In the case of UTM cluster applications, it also indicates how you can use the KDCUPD tool to transfer this data to the new UTM cluster files.

Linking, starting and using UTM applications

In order to be able to use UTM applications, you will need the **Using UTM Applications** manual for the relevant operating system (BS2000 or Unix, Linux and Windows systems). This describes how to link and start a UTM application program, how to sign on and off to and from a UTM application and how to replace application programs dynamically and in a structured manner. It also contains the UTM commands that are available to the terminal user. Additionally, those issues are described in detail that need to be considered when operating UTM cluster applications.

Administering applications and changing configurations dynamically

- The **Administering Applications** manual describes the program interface for administration and the UTM administration commands. It provides information on how to create your own administration programs for operating a standalone UTM application or a UTM cluster application and on the facilities for administering several different applications centrally. It also describes how to administer message queues and printers using the KDCS calls DADM and PADM.
- If you are using the graphical administration workstation **openUTM WinAdmin** or the Web application **openUTM WebAdmin**, which provides comparable functionality, then the following documentation is available to you:
 - A **description of WinAdmin** and **description of WebAdmin**, which provide a comprehensive overview of the functional scope and handling of WinAdmin/WebAdmin.
 - The respective **online help systems**, which provide context-sensitive help information on all dialog boxes and associated parameters offered by the graphical user interface. In addition, it also tells you how to configure WinAdmin or WebAdmin in order to administer standalone UTM applications and UTM cluster applications.

i For detailed information on the integration of openUTM WebAdmin in SE Server's SE Manager, see the SE Server manual **Operation and Administration**.

Testing and diagnosing errors

You will also require the **Messages, Debugging and Diagnostics** manuals (there are separate manuals for Unix, Linux and Windows systems and for BS2000 systems) to carry out the tasks mentioned above. These manuals describe how to debug a UTM application, the contents and evaluation of a UTM dump, the openUTM message system, and also lists all messages and return codes output by openUTM.

Creating openUTM clients

The following manuals are available to you if you want to create client applications for communication with UTM applications:

- The **openUTM-Client for the UPIC Carrier System** describes the creation and operation of client applications based on UPIC. It indicates what needs to be taken into account when programming a CPI-C application and what restrictions apply compared with the X/Open CPI-C interface.

-
- The **openUTM-Client for the OpenCPIC Carrier System** manual describes how to install and configure OpenCPIC and configure an OpenCPIC application. It indicates what needs to be taken into account when programming a CPI-C application and what restrictions apply compared with the X/Open CPI-C interface.
 - The documentation for the product **openUTM-JConnect** shipped with **BeanConnect** consists of the manual and a Java documentation with a description of the Java classes.
 - The **BizXML2Cobol** manual describes how you can extend existing COBOL programs of a UTM application in such a way that they can be used as an XML-based standard Web service. How to work with the graphical user interface is described in the **online help system**.
 - You can also use the software product WS4UTM (WebServices for openUTM) to provide services of UTM applications as Web services. To do this, you need the **Web Services for openUTM** manual. Working with the graphical user interface is described in the corresponding **online help system**.

Communicating with the IBM world

If you want to communicate with IBM transaction systems, then you will also require the manual **Distributed Transaction Processing between openUTM and CICS, IMS and LU6.2 Applications**. This describes the CICS commands, IMS macros and UTM calls that are required to link UTM applications to CICS and IMS applications. The link capabilities are described using detailed configuration and generation examples. The manual also describes communication via openUTM-LU62 as well as its installation, generation and administration.

PCMX documentation

The communications program PCMX is supplied with openUTM on Unix, Linux and Windows systems. The functions of PCMX are described in the following documents:

- CMX manual "Betrieb und Administration" (Unix-Systeme) for Unix, Linux and Windows systems (only available in German)
- PCMX online help system for Windows systems

1.2.2 Documentation for the openSEAS product environment

The **Concepts and Functions** manual briefly describes how openUTM is connected to the openSEAS product environment. The following sections indicate which openSEAS documentation is relevant to openUTM.

Integrating Java EE application servers and UTM applications

The BeanConnect adapter forms part of the openSEAS product suite. The BeanConnect adapter implements the connection between conventional transaction monitors and Java EE application servers and thus permits the efficient integration of legacy applications in Java applications.

The manual **BeanConnect** describes the product BeanConnect, that provides a JCA 1.5- and JCA 1.6-compliant adapter which connects UTM applications with applications based on Java EE, e.g. the Oracle application server.

Connecting to the web and application integration

Alternatively, you can use the WebTransactions product instead of the UTM HTTP program interface. Then you will need the **WebTransactions** manuals. The manuals will also be supplemented by JavaDocs.

1.2.3 Readme files

Information on any functional changes and additions to the current product version described in this manual can be found in the product-specific Readme files.

Readme files are available to you online in addition to the product manuals under the various products at <https://bs2manuals.ts.fujitsu.com>. For the BS2000 platform, you will also find the Readme files on the Softbook DVD.

Information on BS2000 systems

When a Readme file exists for a product version, you will find the following file on the BS2000 system:

```
SYSRME.<product>.<version>.<lang>
```

This file contains brief information on the Readme file in English or German (<lang>=E/D). You can view this information on screen using the `/SHOW-FILE` command or an editor.

The `/SHOW-INSTALLATION-PATH INSTALLATION-UNIT=<product>` command shows the user ID under which the product's files are stored.

Additional product information

Current information, version and hardware dependencies, and instructions for installing and using a product version are contained in the associated Release Notice. These Release Notices are available online at <https://bs2manuals.ts.fujitsu.com>.

1.3 Changes in openUTM V7.0

The following sections provide more details about the changes in the individual functional areas.

1.3.1 New server functions

UTM as HTTP-Server

A UTM application can also act as an HTTP server.

GET, PUT, POST and DELETE are supported as methods. In addition to HTTP, access via HTTPS is also supported.

The following interfaces have been changed:

- Generation

All systems:

- KDCDEF statement BCAMAPPL:

- Additional specification for the transport protocol for the operand T-PROT= with value SOCKET

*USP: The UTM socket protocol is to be used on connections from this access point.

*HTTP: The HTTP protocol is to be used for connections from this access point.

*ANY: Both the UTM socket protocol and the HTTP protocol are supported on connections from this access point.

- Additional specification for encryption for the operand T-PROT= with value SOCKET

SECURE: On connections from this access point, communication takes place using transport layer security (TLS).

- New operand USER-AUTH = *NONE | *BASIC. Herewith you can specify which authentication mechanism HTTP clients must use for this access point.

- KDCDEF statement HTTP-DESCRIPTOR:

This statement defines a mapping of the path received in an HTTP request to a TAC and additional processing parameters can be specified.

BS2000 systems:

- KDCDEF statement CHAR-SET:

With this statement, each of the four UTM code conversions provided by openUTM can be assigned up to four character set names.

- Programming

- KDCS communication area (KB):

In the header of the KDCS communication area, there are new indicators for the client protocols HTTP, USP-SECURE, and HTTPS in the *kccp/KCCP* field.

- KDCS call INIT PU:

- The version of the interface has been increased to 7.

- To obtain the complete available information, the value 372 must be specified in the KCLI field.

- New fields for requesting (KCHTTP/http_info) and returning (KCHTTPINF/httpInfo) HTTP-specific information.

- Administration interface KDCADMI

- The data structure version of KDCADMI has been changed to version 11 (field *version_data* in the parameter area).

-
- New structure *kc_http_descriptor_str* in the identification area to support the HTTP descriptor.
 - New structure *kc_character_set_str* in the identification area for supporting the HTTP character set.
 - New fields *secure_soc* and *user_auth* in structure *kc_bcamappl_str* for the support of HTTP access points.
 - UTM-HTTP program interface

In addition to the KDCS interface, UTM provides an interface for reading and writing HTTP protocol information and handling the HTTP message body.

The functions of the interface are briefly listed below:

- Function *kcHttpGetHeaderByIndex()*
This function returns the name and value of the HTTP header field for the specified index.
- Function *kcHttpGetHeaderByName()*
The function returns the value of the HTTP header field specified by the name.
- Function *kcHttpGetHeaderCount()*
This function returns the number of header fields contained in the HTTP request, that can be read by the program unit.
- Function *kcHttpGetMethod()*
This function returns the HTTP method of the HTTP request.
- Function *kcHttpGetMputMsg()*
This function returns the MPUT message generated by the program unit.
- Function *kcHttpGetPath()*
This function returns the HTTP path of the HTTP request normalized with *KC_HTTP_NORM_UNRESERVED*.
- Function *kcHttpGetQuery()*
This function returns the HTTP query of the HTTP request normalized with *KC_HTTP_NORM_UNRESERVED*.
- Function *kcHttpGetRc2String()*
Help function to convert a function result of type enum into a printable zero terminated string.
- Function *kcHttpGetReqMsgBody()*
This function returns the message body of the HTTP request.
- Function *kcHttpGetScheme()*
This function returns the schema of the HTTP request.
- Function *kcHttpGetVersion()*
This function returns the version of the HTTP request.
- Function *kcHttpPercentDecode()*
Function to convert characters in percent representation in strings to their normal one-character representation.
- Function *kcHttpPutHeader()*
This function passes an HTTP header for the HTTP response.
- Function *kcHttpPutMgetMsg()*
This function passes a message for the program unit, which can be read with MGET.
- Function *kcHttpPutRspMsgBody()*
This function passes a message for the message body of the HTTP response.
- Function *kcHttpPutStatus()*
This function passes a HTTP status code for the HTTP response.

- Communication via the Secure Socket Layer (SSL)

BS2000 systems:

- If a BCAMAPPL with T-PROT=(SOCKET,...,SECURE) has been generated for a UTM application, an additional task is started with a reverse proxy when UTM starts the application. The reverse proxy acts as the TLS Termination Proxy for the application and handles all SSL communication.

Unix, Linux and Windows systems :

- Another network process of the type *utmnetss/* is available for secure access with TLS.

If BCAMAPPL is generated with T-PROT=(SOCKET,...,SECURE) for a UTM application, a number of *utmnetss/* processes are started when UTM is started. The number of these processes depends on the value LISTENER-ID of these BCAMAPPL objects. All TLS communication for the assigned BCAMAPPL port numbers is handled in a *utmnetss/* process.

Encryption

The encryption functionality in UTM between a UTM application and a UPIC client has been revised. Security gaps have been closed, modern methods have been adopted and delivery has been simplified as follows:

- UTM-CRYPT variant

Previously, the encryption functionality in UTM was only available if the product UTM-CRYPT had been installed. With UTM V7.0 this is no longer necessary. As of this version, the decision as to whether or not to use the encryption functionality is made via generation or at the time of application start.

- Security

A vulnerability has been fixed in the communication between a UTM application and a UPIC client.

! This means that encrypted communication with a UTM application V7.0 is only possible together with UPIC client applications as of UPIC V7.0!

- Encryption Level 5 (*Unix, Linux and Windows systems*)

KDCDEF statements PTERM, TAC and TPOOL

The operand ENCRYPTION-LEVEL has an additional level 5, where the Diffie-Hellman method based on Elliptic Curves is used to agree the session key and input/output messages are encrypted with the AES-GCM algorithm.

OSI-TP communication and port numbers

BS2000 systems:

- KDCDEF statement OSI-CON

The operand LISTENER-PORT can also be specified on BS2000 systems.

- Administration interface KDCADMI

In the structure *kc_osi_con_str*, the port number is also displayed in the *listener-port* field on BS2000 systems.

Subnets

In a UTM application, subnets can also be generated on BS2000 systems in order to restrict access to UTM applications to defined IP address ranges. In addition, name resolution can be controlled via DNS.

The following interfaces have been changed for this purpose:

- Generation

BS2000 systems:

- KDCDEF statement SUBNET:

The SUBNET statement can also be specified on BS2000 systems.

All systems:

- KDCDEF statement SUBNET:

RESOLVE-NAMES=YES/NO can be used to specify whether or not a name resolution via DNS is to take place after a connection is established.

If name resolution takes place, the real processor name of the communication partner is displayed via the administration interface and in messages. Otherwise, the IP address of the communication partner and the name of the subnet defined in the generation are displayed as the processor name.

- Administration interface KDCADMI

The structures *kc_subnet_str* and *kc_tpool_str* contain a new field *resolve_names*.

Access data for the XA database connection

A modified but not yet activated user name for the XA database connection can be read by Administration (KDCADMI):

- Operation code KC_GET_OBJECT:

Data Structure *kc_db_info_str*. New field *db_new_userid*.

Reconnect for the XA database connection

If an XA action to control the transaction detects that the connection to the database has been lost, the system tries to renew the connection and repeat the XA action.

Only if this is not successful, the affected UTM process and the UTM application are terminated abnormally.

Previously, the UTM application was terminated abnormally, if a XA-Connection was lost without trying to reconnect.

Other changes

- XA messages

The messages regarding the XA interface were extended by the inserts UTM-Userid and TAC. The messages K204-K207, K212-K215 and K217-K218 are affected.

- UTM-Tool KDCEVAL

In the TRACE 2 record of KDCEVAL the type of the last order (bourse announcement) was recorded in the WAITEND record (first two bytes can be printed).

1.3.2 Discontinued server functions

In particular, the following functions has been discontinued:

- **KDCDEF utility**

Several functions have been deleted and can no longer be generated in KDCDEF. If they are still specified, this will be rejected with a syntax error in the KDCDEF run.

- **KDCDEF statement PTERM**
Operand values 1 and 2 for ENCRYPTION-LEVEL
- **KDCDEF statement TPOOL**
Operanden values 1 and 2 for ENCRYPTION-LEVEL
- **KDCDEF statement TAC**
Operanden value 1 for ENCRYPTION-LEVEL

- *BS2000 systems*

- **UTM Cluster:**
UTM cluster applications are no longer supported on BS2000 systems.

- *Unix, Linux and Windows systems*

- **TNS operation:**
When starting a UTM application, the TNS generation is no longer read. The addressing information must be stored completely during configuration with KDCDEF.

1.3.3 New client functions

Encryption

The encryption functionality in openUTM-Client has been revised. Security gaps have been closed, modern methods have been adopted and delivery has been simplified as follows:

- **UTM-CLIENT-CRYPT variant**
Until now, the encryption functionality in openUTM-Client was only available if the product UTM-CLIENT-CRYPT was installed. With openUTM Client V7.0 this is no longer necessary. As of this version, it is decided at runtime whether the encryption functionality is available or not.
- **Security**
A vulnerability has been fixed when communicating with a UTM application.
- **Encryption Level 5**
The openUTM client V7.0 supports communication with UTM V7.0 applications when ENCRYPTION-LEVEL 5 was generated for the connections to the UPIC client.
With Level 5 the Diffie-Hellman method, based on Elliptic Curves, is used to agree on the session key. Input /output messages are encrypted using the AES-GCM algorithm. AES-GCM is an [authenticated encryption](#) algorithm designed to provide both data authenticity (integrity) and confidentiality.
Level 5 is supported by the openUTM-Client on all platforms.
- **Encryption BS2000**
openUTM-Client (BS2000) uses openssl instead of BS2000-CRYPT analogous to Unix, Linux and Windows systems.

1.3.4 New functions for openUTM WinAdmin

WinAdmin supports all new features of openUTM 7.0 relating to the program interface for the administration.

1.3.5 New functions for openUTM WebAdmin

WebAdmin supports all new features of openUTM 7.0 relating to the program interface for the administration.

1.4 Notational conventions

Metasyntax

The table below lists the metasyntax and notational conventions used throughout this manual:

Representation	Meaning	Example
UPPERCASE LETTERS	Uppercase letters denote constants (names of calls, statements, field names, commands and operands etc.) that are to be entered in this format.	LOAD-MODE=STARTUP
lowercase letters	In syntax diagrams and operand descriptions, lowercase letters are used to denote place-holders for the operand values.	KDCFILE=filebase
<i>lowercase letters in italics</i>	In running text, variables and the names of data structures and fields are indicated by lowercase letters in italics.	<i>utm-installationpath</i> is the UTM installation directory
Typewriter font	Typewriter font (Courier) is used in running text to identify commands, file names, messages and examples that must be entered in exactly this form or which always have exactly this name or form.	The call tpcall
{ } and	Curly brackets contain alternative entries, of which you must choose one. The individual alternatives are separated within the curly brackets by pipe characters.	STATUS={ ON OFF }
[]	Square brackets contain optional entries that can also be omitted.	KDCFILE=(filebase [, { SINGLE DOUBLE }])
()	Where a list of parameters can be specified for an operand, the individual parameters are to be listed in parentheses and separated by commas. If only one parameter is actually specified, you can omit the parentheses.	KEYS=(key1,key2,...key <i>n</i>)
<u>Underscoring</u>	Underscoring denotes the default value.	CONNECT= { YES <u>NO</u> }
abbreviated form	The standard abbreviated form of statements, operands and operand values is emphasized in boldface type. The abbreviated form can be entered in place of the full designation.	TRANSPORT-SELECTOR =c`C`
...	An ellipsis indicates that a syntactical unit can be repeated. It can also be used to indicate sections of a program or syntax description etc.	Start KDCDEF ... OPTION DATA=statement_file ... END

Symbols



Indicates references to comprehensive, detailed information on the relevant topic.



Indicates notes that are of particular importance.



Indicates warnings.

Other

utmpath On Unix, Linux and Windows systems, designates the directory under which openUTM was installed.

filebase On Unix, Linux and Windows systems, designates the directory of the UTM application. This is the base name generated in the KDCDEF statement MAX KDCFILE=.

\$userid On BS2000 systems, designates the user ID under which openUTM was installed.

upic_dir The directory under which UPIC Client for UPIC Carrier System is installed on Unix, Linux, or Windows system.

2 Structure and use of UTM programs

In this chapter you will be presented with an initial overview of programming UTM applications. You will learn what services and program units are and how you can apply the openUTM concepts to implement the business logic of your applications.

A UTM application provides your users with certain services: it processes service requests (jobs) which are sent by terminal users, client programs or other applications.

A **service** serves to process a job from a UTM application. It consists of one or more transactions and one or more program runs. openUTM differentiates between dialog services and asynchronous services. A UTM service generally corresponds to a business transaction of the application logic.

When you design an application you program the business transactions of the application logic in the form of **program units**, also called **service routines**. The program units run as subprograms and are under the control of the main routine of a UTM application; the main routine is a component of the openUTM system code.

You specify the task of the service you wish to provide the users of your application with in the business logic implemented in the program units. The program units can be programmed in one of the common programming languages (C, C++, COBOL and others).

You can access UTM system functions and external resource managers such as databases from within the program units. The program units utilize the UTM system functions using integrated **UTM calls**, e.g. for transaction management or to send messages to a communication partner.

You can use various interfaces for these UTM calls: In addition to the KDCS interface described in this manual you can also use the X/Open interfaces CPI-C, XATMI and TX (see the openUTM manual "Creating Applications with X/Open Interfaces").

In addition, openUTM provides you with the UTM-HTTP program interface functions that you can use when communicating with HTTP clients. These are described in the chapter "[UTM-HTTP Calls](#)".

Characteristics of the KDCS interface

The KDCS interface (compatible data communication system) has been defined and standardized (DIN 66 265) as a manufacturer-independent interface for transaction-oriented applications. openUTM supports the full extent of this standard and offers significant extensions, e.g. for distributed processing. For an overview of these extensions refer to the table in chapter "[Complete overview of KDCS calls](#)".

KDCS possesses the following function characteristics:

- extensive range of function calls for universal use
(e.g. also for pseudo conversations, message queuing or direct communication with terminals)
- KDCS specific storage area for simple and safe programming
- event functions for event control

KDCS is available for the C, C++ and COBOL programming languages;
on BS2000 systems, it is also available for Assembler, Fortran, PL/I and Pascal-XT.

UTM application program - UTM application

A UTM application program consists of the UTM main routine KDCROOT and the UTM program units.

The main routine KDCROOT controls the flow of the application as part of the UTM system code. It is created when the application is generated (see the openUTM manual “Generating Applications”).

In order to run the UTM program units under openUTM management, you have to link the compiled service routines, together with other modules (assignment tables, messages, used libraries, etc.) and the main routine KDCROOT to the **UTM application program** (see the openUTM manual “Using UTM Applications on BS2000 Systems” and the openUTM manual “Using UTM Applications on Unix, Linux and Windows Systems”).

The linking can be done statically (i.e. before the application is started) or dynamically (i.e. when the application is started or during its operation).

At **UTM application** startup the UTM application is started in a number of processes which is specified by you. From a technical point of view, the UTM application is therefore a processing group which constitutes a logical server unit at runtime.

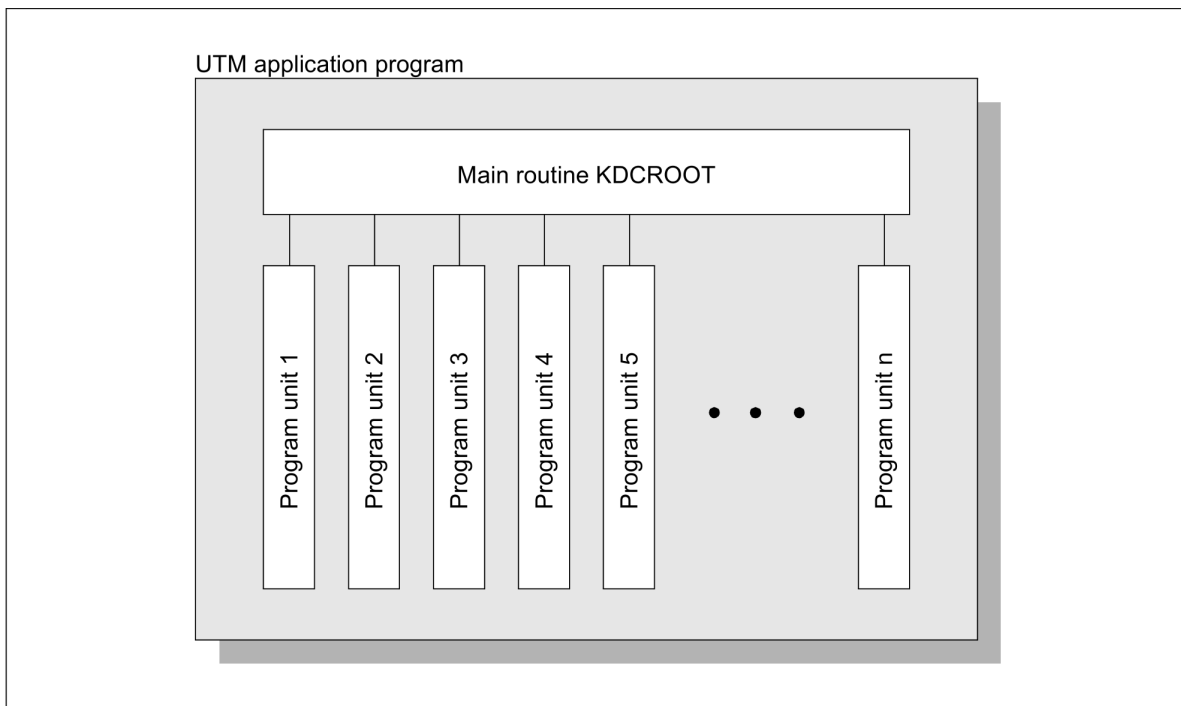


Figure: Main routine KDCROOT and multiple program units

The program units and the main routine KDCROOT interact via **KDCS calls**. In a program unit, the KDCS calls are used to inform the main routine KDCROOT which function openUTM is to perform. You use the KDCS parameter area to specify the necessary entries and pass its address as the first parameter with each KDCS call.

Predefined language-specific data structures enable you to structure the KDCS parameter area, in COBOL these are located in the KCPAC COPY element and in C/C++ in the *kcmac.h* include file. For a language-independent description of the value to be entered in this area for the individual KDCS calls refer to chapter “[KDCS calls](#)”. For language-specific particularities refer to the chapters “[Additional information for C/C++](#)” and “[Additional information for COBOL](#)”.

The sections below explain the way in which you can structure an application program.

i As used in this chapter, the terms "program" and "program unit" refer to the execution of this program unit, not to the program text. For example, the phrase "sequence of calls in a program unit" refers to the sequence in which these calls are run, not the sequence in which they appear in the source program. This is also referred to as the **program unit run**.

2.1 The openUTM service concept

Starting a service

One or more transaction codes are assigned to each program unit, either during application generation or using dynamic configuration.

The transaction code of the first program unit of a service has a special function because it is used to start this service. This transaction code is also called the service transaction code or service TAC for short. openUTM sets up a specific context (storage area, etc.) for each service started.

You can enter the service TAC in a large number of ways, e.g. by entering it at the terminal, selecting a menu item in an alphanumeric format, mouse clicking on a GUI client or using a Web browser.

Together with the transaction code you may transfer a message to openUTM containing necessary data for the required processing.

Dialog step and processing step

In the simplest case, a service consists of a single processing step, i.e. no interactions are required to process the service request: the result is output following the input of the service TAC, e.g. "All finished".

However, in many cases this structure is inadequate: you may have to request additional data, display intermediate results, or take account of individual selection options and branches in the service sequence. A service therefore often consists of multiple dialog steps.

A **dialog step** starts with a dialog message which one communication partner sends to the UTM application, and terminates with a dialog message which the service sends to the same communication partner as a response. Between these two points in time, the data is processed and there is no communication with this communication partner.

In distributed processing, a service does not only communicate with the user who started the service, but also with one or more partner services. A service started by a user may therefore not send the next message to the user but to another service application. In this case, since the message is not a response, it is called a processing step rather than a dialog step: A **processing step** starts when a dialog message is received and ends when the next dialog message is sent. This can be a response to the same partner (in which case the processing step corresponds to a dialog step) or a message to a third party.

A service may therefore be divided into multiple dialog steps, and a dialog step – in distributed processing – into multiple processing steps.

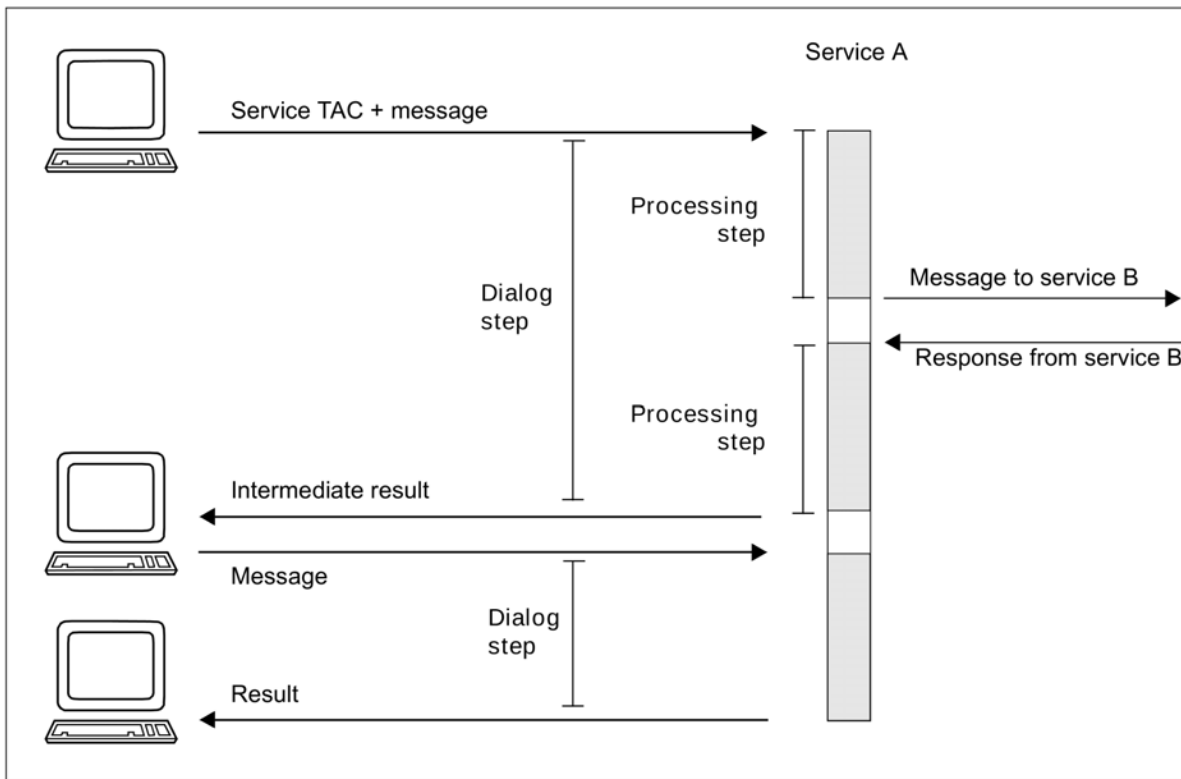


Figure: Dialog steps and processing steps

Switching between inputs and responses

openUTM requires a "strict dialog" to structure dialog services, i.e. each message must be followed by an answer. After sending a message to a service, you must receive a response before you can send another message to this partner.

This sequence - together with the modular service structure for processing steps - enables openUTM to maximize process utilization (see following two sections).

Modular processing steps in service structure

If a service consists of multiple dialog or processing steps, the service does not usually consist of only **one** service routine. Instead, it consists of a sequence of separate service routines called **program units**. Normally a program unit is equivalent to a processing step, i.e. a program unit reads a message and issues a message when it terminates. Subsequently the process is automatically released and is available for other jobs. The next program unit does not start until the next message is received from the communication partner.

For example, the service does not occupy a process while a user reads the output and prepares the next input at a terminal. As soon as the terminal user has finished the input, another process may, under certain circumstances, continue the dialog without notifying the user or the program unit.

Hence openUTM optimizes process utilization and this has a positive effect on system performance. openUTM uses this dialog concept (also called "**pseudo-conversational**") for dialogs with terminal users as well as for program-program communication.

In addition, the basic design for the use of modular processing steps simplifies the design of applications and results in clearly structured programs. However, it is flexible enough not to limit the programmer and makes a number of variations available to openUTM.

For examples of multi-step services and more information about connections between program units refer to section [“Structuring services”](#).

Asynchronous services

Using openUTM you can define services which run in the dialog with the user as well as services which can be started even when disconnected from the user. The message queuing functionality integrated in openUTM enables you, for example, to disconnect particularly large and non-time critical jobs - such as long statistical calculations or sorting tasks - from online dialogs without discontinuing transaction logging. You can use the message queuing functionality not just to perform processing jobs; it also lets you output messages, e.g. for print jobs, messages to a terminal or messages to service-controlled queues ([“Messages to service-controlled queues”](#)).

The message queuing concept and its scope of application are introduced in the openUTM manual “Concepts and Functions”, for further information see section [“Message Queuing \(asynchronous processing\)”](#) of the present manual.

2.2 Structure of a program unit

Before we explain the structure of more complex services we will describe the structure of a single program unit in this section. First the program framework applicable for all types of program units is explained followed by the structure of a dialog program unit.

The structure of an asynchronous program unit is explained in section [“Structure of an asynchronous service”](#).

2.2.1 Program framework

The interaction between the program units and openUTM is implemented using **KDCS calls**. With these calls you inform openUTM which functions are to be executed. You pass the address of the **KDCS parameter area** in every KDCS call, and in some calls you pass the address of a message area.

The call parameters are passed to openUTM in the KDCS parameter area. You are provided with predefined language-specific data structures for the KDCS parameter area, in COBOL these are located in the KCPAC COPY element and in C/C++ in the *kcpa.h* include file. For a language-independent description of the value to be entered in this area for the individual KDCS calls refer to chapter “[KDCS calls](#)”.

openUTM passes return information after every KDCS call (except for PEND) in the **KB return area**. The evaluation of the return codes tells you if the execution was successful or unsuccessful and can be used to take the appropriate control measures in the program (see also section “[Programming error routines](#)”).

You will also find the current information on users, services, program units and communication partners after every KDCS call in the **KB header**.

The KB header and the KB return area are part of the **communication area (KB)**, see “[Communication area \(KB\)](#)”. openUTM provides a program unit with the address of the KB in a call parameter when the program unit is called.

You are provided with predefined language-specific data structures - for COBOL in the COPY element KCKBC and for C/C++ in the *kcca.h* include file - for the structure of the KB header and KB return area.

The first UTM call in a program unit run is the INIT call. This call initiates the interoperation of a program unit and openUTM. Other program code may precede the INIT call. After the INIT call, openUTM provides current, runtime-specific information in the KB header and in the message area.

The final call in a program unit run is the PEND call. This call terminates the program unit; control is not returned to the program unit once this call has been issued.

The different variants of the PEND call are used to control execution of a UTM service. You have the following options:

- PEND PR continues the processing step continues in another program unit without carrying out a message exchange with the partner.
- PEND PA same as PEND PR.
- PEND PS specially for the sign-on service, similar to PEND PR.
- PEND KP terminates the processing step but not the transaction.
- PEND SP terminates the transaction but not the processing step.
- PEND RE simultaneously terminates the processing step and the transaction.
- PEND FI terminates dialog step, transaction and service.
- PEND FC terminates transaction and service and continues the dialog step in another service.
- PEND RS aborts the processing step and rolls back the transaction to the last synchronization point.

PEND ER aborts the processing step, rolls back the transaction, terminates the service and generates a UTM dump. On BS2000 systems the application program is loaded dynamically; on Unix, Linux and Windows systems it is restarted.

PEND FR same effect as **PEND ER** but without dynamic loading or restarting of the application program.

Note that many actions, such as the sending of an output message to the communication partner of a UTM service, are not executed by openUTM until the **PEND** call is issued, i.e. they are not executed during the program unit run. The source of this behavior is the transaction-oriented manner in which openUTM functions; you can decide if the action executed in this transaction by the program unit is to be committed or rolled back up until the end of the transaction.

If a serious error occurs in a UTM transaction, then openUTM independently rolls back the entire transaction to the most recent synchronization point and terminates the service (see also the openUTM manual “Concepts and Functions”).

2.2.2 Structure of a dialog program unit

openUTM requires a "strict dialog" for dialog program units, i.e. each message input must be followed by a message output specifying the result or an error message.

Following **INIT**, the program unit can use **MGET** to read the dialog message, which can be received from a terminal, a client program or from another program.

This message can be:

- a complete message or
- a message segment
- an empty message if, for example, only a TAC has been specified
- a rollback message from a program unit which has been terminated using PEND RS
- a return code if, for example, the user pressed a function key. In this case, the message must be read with another MGET.
- in the case of distributed processing, status information from, for example, a job receiver which terminated following an error
- in the case of distributed processing using OSI TP, a handshake request (sent by the partner using MPUT HM) or a negative handshake confirmation (sent using MPUT EM)

After this input has been processed, you have either to continue the processing step in another program unit or to use **MPUT** to answer your partner's query (end of dialog step). In the case of distributed processing the message can also be addressed to a job-receiving service (no end of dialog step, only end of processing step).

The final UTM call in your program unit must be a **PEND**, as described in section "[Program framework](#)".

If the PEND call terminates the processing step, openUTM outputs the message to the terminal, the client program or another program after PEND processing.

i As a general principle, you have to issue an MPUT call before a PEND call which terminates a processing step. Exceptions to this rule will be indicated explicitly.

The diagram below shows the basic structure of a dialog program unit:

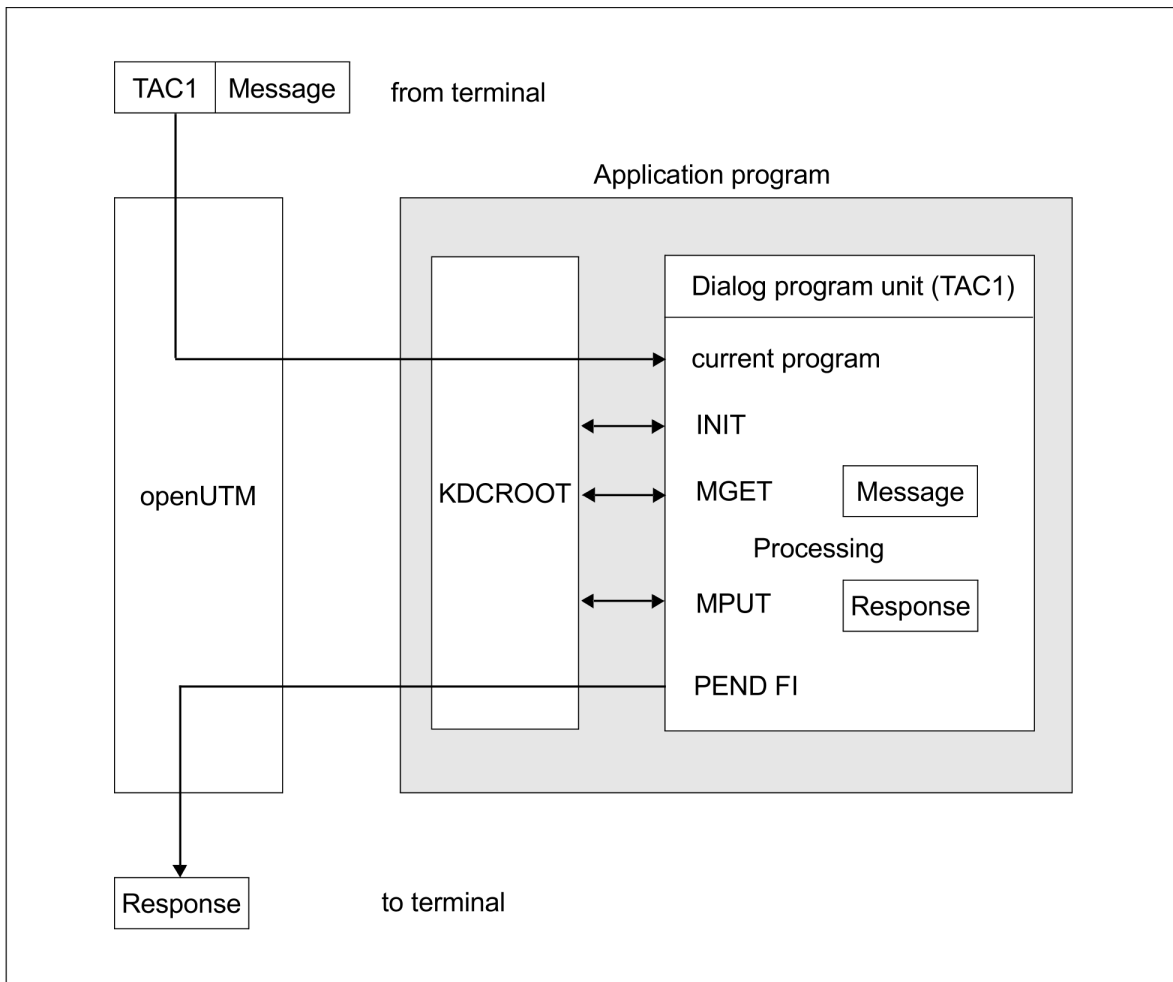


Figure: Structure of a dialog program

The transaction code "TAC1" is input by the terminal user. TAC1 was assigned to the program unit at generation time (KDCDEF statement TAC, operand PROGRAM=current program name).

2.2.3 Reentrant capability of program units

openUTM always uses a transaction code to call a program unit. However, the program unit is not loaded each time it is called, instead a program copy in virtual memory processes unrelated jobs in sequence. In practice this means that there may be a switch to another process following a PENDING, with the result that the subsequent program unit runs in another process and may therefore be confronted by another data environment.

A UTM program unit must therefore be serially reusable, i.e. it must be a reentrant program:

- program-specific data must be set to its initial status at the beginning of the program unit run
- a program-specific data field may only be read if it has already been written in the same program unit run.

openUTM simplifies the programming of reentrant programs for you. It provides a special program unit-specific storage area (SPAB see "[Standard primary working area \(SPAB\)](#)") which is managed by openUTM. If you use this storage area for all variable data, openUTM automatically ensures that your programs are reentrant.

What this means for COBOL program units is that variables in the WORKING STORAGE SECTION must be installed again when calling the program unit, assuming they have been defined in an earlier program unit run. For C/C++ this applies to the variables with the storage class attribute *static* or *extern* and to those with an external connection (global module variables without a storage class attribute). For variables whose scope applies to more than one process (i.e. which lie in shared memory) at least write access to such variables must be serialized. However, the variables mentioned above can be used without restrictions for read-only access.

For C and C++, variables with the storage class attribute *auto* or *register* can be used without problems. They must, however, be defined before reading.

2.3 Structuring services

A service may consist of one or more program units. The structure of a service consisting of only one program unit and processing a single processing step (single-step service) is illustrated in the diagram on "[Structure of a dialog program unit](#)":

A single program unit processes the required task entirely in one step and subsequently terminates it using PENDING.

For complex tasks which require multiple steps, you can structure a service or transaction into multiple parts. To do this, you have the following options:

- multi-step services
- multiple program units in one processing step
- multiple processing steps in one program unit
- subprogram calls issued by program units
- chained services
- stacked services

You may also use a combination of these options.

You have considerable freedom when designing your UTM program units: the only obligatory rules are that you use INIT and PENDING to establish the program framework and MPUT for the processing steps.

2.3.1 Multi-step services

Dialogs consisting of multiple processing steps constitute a frequent type of transaction processing. This technique is designed to simplify the work of application users. They should be able to formulate jobs interactively step by step and thus be able to evaluate the interim results at each processing step.

The reservation of train tickets, for example, can be programmed as a service in two steps:

1st step: Query whether seats are still available.

2nd step: Reserve the seat and confirm reservation.

By chaining the programs that implement the individual processing steps, you ensure that the entire service is processed in the right order. You chain program units via entries in the PEND call. Here you select the RE operation modifier in the KCOM field if you also want to set a synchronization point at the end of the processing step and specify the transaction code of the follow-up program in the KCRN field. If you only want to terminate the processing step without setting a synchronization point, you have to select the KP operation modifier instead of RE in the PEND call. The follow-up program is started when openUTM receives the next input message.

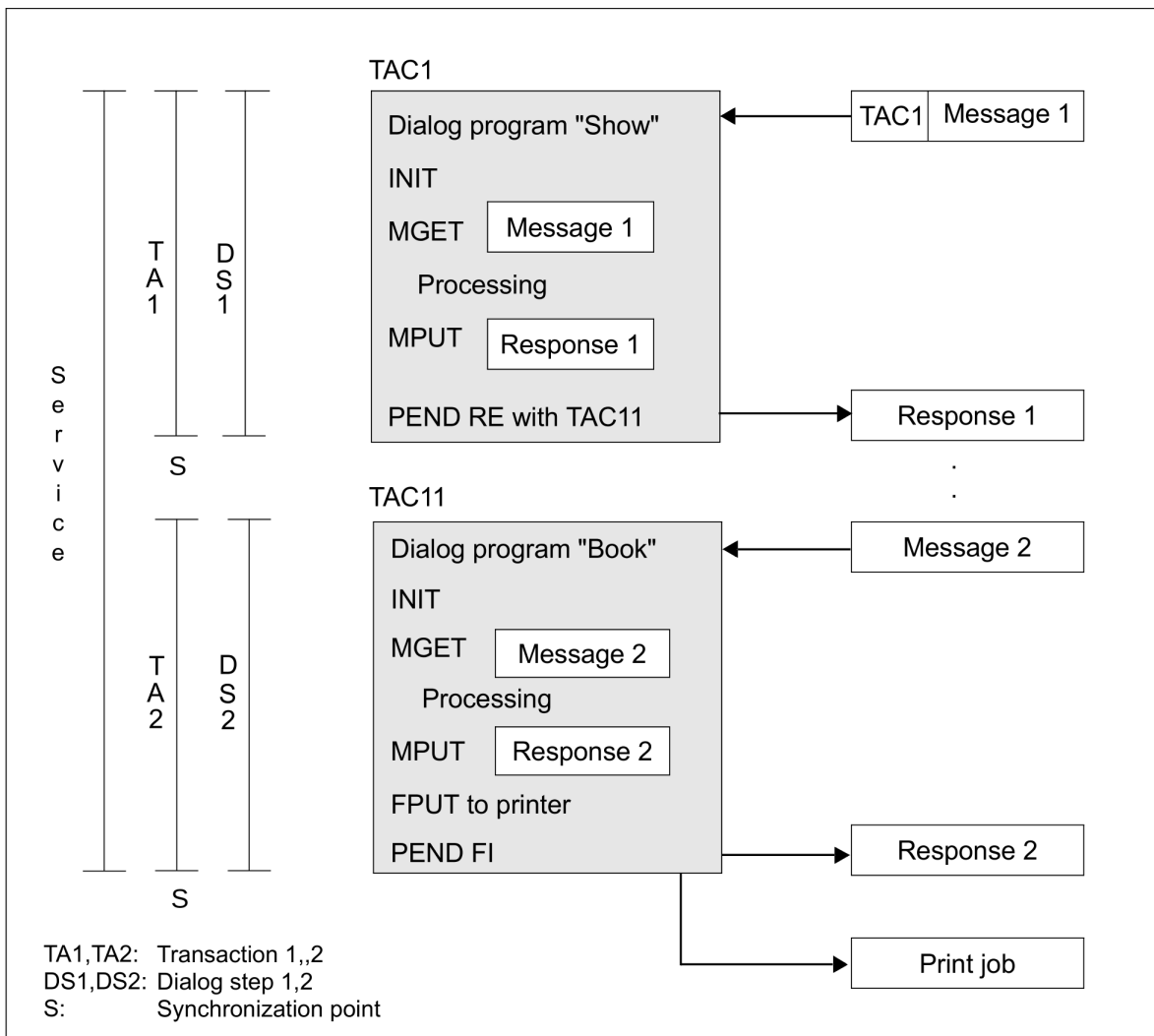


Figure: Multi-step service

The service presented in the figure consists of two program units which perform one dialog step each. However, there is no limit to the number of program units that you can combine in a service. For all program units of a service, openUTM provides service-specific storage areas which can be used by the program units to transfer information (see "[KDCS storage areas in openUTM](#)"). These storage areas are included in transaction logging.

The second program unit contains an FPUT call in addition to the MPUT call. This call does not create a dialog message. It creates an asynchronous message, in this case an output message to the printer.

Same processing step for differing actions

If two or more actions of the same type are performed in an application, it is advisable to handle processing steps that are identical for all actions in a single program unit. This is demonstrated using multiple step services in the example below:

The data of an insurance policy is to be displayed at the outset of different actions, so that one of the following steps can be performed:

- modify data
- delete data
- calculate premium
- report a claim

The first step is identical for all four actions, while the subsequent steps are all different (see diagram below).

First, all four actions are processed in the same program unit. Each action has its own transaction code, i.e. four different transaction codes are assigned to the first program unit. When the program unit is started, openUTM displays the transaction code used for the service start in the KCTACVG/ kccv_tac field of the KB header.

Depending on the transaction code the program unit determines which program unit is started as follow-up program unit, i.e. which follow-up TAC is entered in the KCRN field when calling PEND.

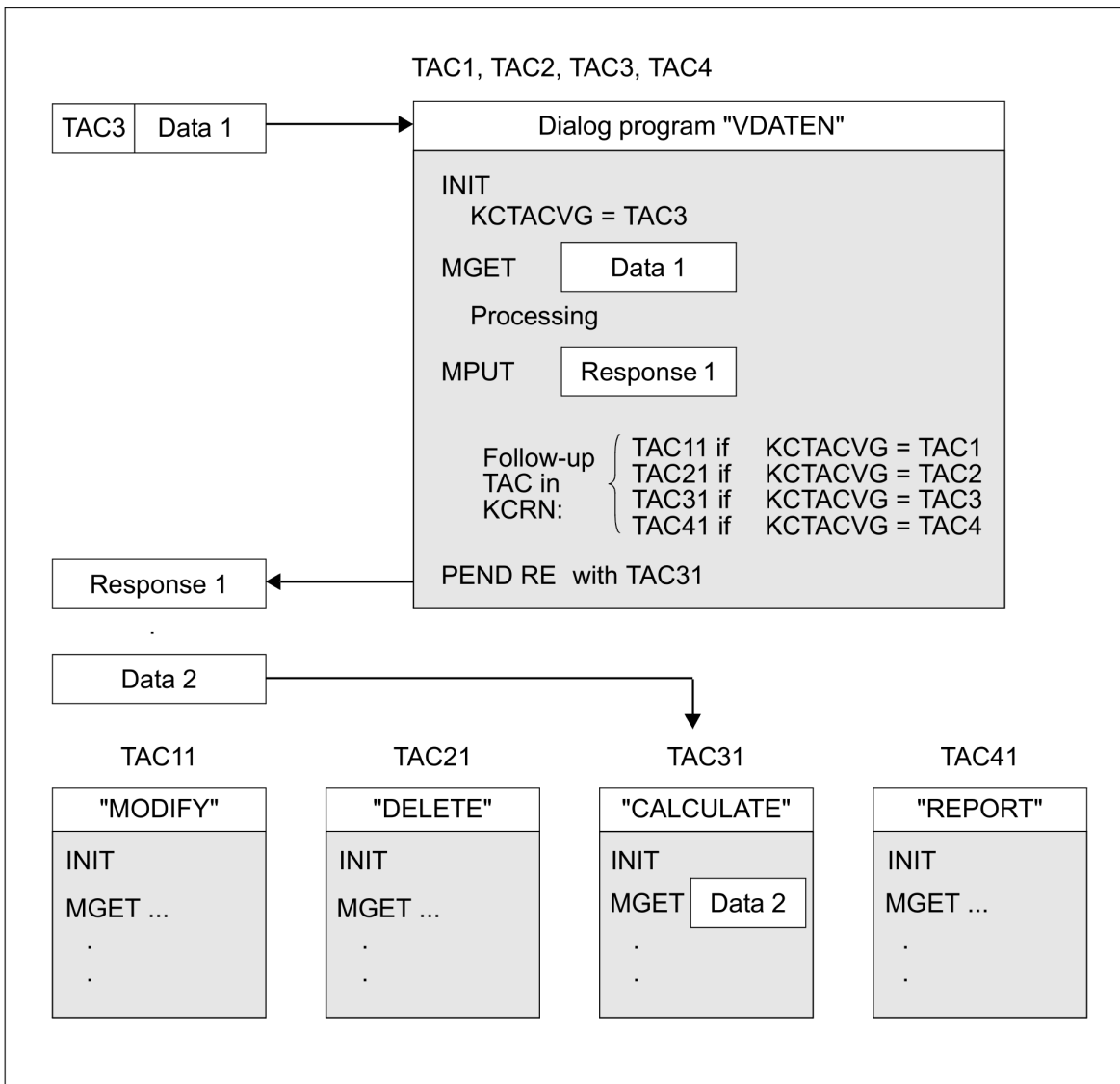


Figure: Program unit to which multiple transaction codes are assigned

2.3.2 Multiple program units in one processing step

If different processing steps contain identical subtasks, it is advisable to split the individual processing steps into several parts. You write a separate program unit for each subtask and this can be used jointly by all processing steps. This is an exception to the basic rule for a service structure "one processing step = one program unit": here, **one** processing step is performed by **multiple** program units. This is achieved by using the PEND PR/PA/SP calls which terminate the program unit, but not the processing step. If you use PEND SP, a synchronization point is set. If you use PEND PA/PR, the transaction remains open.

In the following diagram, the two processes are single-step services, although each of them consists of three program unit runs:

- The service to which the TAC1 transaction code is assigned changes the data of an insurance contract.
- The service to which the TAC2 transaction code is assigned deletes the data of an insurance contract.

What is common to both services is that they have to change the initial data record. In order to create a separate program unit to perform this common task the processing step is split into individual parts.

After the INIT call the KCTACVG field contains the TAC which was used to start the service. The program unit "CENTRAL" then determines which program unit has to be used to continue the transaction. You have to specify the TAC of this program unit in the KCRN field for both MPUT as well as PEND PR. The MPUT message is not sent to the communication partner, but to the follow-up program unit where it is read using MGET. Since the processing step is not terminated in the program unit "CENTRAL", an MPUT call is not mandatory in this program unit: you may also transfer the data using service-specific storage areas instead of MPUT (see also section "[KDCS storage areas in openUTM](#)").

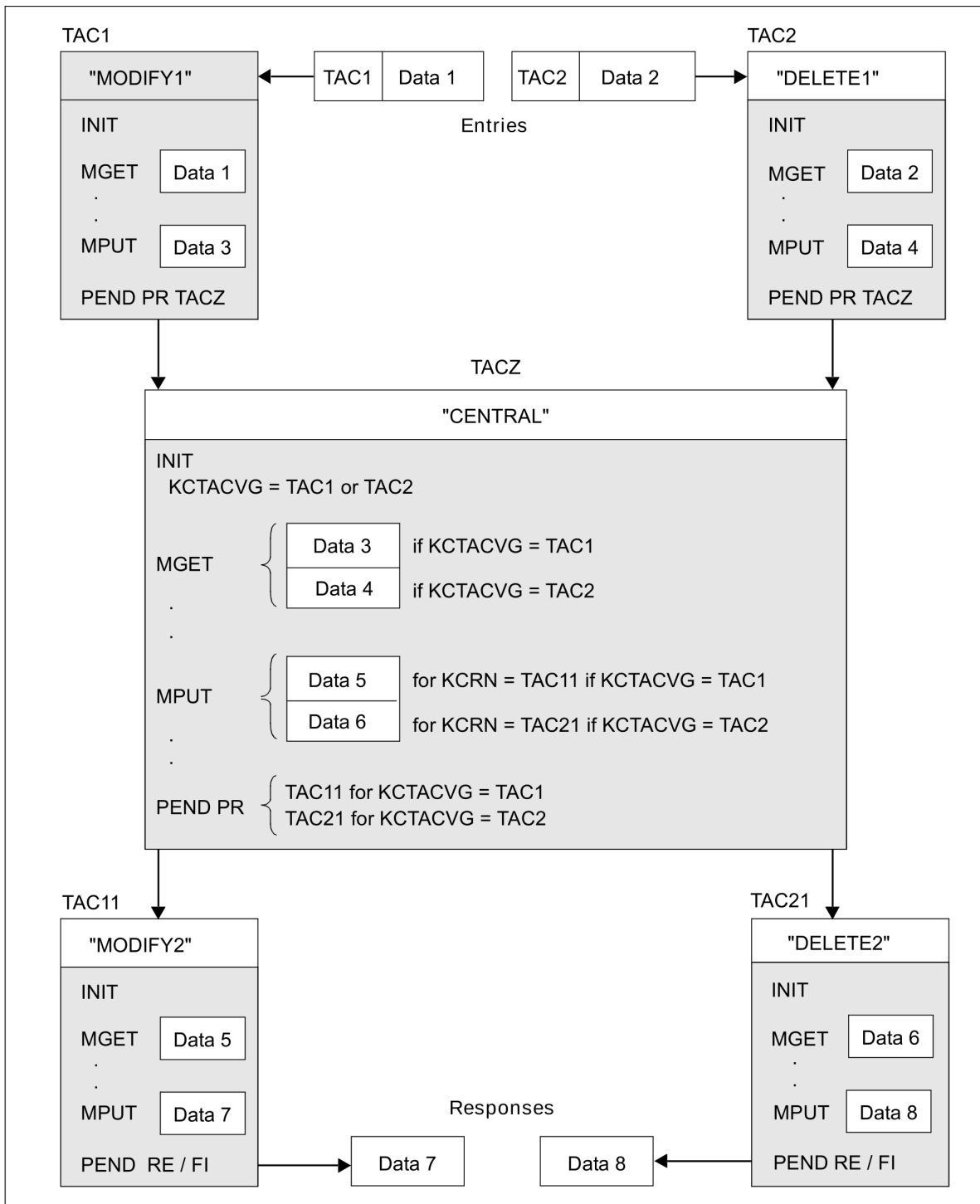


Figure: Multiple program units performing one processing step

2.3.3 Multiple processing steps in a single program unit

A UTM program unit runs in a process between INIT and PEND. Since the process is released at the end of the program unit, a follow-up program unit may run in a different process from the first. This means that the follow-up program unit cannot access the process-specific environment (context), such as resources and program-specific data areas of the first program unit. Usually this is not necessary, since data can either be transferred via an MPUT call issued to the follow-up program or via process-specific storage areas provided by openUTM.

However, openUTM also allows you to retain the process-specific context of a program unit for multiple processing steps. You use a PGWT (program wait) call with the operation modifiers KP, PR, CM and RB. This sets a wait point without terminating the program unit, i.e. the program context is preserved. These variants are used for different purposes.

- PGWT KP terminates the processing step and sends the MPUT message. The program unit waits until the next message arrives from the partner. PGWT KP corresponds to the PEND KP call in the previous program unit and the INIT call in the next program unit.
- PGWT PR waits for a message to a queue without terminating the processing step. PGWT PR corresponds to a PEND PA/PR call in the previous program unit and an INIT call in the next program unit.
- PGWT CM terminates the transaction without terminating the program unit. However, a synchronization point set with PGWT CM is not a restart point. The follow-up transaction can therefore be rolled back with PGWT RB only and not with PEND RS.

The following also applies:

- If an MPUT call was executed before the PGWT CM, the MPUT message is sent and the program unit waits until a response is received from the partner. This PGWT CM corresponds to a PEND RE call in the previous program unit and an INIT call in the next program unit.
- If no MPUT was executed before the PGWT CM call, the program unit is continued immediately. A PGWT CM without a preceding MPUT call corresponds to a PEND SP call in the previous program unit and an INIT call in the next program unit.
- PGWT RB rolls back a transaction.

The functions of two successive program units can therefore be performed by one program unit. The entire functional sequence then runs under one and the same process. The process-specific context is available until the end of the program unit run.

During that period, the program unit occupies a process exclusively. As a result, the UTM application usually requires more resources (processes).

The PGWT call permits the simple integration of program systems which expect a combined SEND/RECEIVE interface into openUTM.

Alongside the PEND PR/PA/SP calls, the PGWT call represents another way of varying the modular processing step structure:

While the **PEND PR/PA/SP** calls enable you to split **one** processing step over **multiple** program units, the **PGWT** calls make possible **multiple** processing steps in **one** program unit.

Since valuable resources are involved with the PWGT calls, these calls should be used only sparingly in an application; it should **only** be used where the other options of the KDCS interface are inadequate; the frequent use of PGWT calls can have a negative effect on the performance of a UTM application.

2.3.4 Subprogram calls from program units

In a program unit you can also issue subprogram calls, e.g. C/C++ functions or COBOL subprograms. These subprograms may contain subprogram calls themselves. Using subprogram calls you call programs via their program name (in C/C++: function name) and not via their transaction code.

Subprograms can also be written in a programming language other than that of the calling program.

For BS2000 systems, the points that then need to be taken into account and the compilers and runtime systems that are required are described in openUTM manual "Using UTM Applications on BS2000 Systems".

You will find more information on subprogram calls in the section "[C/C++ program units as subroutines](#)" and section "[COBOL program units as subroutines](#)".

The program run must either return to the program unit or be terminated in a subprogram using the PEND call.

2.3.5 Chaining services

Services are usually terminated by the **PEND FI** (finish) call. If you call PENDING a dialog message is sent to the terminal, a client program or another program. The end of service is also the end of the processing step.

However, you can use the **PEND FC** (finish and continue) call to chain another service and continue the processing step within that service. This is useful, for example, if a dialog message is not to be output to the client or if the use of TACs is to be hidden from the user.

Like PENDING, PENDING FC terminates both the transaction and the service and releases service-specific storage areas (LSSBs, KB). Data is transferred to the chained service using an MPUT call; you cannot use service-specific storage areas to do this.

The differences in programming to PENDING FI are as follows:

- With PENDING FC you have to enter the TAC of the chained service in the KCRN field.
- MPUT is not necessary before PENDING FC. However, if an MPUT call is issued then the follow-up TAC must also be entered in KCRN (as in PENDING PA/PR).

If the first transaction of the chained service is rolled back, then openUTM restarts at the synchronization point in PENDING FC and restarts the chained service.

2.3.6 Stacking services

A terminal user can stack a service, i.e. he or she can interrupt an already started service, insert another service and, when this terminates, continue the interrupted service. A service can only be stacked if it is located at a synchronization point, i.e. directly after a PEND RE.

There are two ways of doing this:

- by pressing a function key generated with SFUNC ...,STACK=...
- by using the event exit INPUT

Continuing a stacked service

A stacked service, also known as a predecessor, is reactivated as soon as the inserted service is terminated by PEND FI. The terminated service generates an output message. Since openUTM only permits service stacking at a synchronization point, both the last output message and the service-specific areas (KB, LSSB) of the predecessor are still available. You use the (last) MPUT call in the inserted service to determine how the output messages of the two services are to be processed.

You have three options:

- MPUT NE in the inserted service outputs the message of this service on the screen together with message K096. The terminal user presses Enter to receive the last output message of the predecessor.
- MPUT PM with KCLM = 0 immediately outputs the last output message of the predecessor (PM stands for "predecessor message").
- MPUT PM with KCLM > 0 (permitted only in format mode) overwrites the output message of the predecessor with the message of the inserted service to the length defined in KCLM. openUTM then outputs this revised predecessor message. The format specified in MPUT PM should be a partial format of the predecessor format.

MPUT PM is only permitted in an inserted service if the program unit is terminated by PEND FI, i.e. only in the last processing step of the service.

Service stacks

Service batches are formed by stacking services.

You can retrieve information about the current service stack in the following ways:

- the KCHSTA and KCDSTA fields of the KB header show the size of the stack and how this has changed since the last program unit run
- the INFO call INFO PC (predecessor service) provides information about the direct predecessor in the batch.

PEND FI in an inserted service always returns you to the immediate predecessor; a stack is deleted when the last inserted service has terminated.

2.4 Message Queuing (asynchronous processing)

Message Queuing (MQ) is a form of communication in which messages are exchanged via intermediate queues (store and forward) instead of being directly exchanged. Because there is no synchronization between the sending and receipt of messages, message to message queues are also called **asynchronous messages**. Communication takes place by means of **asynchronous jobs**. An asynchronous job consists of the asynchronous message, the recipient of the message and possibly also the desired time of execution.

openUTM provides you with two types of message queues:

- **UTM-controlled queues:**

In the case of UTM-controlled queues, the interposed queuing mechanism is made available in its entirety by openUTM. In other words, in addition to pure queuing functionality, openUTM also takes on the subsequent processing of the message (e.g. output to a communication partner or startup of a service).

- **Service-controlled queues:**

In the case of service-controlled queues, a service is responsible for the further processing of the message. In other words, openUTM provides only the queuing functionality. The communication partner for whom the message is intended must read the message from the queue independently (using the KDCS call DGET). If there is no message in the queue, a service can also wait for the arrival of a message.

Unix, Linux and Windows systems

In UTM cluster applications message queuing is only supported locally in the node. This means that asynchronous messages can only run and be read, displayed or administered in the node application in which they were created. The one exception is that you can transfer asynchronous jobs from a terminated node application into a running node application using the online import facility.

i For general information about the message queuing concept and how to use it, refer to the openUTM manual “Concepts and Functions”.

2.4.1 Dead Letter Queue

The **dead letter queue** is a TAC queue with the fixed name KDCDLETQ. It is always available to save queued messages sent to transaction codes, TAC queues, LPAPs or OSI-LPAPs but which could not be processed. During generation, the saving of queued messages in the dead letter queue can be activated or deactivated for each message destination individually using the TAC, LPAP or OSI-LPAP statement's DEAD-LETTER-Q parameter.

To be able to process the messages in the dead letter queue, for example after eliminating an error, you must either reassign them to their original destination or assign them to a new destination. You can use DADM MV to move an individual message and DADM MA to move all the messages in the dead letter queue to a specified or to the original queues. Please note that messages can only be moved to a destination of the same type as the original destination (TAC TAC, LPAP LPAP, OSI-LPAP OSI-LPAP).

The K134 message makes it possible to monitor the message volume arriving in the dead letter queue (see openUTM manual "Generating Applications", DEAD-LETTER-Q-ALARM operand in the MAX statement).

Preventing a page pool bottleneck

Since the dead letter queue is stored in the page pool, the page pool should be generated with enough space to save messages in the dead letter queue.

The following actions are available to prevent or remove a bottleneck in the page pool:

- Moving messages from the dead letter queue (DADM MV/MA).
- Deleting messages from the dead letter queue (DADM DL/DA).
- Generating QLEV to limit the maximum number of messages in the dead letter queue.
- Temporarily locking the dead letter queue (STATUS = OFF).
- Temporarily deactivating the saving of messages in the dead letter queue for individual destinations, e.g. using WinAdmin, WebAdmin or programmed administration.

2.4.2 Messages to UTM-controlled queues

In the case of UTM-controlled queues, openUTM monitors the subsequent processing of messages written by a program unit to UTM-controlled queues. In other words, when a message is sent to a UTM-controlled queue, it is specified how the message is to be processed subsequently. The jobs associated with this message are therefore classified according to the recipient:

- output jobs
- background jobs

in the case of background jobs we distinguish between:

- **local** background jobs
i.e. background jobs, which request services from their own application.
- background jobs which request **remote** services
There is more information on this in the section [“UTM-controlled queues in distributed processing”](#).

2.4.2.1 Output jobs

Output jobs are asynchronous jobs which output a message, for example a document, to a printer or a terminal. However, the output target may also be another application connected via a transport system interface.

Output jobs consist of the target specification together with the asynchronous message to be output.

Output jobs are initiated by corresponding MQ calls from a program unit of the UTM application.

2.4.2.2 Background jobs

Background jobs are asynchronous jobs which are addressed to an asynchronous service of its own or a remote application. Background jobs are particularly suitable for time consuming or non-time critical processing, in which the result has no direct effect on the current dialog.

Background jobs consist of the transaction code (TAC) of the program unit used to start the background job (service TAC) and possibly a message for the program unit. The type of transaction code determines whether the job is to be processed as an asynchronous job or as a dialog message.

Background jobs can be created as follows:

- by an input from a terminal
- by an MQ call from a service of the UTM application
- by a message from another application that communicates with the UTM application via the LU6.1, LU6.2 or OSI TP protocol
- by an input from another application connected via the transport system interface
- by a UTM message when the message is assigned the message destination MSGTAC (i.e. event-driven, see "[Asynchronous service MSGTAC](#)") or is assigned the TAC of an asynchronous service as the user-specific message destination

Background jobs can be restarted after abnormal termination of a service (redelivery), see "[Redelivery with background jobs](#)" or sent to the dead letter queue.

2.4.2.3 MQ calls of the KDCS interface

openUTM provides calls for UTM-controlled queues that are powerful in terms of the functions they offer but nevertheless easy to program. The "free" element in the call names reflects that message queuing is a type of communication which is disconnected from the sender and which is not dependent on the availability of the receiver.

- **FPUT (Free message PUT)**
You use FPUT calls to send asynchronous messages. The target may be an output device (output job), an asynchronous service (background job) or an application (see "[UTM-controlled queues in distributed processing](#)").
An asynchronous message may also consist of multiple message segments. In this case you have to use a separate FPUT call for each message segment.
- **DPUT (Delayed free message PUT)**
The DPUT call can also be used to send an asynchronous message or a message segment to an output device, an asynchronous service or another application (see "[UTM-controlled queues in distributed processing](#)").
However, compared to the FPUT call, the DPUT call also allows you to use time control and confirmation jobs.
- **FGET (Free message GET)**
You use the FGET call to read asynchronous message or message segments within an asynchronous service.
- **MCOM (Message COMplex)**
You use the MCOM call to assign confirmation jobs to asynchronous jobs.
- **DADM (Delayed free message ADMInistration)**
You can use the DADM call to request summary information about the entire contents of a queue or information about its individual elements. Additionally you can also control the processing sequence with DADM: you can advance jobs, cancel individual jobs or delete the entire queue.

For the precise format and further information about these calls refer to the chapter "[KDCS calls](#)".

2.4.2.4 Structure of an asynchronous service

An asynchronous service starts with an asynchronous program unit. The program unit is assigned a transaction code TYPE=A (asynchronous) at generation. An asynchronous program unit does not only differ from a dialog program unit in its transaction code type, it is also differently structured.

Structure of an asynchronous program unit

Asynchronous programs do not have to read an input message or create an output message. In the first program unit of the first processing step you can issue an FGET call following an INIT. This call makes it possible to read the asynchronous message of the creator of the background. This may be:

- a complete message
- a message segment or
- an empty message in cases where the job consists of one TAC only (e.g. created via a function key at the terminal).

These may be followed by any number of KDCS calls, with the exception of MGET. However, you can use an MGET call in a follow-up program or follow-up processing step.

You cannot use MPUT to send a response to the communication partner from which you received the asynchronous message. Since the service runs disconnected from the partner, the partner may no longer be connected to the application at the time of processing. However, you can send a message to the partner with FPUT or DPUT. This message will be inserted in the message queue assigned to the partner. An MPUT call is only permitted if the message is addressed to a follow-up program or a job receiver service.

The last UTM call in your program unit must be PEND, as described in section "[Program framework](#)". An asynchronous program is normally terminated with a PEND FI call. This also terminates the service. openUTM transfers any unsent messages to the partner or partners.

Other PEND variants are possible, such as PEND PA/PR/SP for program unit chaining, and PEND KP and RE for distributed processing. You can also use the PGWT KP, CM and RP calls in an asynchronous program unit (e.g. PGWT KP) if you want to terminate the processing step without terminating the program unit or the transaction in distributed processing.

An asynchronous service may be split into multiple program unit runs, and also into multiple processing steps in the case of distributed processing (see "[Asynchronous service with multiple program units](#)" or "[Asynchronous services which also issue jobs](#)").

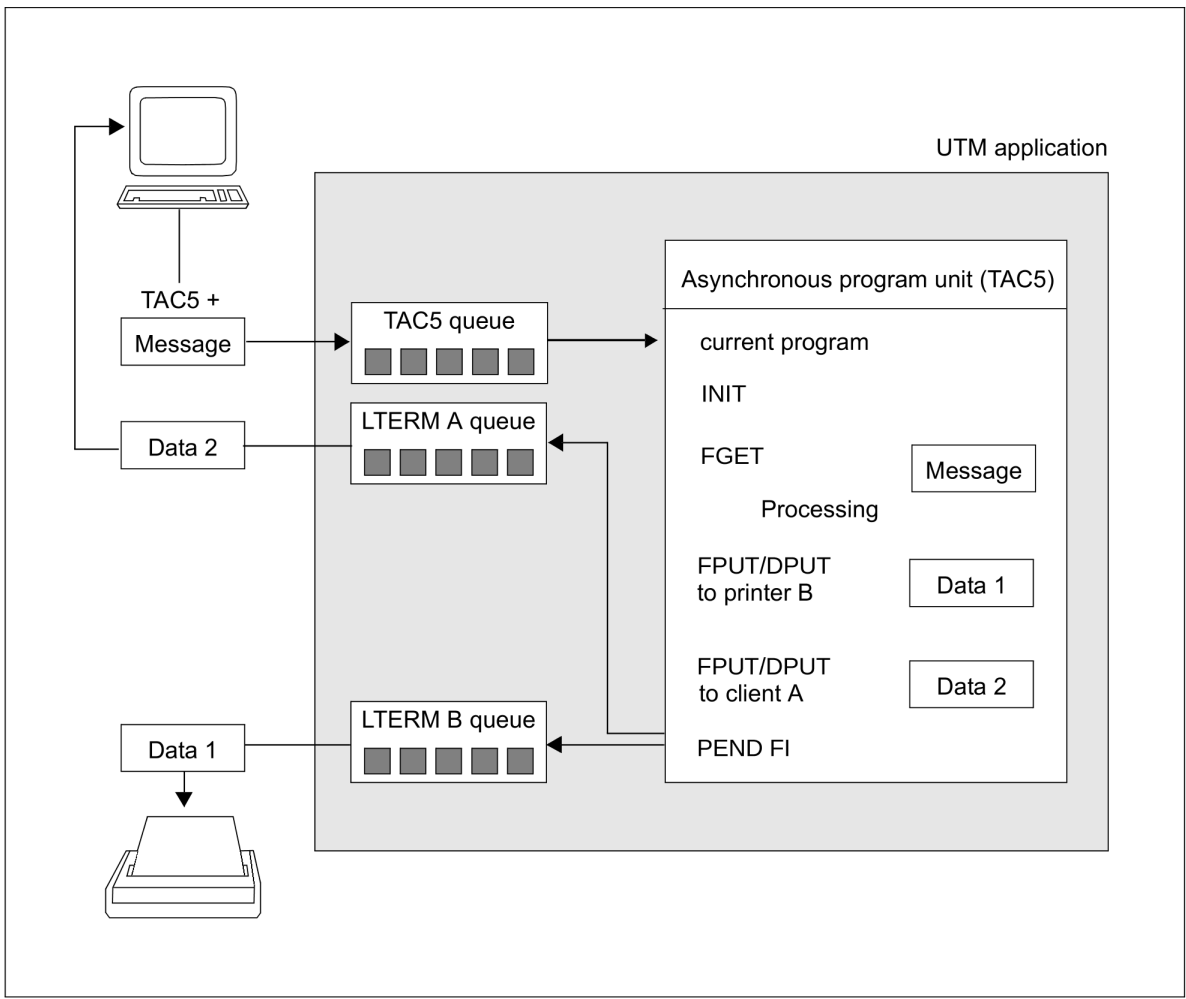


Figure: Structure of an asynchronous program unit

Combined dialog and asynchronous program

You can assign multiple transaction codes to a program unit. It is also possible to assign a dialog TAC and an asynchronous TAC to the same program unit. This means that you can start the program in dialog mode or asynchronously. openUTM indicates the way the program unit was started in the KCPRIND field of the KB header: "A" for asynchronous, "D" for dialog. The program unit can evaluate this field and branches accordingly.

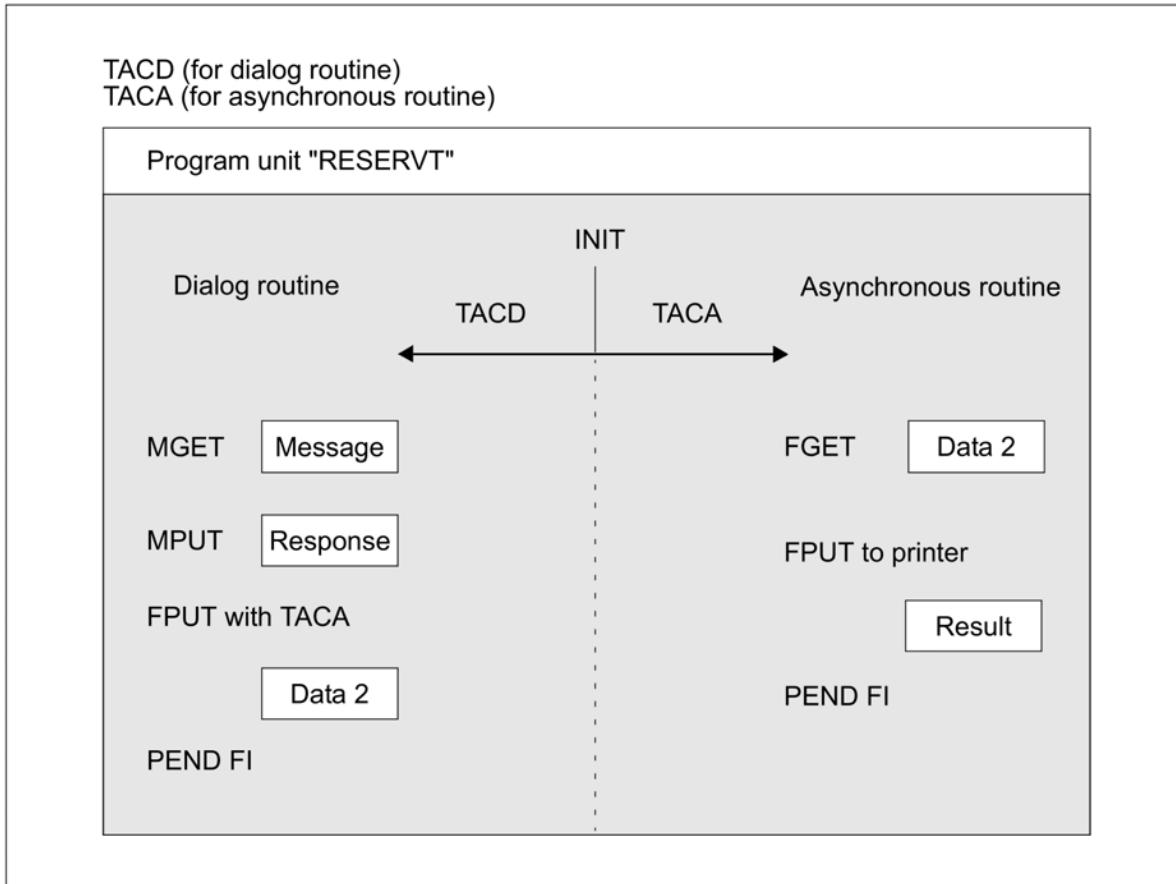


Figure: Dialog and asynchronous processing in a program

If the program in the diagram is started with TACD, FPUT is executed after PEND. This means that the same program unit is called again to process an independent second service. The processing of an asynchronous service outside the dialog program may lead to better response times in the dialog with the client.

Asynchronous service with multiple program units

An asynchronous service may be structured into multiple program units and transactions. The last program unit is terminated with PENDING FI. In the preceding program units the PENDING variants SP or PA/PA are possible.

PENDING variants such as PENDING KP or PENDING RE which terminate a processing step are only possible within an asynchronous service if distributed processing is used (see diagram on next page).

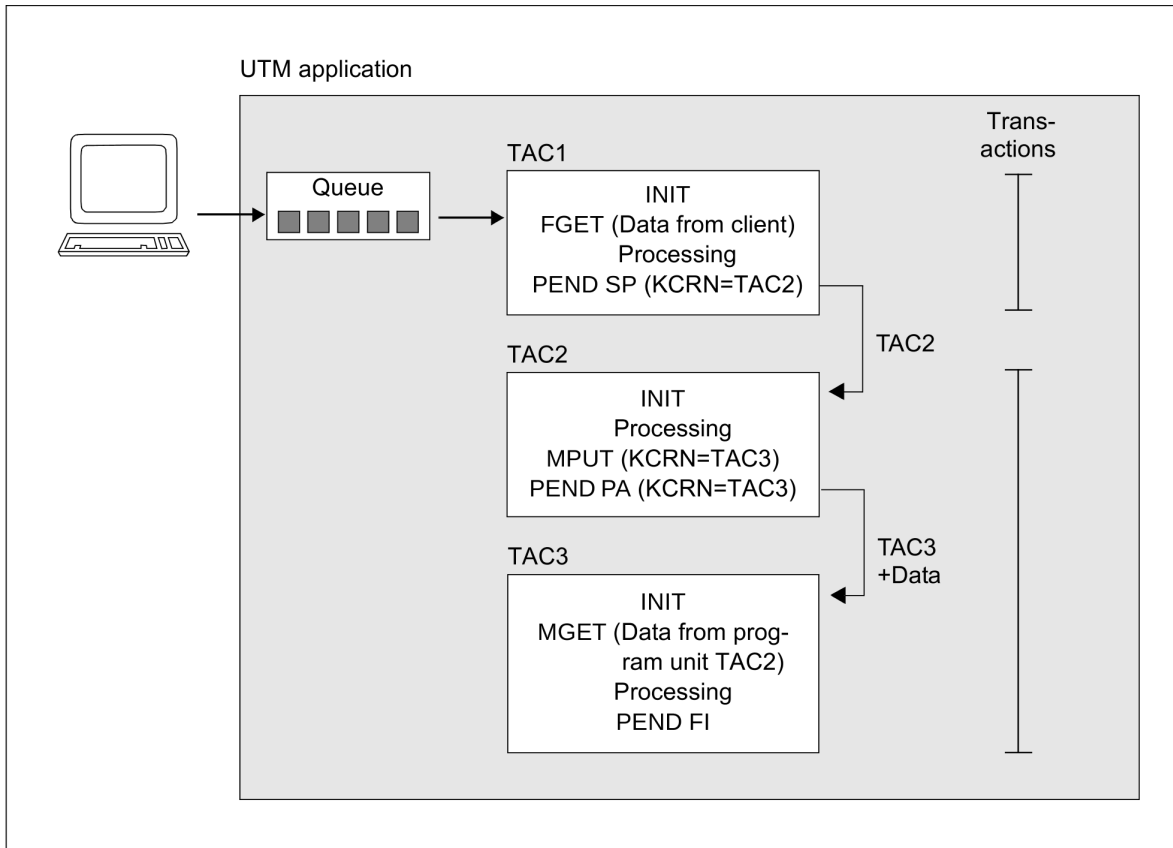


Figure: Structure of an asynchronous service split into three program units

In the depicted example a background job is issued to an asynchronous job of the same application from a terminal. To do this, you have to enter the transaction code of this service and, if necessary, a message at the terminal. openUTM automatically places the job in the relevant queue and starts the asynchronous service disconnected from the job submitter as soon as the necessary resources are available. The first program unit reads the data with FGET and terminates with PENDING SP. A synchronization point is set and the follow-up program specified in KCRN is started.

The TAC1 program has not transferred an MPUT to the TAC2 program. However information can be forwarded in the service-specific storage areas. The TAC2 program selects an MPUT call for the transfer of information to TAC3 and terminates with PENDING PA. This means that no synchronization point is set. In the TAC3 program the service is terminated with PENDING FI.

Asynchronous services which also issue jobs

An asynchronous service may in its turn create asynchronous jobs. These may be output jobs or further background jobs. In distributed processing, you can also issue dialog jobs to partner applications from an asynchronous service, i.e. the asynchronous service communicates with remote dialog services.

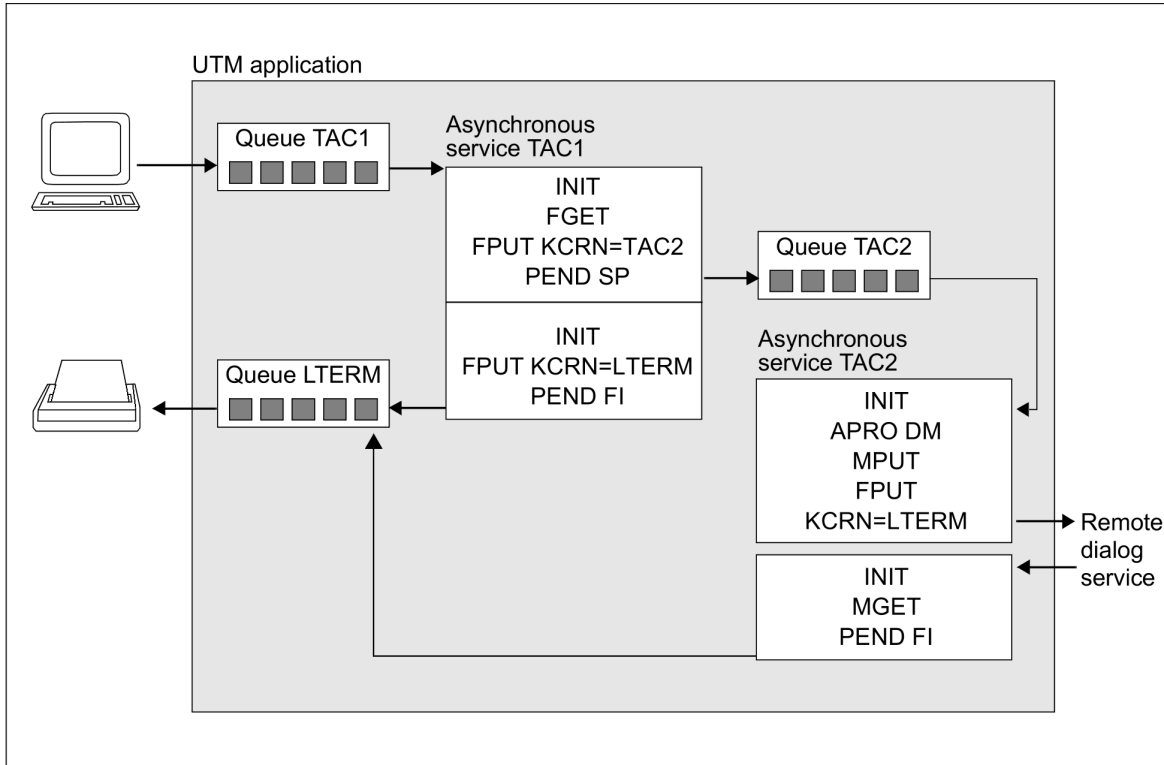


Figure: Asynchronous services which also issue jobs

In the first program unit of the TAC 1 asynchronous service, a job is issued to the TAC2 asynchronous service. To do this, you have to specify the TAC2 transaction code in the KCRN field when you call FPUT. Since the program unit terminates at a synchronization point, the job is already inserted in the relevant queue at the end of the program unit.

An asynchronous job is also issued in the TAC2 service of the first program unit. This is an output job to the printer. You have to specify the LTERM name of the printer in the KCRN field when you call FPUT. Since this program unit does not terminate at a synchronization point the job is inserted into the LTERM queue at the end of the service (next synchronization point).

The TAC 2 service is divided into two processing steps. The first program unit uses MPUT to send a message to a remote dialog service. The second program unit is started when the response is received from the remote service. This is read using MGET.

Job complexes

Together with the asynchronous job ("basic job") you can describe up to two more **confirmation jobs** which are associated with the positive or negative result of job processing. These confirmation jobs are processed after the basic job is processed. The job submitter can use the confirmation jobs to react to a positive or negative job result. A confirmation job which is not used, e.g. a negative confirmation job for a positive result, is deleted. The entity formed by a basic job and its associated confirmation jobs is called a **job complex**.

The following table shows some of the possible events which may occur during asynchronous processing and the effects of these events on the confirmation jobs.

The beginning and the end of a job complex are defined by means of separate KDCS calls, the **MCOM BC** (begin of complex) call and the **MCOM EC** (end of complex) call. With the MCOM BC call you define the complex identifier (complex ID), the destination of the asynchronous job and the TACs of the asynchronous programs which are to process the positive or negative confirmation. All the jobs generated within the complex are described using DPUT calls. You must specify the complex ID as the target.

A job complex can be defined both in dialog and in asynchronous programs.

If the basic job of an job complex is addressed to a remote asynchronous service, then the service identifier must be assigned (via APRO AM) before the beginning of the job complex. With MCOM BC you define the service ID in KCRN; the confirmation jobs have to be processed by the local application.

Event	Effect on confirmation job
PEND FI in the local asynchronous service	Start of positive confirmation job and deletion of negative confirmation job
For background job, successful transfer to asynchronous service	
Positive print confirmation from printer or print administration	
Processing a message of a TAC queue and termination of the transaction	
PEND ER/FR in local asynchronous service without redelivery	Start of negative confirmation job and deletion of positive confirmation job
Error while preparing the output message by VTSU-B on BS2000 systems	
Error while formatting the output message on BS2000 systems	
Processing a message of a TAC queue and rollback of the transaction without redelivery	
For background job to asynchronous service, rejection of the job	
Deletion of a job by administration	
Delete the output job when establishing or clearing down the connection of a RESTART=NO client.	
PEND ER/FR in the local asynchronous service with redelivery	Without effect, since basic job is still present
Negative print confirmation from printer or timeout waiting for a confirmation	
Sequence of jobs changed by administration	
Repetition of a print job	
Processing a message of a TAC queue and rollback of the transaction with redelivery	

Event	Effect on confirmation job
Deletion of a job with confirmation jobs by print administration	Confirmation jobs are deleted; logged in SYSLOG
KDCUPD does not accept a job	Confirmation jobs are also not accepted (see KDCUPD log)

The following diagram illustrates a job complex, taking a print job as an example.

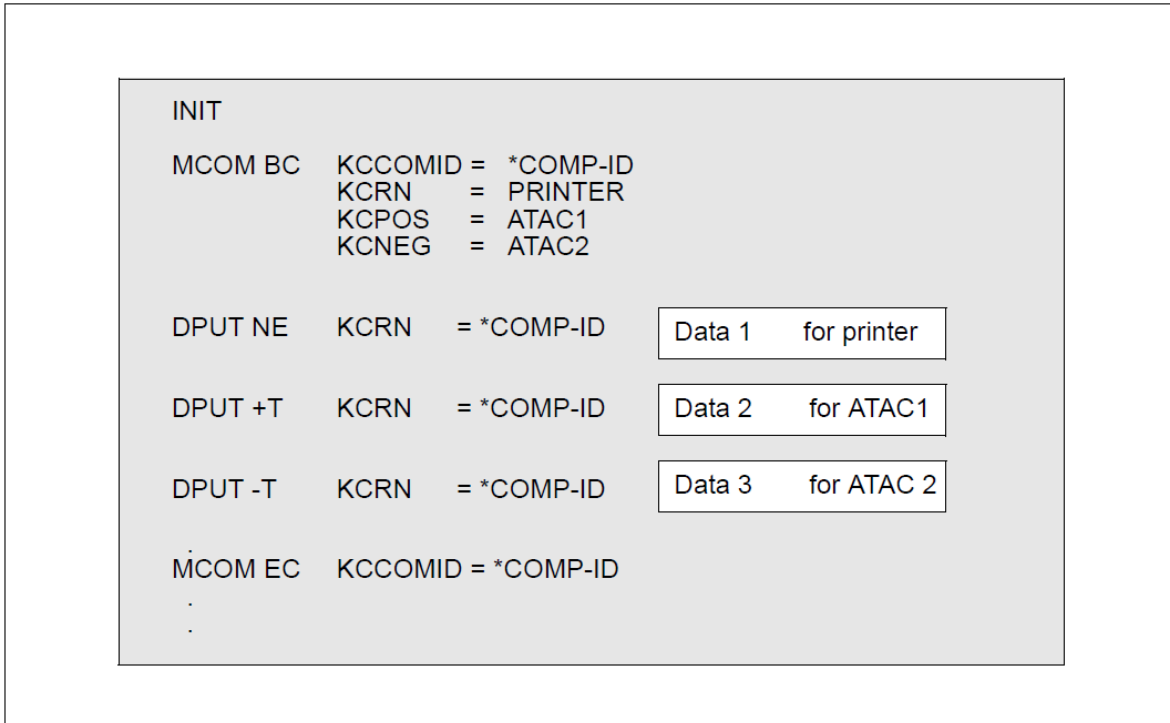


Figure: Job complex for a print job

2.4.2.5 Redelivery with background jobs

If an asynchronous service is terminated abnormally by PENDING/FR or by a system PENDING before a transaction was completed with Commit, the service is restarted and the FGET message is redelivered, providing this functionality has been activated at generation.

Whether redelivery is possible and how often redelivery is attempted can be defined at generation (REDELIVERY operand in the MAX statement). When the FGET call is executed, the number of redeliveries is output in the KB return area.

2.4.3 Messages to service-controlled queues

In the case of service-controlled queues, the subsequent processing of messages sent by a program unit to a service-controlled queue is dealt with by the services of the application. openUTM merely ensures that the messages in the queues are saved. The application programs must themselves read the messages saved in these queues; if there are no messages in a queue, an application program unit can also wait for a message to arrive in a queue.

openUTM distinguishes between USER queues, TAC queues and temporary queues. The properties of these queues are described in sections “[USER queues](#)” to “[Temporary queues](#)”. The associated MQ calls are listed in section “[MQ calls of the KDCS interface](#)”. For more information on the lifetime of queues and messages in queues, refer to section “[Lifetime of queues and queue messages](#)”.

Service-controlled queues offer new communication opportunities in a large number of cases; it is possible, for example, to use message queues to implement the following scenarios:

- communication between independent services in an application
- “pseudo dialogs” with remote transport system applications
- parallel processing of database accesses in (read) transactions
- sending of messages to UTM users (mailbox functionality)
- sending of asynchronous messages to UPIC clients
- sending of messages to queues in other applications (remote queues: see section “[Service-controlled queues in distributed processing](#)”)
- outputting of UTM messages at the UTM administration workstation WinAdmin or WebAdmin
- implementation of user-controlled processing of asynchronous messages
- serialization of program units (running in the dialog and asynchronously)
- output of the data of other TLS blocks to the data station in the dialog
- as global storage areas of unlimited size

The queues can be administered with the DADM call.

2.4.3.1 USER queues

USER queues are permanent, service-controlled message queues. A USER queue is available to every generated UTM user at all times. USER queues can be accessed by any service by means of a program call, provided it knows the name of the user.

By means of this queue, messages can be sent to the user at the terminal, for example, or to a user signed on via a UPIC client. The USER queue is used as a mailbox in this case. The queue can also be used for communication between the dialog service of the user and asynchronous services that run under the same user ID.

In this way, you can, for example, distribute multiprocessor-capable, parallel database information across a number of asynchronous services and “collect” the results in the dialog service.

At generation, read and write protection can be assigned for the USER queue in the KDCDEF statement USER (Q-READ-ACL and Q-WRITE-ACL parameters). You will find more information on the generation of data access control in the openUTM manual “Generating Applications” under the KDCDEF statement USER. Regardless of the data access control in existence, a user can always read messages from and send messages to his or her own user queue.

Time-controlled messages cannot be sent to USER queues.

By means of the KDCS call INIT PU, a program unit can query how many messages there are for the user ID under which it is running.

2.4.3.2 TAC queues

TAC queues are permanent, service-controlled message queues. Each TAC queue has a fixed name that is generated with the KDCDEF statement TAC ... TYPE=Q. TAC queues can be accessed by any service by means of a program call, provided it knows the name of the queue.

Remote message queues, for example, can be implemented with the help of TAC queues. These remote queues are addressed in the local application by means of the LTAC name (see also "[Service-controlled queues in distributed processing](#)").

TAC queues can also be used in job complexes. Both the basic job and the confirmation jobs can be directed at TAC queues.

Messages can also be sent to TAC queues with time control.

At generation, read and write protection can be assigned for the TAC queue in the KDCDEF statement (READ-ACL and WRITE-ACL parameters). By means of dynamic administration (STATUS attribute), TAC queues can be locked completely for read and/or write access.

For more information on the generation of TAC queues, refer to the section on the KDCDEF statement TAC in the openUTM manual "Generating Applications".

2.4.3.3 Temporary queues

Temporary queues can be created dynamically in the program unit run by means of the KDCS call QCRE and deleted by means of the QREL call. No administration authorization is necessary for these calls.

Temporary queues are particularly suitable for communication between services: a service creates a temporary queue and passes the name of this queue with the asynchronous services it creates. The service subsequently reads the messages that these asynchronous services send to the temporary queue or waits for these messages. The temporary queue is then deleted again. When a new temporary queue is created, messages can be written to this queue in the same transaction. However, these messages cannot be read and administered until after the transaction is successfully completed.

The name of the temporary queue can either be freely selected or created automatically by openUTM. The advantage of having names created automatically by openUTM is that the names assigned are always new. Only after 100 million calls is the same name assigned again.

A temporary queue can be deleted at any time by means of the QREL call. On the successful completion of the transaction, all the messages in the queue are deleted and the name and table space of the queue are released. All services waiting for messages of the deleted queue are continued.

Time-controlled messages cannot be sent to temporary queues.

The maximum number of temporary queues that can be created is specified at the generation of the application (QUEUE statement, NUMBER operand: see also the openUTM manual "Generating Applications"). In the QUEUE statement it is also possible to limit the number of messages stored in the queue using the QLEV (queue level) operand; this allows you to limit the utilization of the page pool. However, you can also specify the queue level dynamically in the QCRE call. If you do this, anything specified at generation is overwritten.

A program unit can obtain the names of all the temporary queues and their properties by means of the KDCADMI call KC_GET_OBJECT (object type: KC_QUEUE).

2.4.3.4 MQ calls of the KDCS interface

The KDCS interface provides the following calls for service-controlled queues:

- **DGET (Delayed free message GET)**
The DGET call is used to read messages or message segments from USER, TAC or temporary queues and to wait for a message of a service-controlled queue. Read with subsequent deletion ("processing") and read without deletion ("browse") are possible.
- **FPUT (Free message PUT)**
FPUT calls are used to send messages to TAC queues. A message can consist of several message segments. A separate FPUT call is required for each message segment.
- **DPUT (Delayed free message PUT)**
The DPUT call sends a message or message segment to a USER, TAC or temporary queue. Time control and basic and confirmation jobs are only possible for TAC queues.
- **QCRE (Queue CREate)**
The QCRE call is used to create a temporary queue.
- **QREL ((Queue RELease)**
The QREL call is used to delete a temporary queue.
- **DADM (Delayed free message ADMInistration)**
You can use DADM to obtain an overview of the entire contents of a queue or of specific elements in it. In addition, DADM also allows you to control the order in which messages are processed: you can bring messages forward or delete individual messages or the contents of the entire queue.

You will find the exact format of these calls and further information on them in chapter ["KDCS calls"](#).

2.4.3.5 Lifetime of queues and queue messages

In UTM-S, all queues and all messages in these queues are preserved after the end of the application. In other words, the messages in the queues are stored safely (failsafe) and are still available after a restart. In the event of regeneration, the messages can be transferred using the KDCUPD utility.

In UTM-F, the USER and TAC queues are preserved after the end of the application, but the temporary queues are lost. The messages stored in all three types of queue are lost.

Redelivery of queue messages

If queue messages were processed and if the transaction is then rolled back, the messages are placed back in the queue. They can be read with DGET. The maximum number of redeliveries can be set at generation (REDELIVERY operand in the MAX statement). Redelivery can also be deactivated using this operand.

When the DGET call is executed, the number of redeliveries is output in the KB return area.

Alternatively, such messages can also be saved in the dead letter queue.

2.4.3.6 Deleting USER and TAC queues by means of programmed administration

USER and TAC queues can be deleted by means of programmed administration.

A USER queue is deleted when the associated user ID is deleted. The deletion can take effect either immediately or at the next generation. However, the immediate deletion of USER queues is only possible for standalone applications.

The dead letter queue cannot be deleted.

The deletion of TAC queues does not take effect until the next generation.

2.4.3.7 Examples

The following sections describe typical application examples and show how you can use service-controlled queues and create the associated program units.

Example 1: Communication between two services in an application

The diagram shows the evaluation of a background job with the help of a temporary queue. The main service "Customer" in a call center searches for the required data by means of a background job and reads the results from a temporary queue or waits for the corresponding message if it is not yet available at the time of the DGET.

UTM application "Call Center"

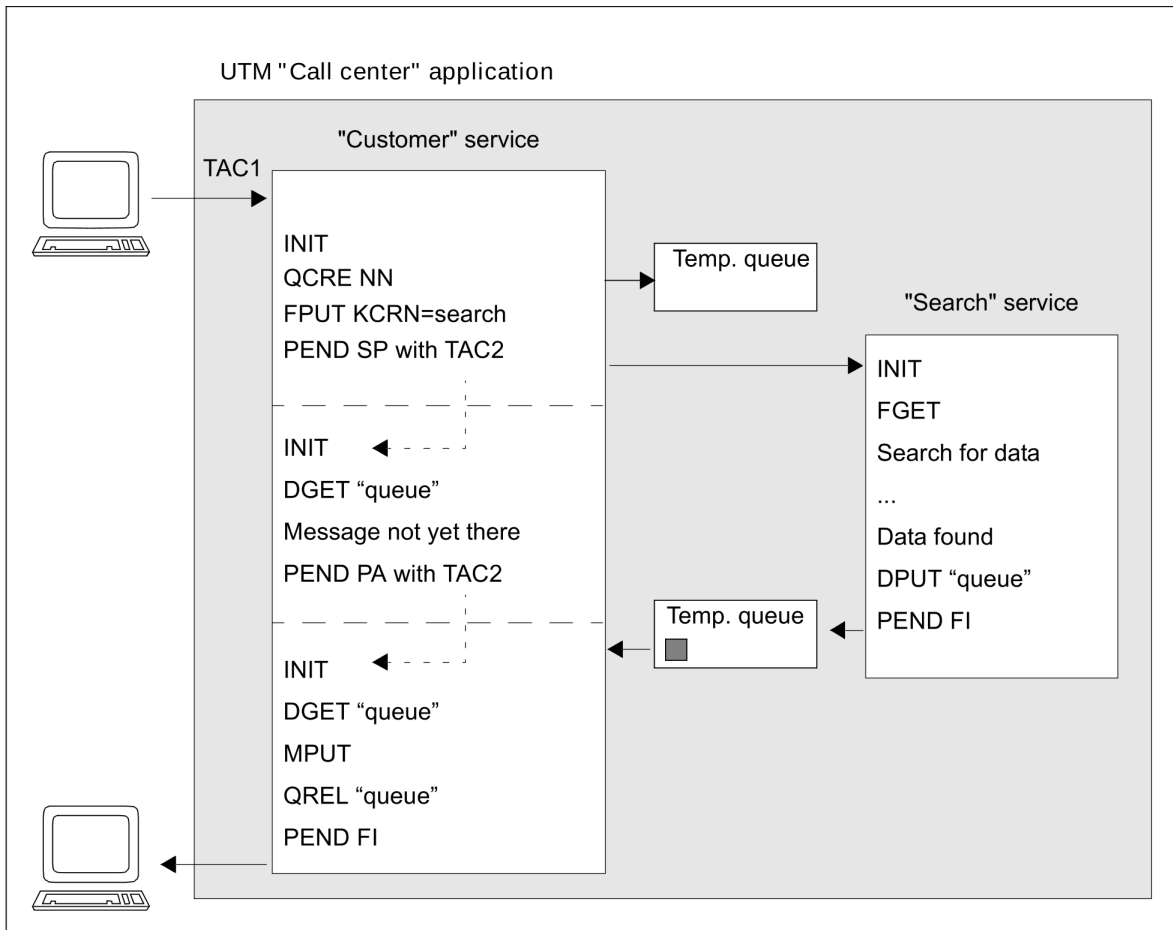


Figure: Communication between two independent services with the help of a temporary queue

A temporary queue is created by means of QCRE NN. The name of the queue is returned in KCRQN. The background job "Search" is then created with FPUT, and the transaction is terminated immediately with PEND SP. The name of the queue is passed with FPUT.

The "Search" service reads the message with the name of the temporary queue and searches for the required data. Meanwhile, the main service, "Customer", queries the result of background processing with DGET. Since the result is not yet available in this case, the current program unit of the main service terminates; openUTM waits for the arrival of the message. The function is implemented in such a way that there is no program unit active and no process linked for the main service in the wait time.

When the “Search” auxiliary service has obtained the required data, it creates a message for the temporary queue and terminates. The DPUT job is thus executed.

The main service is continued when the message arrives. It reads the result from the temporary queue and sends it to the client. It then deletes the temporary queue and terminates (the deletion does not take effect until the successful completion of the transaction).

To control the sequences executed in the program units, an auxiliary field called `WaitForMsg` must be created in the KB communication area so that it can be accessed by all the service’s program units. If the return code 08Z is obtained repeatedly, superfluous waiting is avoided by means of a RSET call.

Program unit TAC1

```
...
QCRE NN
FPUT with KCRN=search
kb.WaitForMsg = 0
PEND SP with TAC2
```

Program unit TAC2 for evaluating the result

```
...
DGET queue
if ( KCRCCC = "08Z" )
then if kb.WaitForMsg = 0
    then kb.WaitForMsg = 1
        PEND PA,<tac2>
    else RSET
else processing
QREL queue
...
PEND FI
```

Example 2: “Pseudo dialogs” with remote transport system applications

Another application example is obtained by carrying out a simple modification of example 1: a dialog or asynchronous service wants read access to a database in another application.

A communication partner of the type APPLI or SOCKET-USP replaces the auxiliary service of example 1. The FPUT call in the main service addresses the LTERM name of the remote application instead of an asynchronous TAC; apart from this change, the calls and processes involved in the two services remain unchanged. If the remote application is a UTM application, the TAC to be called in the remote application must be at the beginning of the FPUT message. The remote application must begin its reply message with the name of the queue in which the main service expects the reply.

openUTM determines the destination of the messages from the name of the queue alone. The name of the temporary queue must therefore not be the same as a TAC or LTERM name of the local application. Name clashes are avoided because the name of the temporary queue is assigned by openUTM (QCRE NN), and neither TAC nor LTERM names begin with a digit.

Example 3: Communication with more than one service

If a service wants to communicate with more than one auxiliary service simultaneously, what happens is similar to what happens in communication with only one auxiliary service. When the replies are read, however, it is important that all the replies are read; it may therefore be necessary to wait for all of these. You must ensure that each message is waited for no more than once.

To control the processes in the program units, auxiliary fields are created in the KB communication area in this example so that all the program units of the service can access them. As it is possible that not all the replies can be read in a program unit run, the browse function is used to implement a wait loop. The replies are not processed until the last message has arrived.

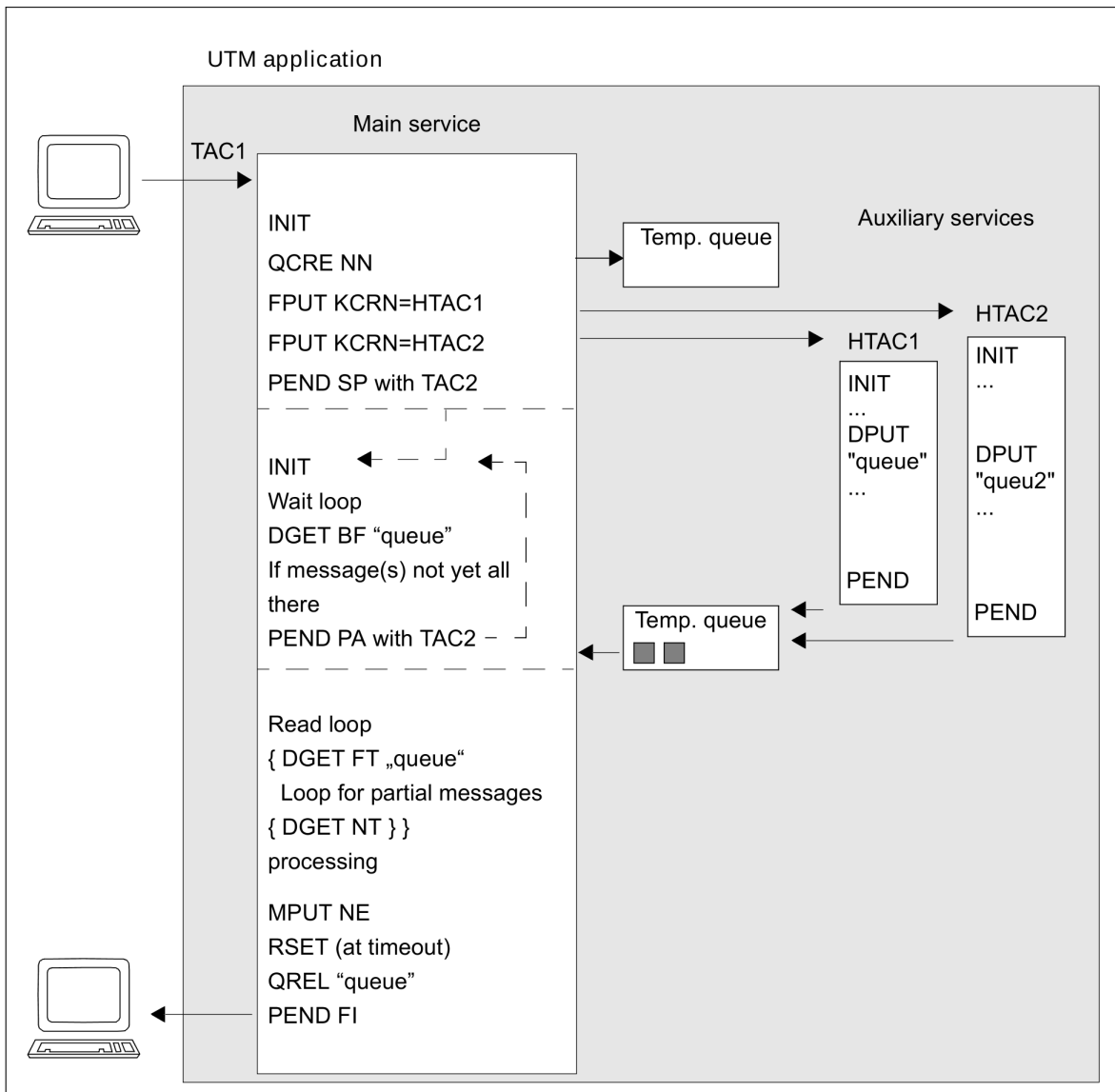


Figure: Communication of a main service with two auxiliary services by means of temporary queues

Auxiliary fields must be used for this communication, and loops must be programmed. The various steps are explained in the following table:

TAC1 program	Explanation
INIT	
QCRE NN	Create temporary queue. The name of the queue is returned in KCRQN.
FPUT KCRN=HTAC1 FPUT KCRN=HTAC2	Create messages for the auxiliary services. The name of the queue is passed in the message.
kb.NrMsgs = 2 kb.WaitForMsg = 0 kb.i = 0 kb.kcgtm = spaces kb.kcdpid = spaces	Initialize fields in the KB program area. These fields control the sequence of execution in the follow-up programs.
PEND SP KCRN=TAC2	Terminate transaction. The asynchronous jobs are started.
TAC2 program	Explanation
INIT	
Timeout = 0	Initialize timeout field.
for(kb.i < kb.NrMsgs AND Timeout = 0) DGET BF with length 0 kb.kcgtm kb.kcdpid	In a loop an attempt is made using DGET BF with waiting to wait for all replies without reading or deleting data; in other words, all messages are retained. Make sure that each message is not waited for more than once.
if (KCRCCC = "08Z") then if kb.WaitForMsg = 1 then Timeout = 1 else kb.WaitForMsg = 1 PEND PA KCRN=TAC2 else kb.i = kb.i +1 kb.WaitForMsg = 0 kb.gtm = KCRGTM kb.kcdpid = KCRDPID	There must be a wait. The program run is then terminated with PEND PA; the current TAC is specified as the follow-up TAC. The counter is incremented when a reply arrives. The creation time and DPUT ID of the message are buffered

TAC1 program	Explanation
<pre> if Timeout = 0 then for (i < kb.NrMsgs) DGET FT for (KCRCCC ! = "10Z") DGET NT processing MPUT NE </pre>	<p>All replies are read in full in two nested loops. Processing of the replies then begins. The result is sent to the client using MPUT.</p>
<pre> else RSET MPUT </pre>	<p>At timeout, superfluous waiting is avoided by means of an RSET.</p>
<pre> QREL "queue" PEND FI </pre>	<p>Before the service terminates, the temporary queue is deleted again.</p>

Example 4: Sending asynchronous messages to UPIC clients

Asynchronous messages must not be directed at a LTERM partner of a UPIC client; with the help of service-controlled queues, however, asynchronous events or messages can also be delivered to a UPIC client. To do this, you either direct the asynchronous messages to the USER queue of the UPIC client or you generate a TAC queue additionally for each UPIC client. The UPIC client starts another dialog service in parallel with its normal dialog services. This dialog service assumes the task of waiting at this queue until a message arrives, reading it out and forwarding it to the UPIC client.

The following diagram shows how this is implemented using USER queues:

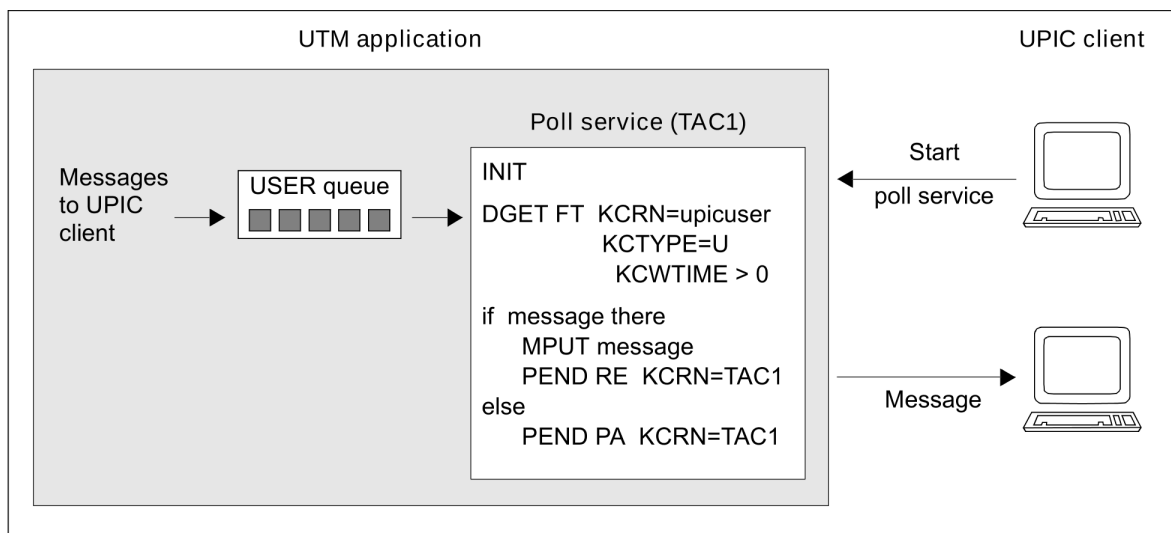


Figure: Sending of asynchronous messages to UPIC clients using USER queues

Example 5: Serialization of program units

If a program (segment) that is executed in both dialog and asynchronous services is to be serialized, you can use a TAC queue for serialization. TAC queues have an advantage over GSSBs (global secondary storage areas) in that waiting takes place outside the program unit context and the process is thus free for other things.

In the following example, a segment of a program unit that can run both in the dialog and asynchronously is secured against parallel processing by means of a TAC queue.

```
Generation
TAC tacqueue,TYPE=Q
```

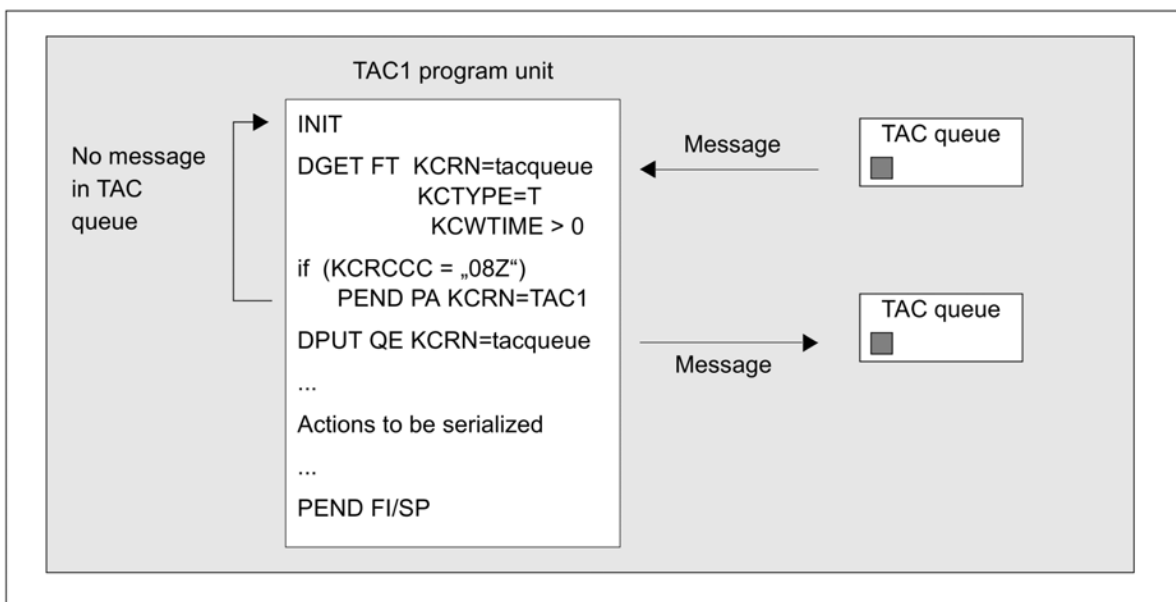


Figure: Serialization of program units using TAC queues

A message is sent to the TAC queue by means of DPUT for the next service to execute the critical program segment. Only on successful completion of the transaction does the DPUT call take effect.

The mechanism described here must be initialized so that the critical program unit segment can be executed. This can be implemented at application startup, for example, by means of an MSGTAC program that responds to a start message (K050, K051) and creates a message for the TAC queue.

Example 6: Output of other TLS blocks in the dialog service

Accesses to TLS blocks of a different data station are only permitted in asynchronous services. The output of data from other TLS blocks from a dialog service to the data station is possible if example 1 is slightly modified:

The dialog service passes to the auxiliary service the name of the TLS block and of the LTERM. The auxiliary service reads the required data with a GTDA call and sends it to the temporary queue.

The dialog service reads the TLS data from the temporary queue and outputs it at the data station.

Example 7: Service-controlled queues as global storage areas

Only serial access to application-global storage areas (GSSBs, see "[Global secondary storage area \(GSSB\)](#)") is possible, i.e. areas of this kind are locked during read/write. If, instead of a GSSB, a temporary queue is used with the "browse" function, several services can then access the storage area in parallel.

Also, fewer restrictions apply to temporary queues than to GSSBs. The storage area of a temporary queue is not limited (GSSB: 32,767 bytes) and more queues than GSSBs are permitted (500,000 as opposed to 32,767).

Using a temporary queue it is possible, for example, to implement an **online auction**:

- DPUT QT/QE puts the descriptions of the objects into a temporary queue one after the other. A fixed name is given to the queue. Later additions can be made to the queue.
- DGET BF/BN allows those interested to read these descriptions; this can also be done in parallel by several services.
- DGET PF/PN processes a description and therefore removes it from the queue, e.g. once an object has been sold in the auction.
- The temporary queue is deleted with QREL at the end of the auction.

The number of messages in a temporary queue can be limited at generation time (KDCDEF QUEUE statement, QLEV operand). If only the latest messages are of interest, wrap mode can be selected (QUEUE statement, QMODE=WRAP-AROUND operand). Once the maximum number of messages has been reached, each new message causes the oldest message to be deleted.

2.5 KDCS storage areas in openUTM

Under openUTM, program units can use various storage areas for the reading and writing of user data. These storage areas ensure a clear distinction possible between program and data areas and ensure that programs are reentrant. Additionally, these areas also enable the transaction-logged, high-performance exchange of information between programs and guarantee the efficient usage of working memory. Some memory areas are specially designed for statistical purposes and for logging.

In addition to the storage areas shown here, openUTM also offers you the chance to use service-controlled queues for communication between program units (see section “[Messages to service-controlled queues](#)”).

The following storage areas are available:

- standard primary working area (SPAB)
- communication area (KB)
- local secondary storage area (LSSB)
- global secondary storage area (GSSB)
- terminal-specific long-term storage (TLS)
- user-specific long-term storage (ULS)
- user log file (for writing only)
- areas (AREA)

The number of GSSBs, LSSBs, TLS blocks and ULS blocks available in a UTM application is specified during generation; names are also assigned for the TLS and ULS blocks at this time; the names of the GSSBs and LSSBs are specified when programming the application.

Storage location for user data

In the case of standalone applications, the user data in the KB, GSSBs, LSSBs, TLS and ULS blocks is stored in the KDCFILE.

Unix, Linux and Windows systems

In a UTM cluster application, each node application possesses a separate KDCFILE. The fact that some data is valid at local node level whereas other data is valid globally throughout the cluster results in a number of peculiarities compared to standalone applications:

- Data that is local to the node is stored only in the KDCFILE file of the relevant node application. Data that is local to the node includes, for example, TLS, asynchronous messages, background jobs and data relating to other node-bound services. The KDCFILES of the individual node applications are not identical at runtime.
- Data that applies globally in the cluster is stored in UTM cluster files such as the cluster page pool or the cluster user file, see the openUTM manual “[Concepts and Functions](#)”. This includes user data such as GSSB, ULS, the service data of users and passwords.

Storage concept

The storage concept supports the following functions:

- reentrant capability of program units (SPAB)
- application data can be accessed by two or more services running in parallel (GSSB, TLS, AREA)
- protection of user-specific data against access by foreign login names (ULS)
- transaction-oriented storage of logging data (user log file)
- independence of program units running in parallel (KB, LSSB).

openUTM provides two types of storage area:

- working memory areas (KB, SPAB)
These are storage areas which are available for the program units in the working memory. You can address them directly.
- secondary storage areas (GSSB, LSSB, TLS, ULS, log files)
openUTM sets up these storage areas in background storage areas and uses special KDCS calls to write to and read from them.

Depending on their function these areas are assigned to:

- a program unit (SPAB)
- a service (KB and LSSB)
- an LTERM, LPAP or OSI-LPAP partner (TLS)
- a user ID (USER), Session (LSES) or Association (OSI-LPAP ASSOCIATION NAMES)
- the application (log file, AREAs, GSSB).

If a service is processed in two or more processing steps or in two or more program units, the data has to be stored and passed on. For this you use:

- the communication area (KB) and the
- local secondary storage area (LSSB).

You should use the KB for data required in each processing step.

LSSBs are to be used either when the data is not required in each program unit run of a service or when there is more than 32 Kbytes of data, which means that it will not fit in the KB.

Function and lifetime of the storage areas

The following table provides a summary of the lifetimes and functions of the KDCS storage areas. The diagram on the next page also shows the KDCS calls you can use for storage processing and illustrates the assignment of the individual storage areas.

Abbreviation	Area type	Lifetime	Function
KB	Communication area	Start of service to end of service	Accesses current information provided by openUTM; exchanges data between program units of a service
SPAB	Standard primary working area	Start of program unit to end of program unit	Transfers parameters for KDCS calls; message buffers
AREA	Additional storage area, declared for each generation	Duration of application	Accepts global data of an application; preferably used for read access only. <i>Unix, Linux and Windows systems</i> You should note that AREAs in a UTM cluster are always node-specific, i.e. one node cannot access the AREAs in another node.
LSSB	Local secondary storage area	From first write call to explicit release or deletion of user ID	Exchanges data between the program units of a service
GSSB	Global secondary storage area	From first write call to explicit release or end of service	Exchanges data across services
ULS	User-specific long-term storage	Generation until generation modification	E.g. statistics which are specific to particular users (USER), LU6.1 Sessions (LSES) or OSI-TP Associations (OSI-LPAP ASSOCIATION-NAMES)
TLS	Terminal-specific long-term storage	Generation until generation modification	Statistics which are specific to particular connection points (LTERMs, LPAPs, OSI LPAPs)
USLOG	User log file	Individually defined	Logging

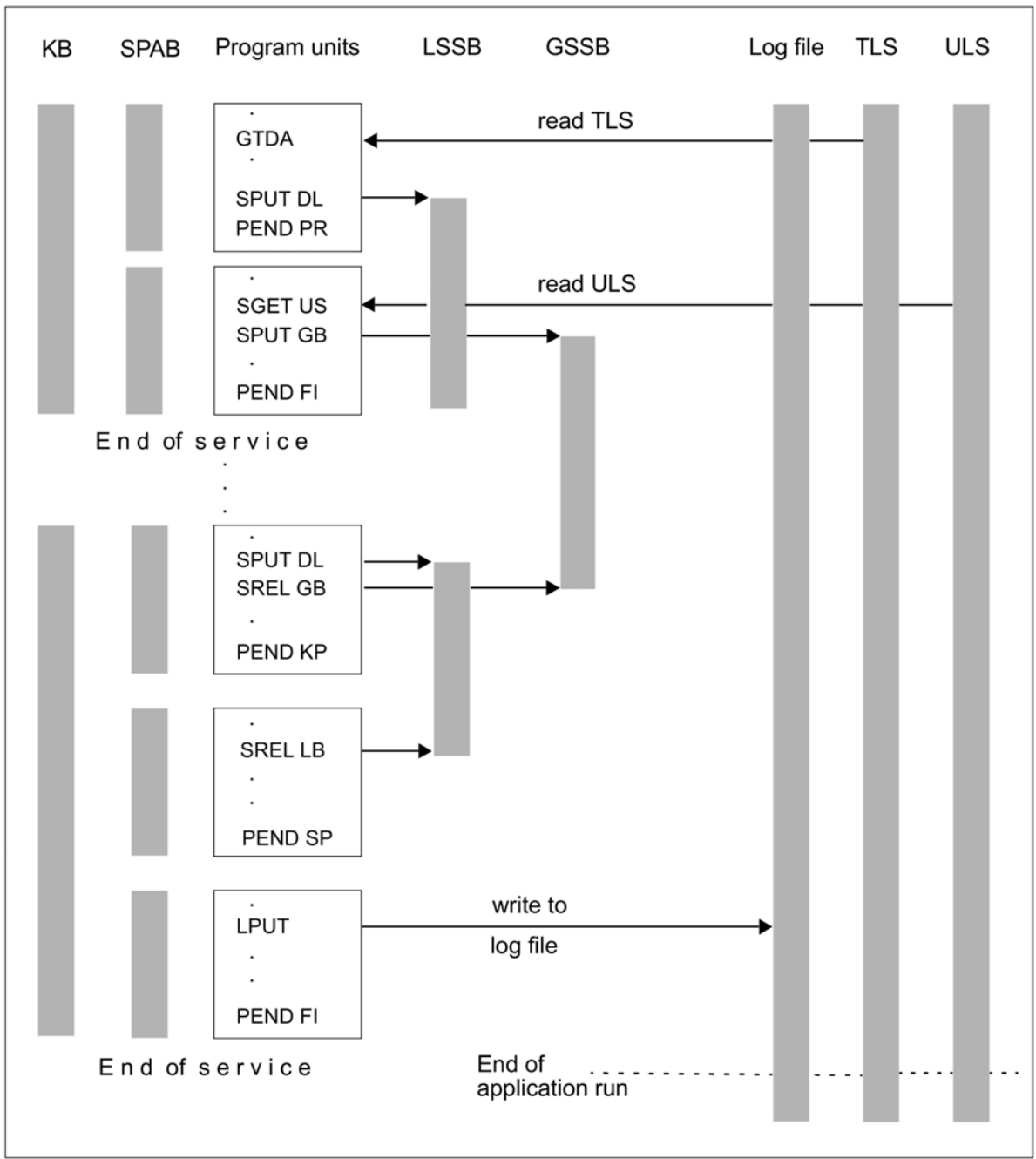


Figure: Assignment of the KDCS storage areas and KCDS calls for storage processing

2.5.1 Standard primary working area (SPAB)

By default openUTM assigns a SPAB to each program unit, the maximum length of which is defined when the application is generated (see the openUTM manual “Generating Applications”). It is available to the program unit from the program start until the PEND call.

No data can be stored or transferred using this area beyond the end of the program unit run. Since the SPAB serves only as a program unit-specific working area, it is **not** included in the transaction and is not rolled back by a RSET call.

The SPAB may contain the following:

- the KDCS parameter area for call execution.
In the parameter area the program transfer the data which is necessary for a KDCS call. The entries in the fields of the KDCS parameter depend on the call in question (see chapter “KDCS calls”). Language-specific data structures are available to structure the parameter area: for COBOL in the KCPAC COPY element and for C/C++ in the *kcmac.h* include file.
- the message area (NB) for provision of the input/output data.
Messages read using MGET, DGET, FGET, SGET or GTDA are entered in the message area. Here, openUTM also presents information which you can request with any of the INIT, DADM, INFO and PADM call variants. When performing output, you also use the message area to make available the data transferred with MPUT, FPUT, DPUT, SPUT, PTDA or LPUT.
For each call you have to specify the address of the message area.
- further areas with variable data specific for the program run.

Freely selectable fill characters

When you generate a UTM application you can specify a fill character of your choice (in the CLRCH operand of the KDCDEF statement MAX). openUTM then overwrites the SPAB with this character at the end of each processing step. After the start of the application program the area is filled with the specified character in the generated length.

This function is important for program testing because it facilitates the discovery of certain errors in single-process mode. Additionally, you can use this function for data protection.

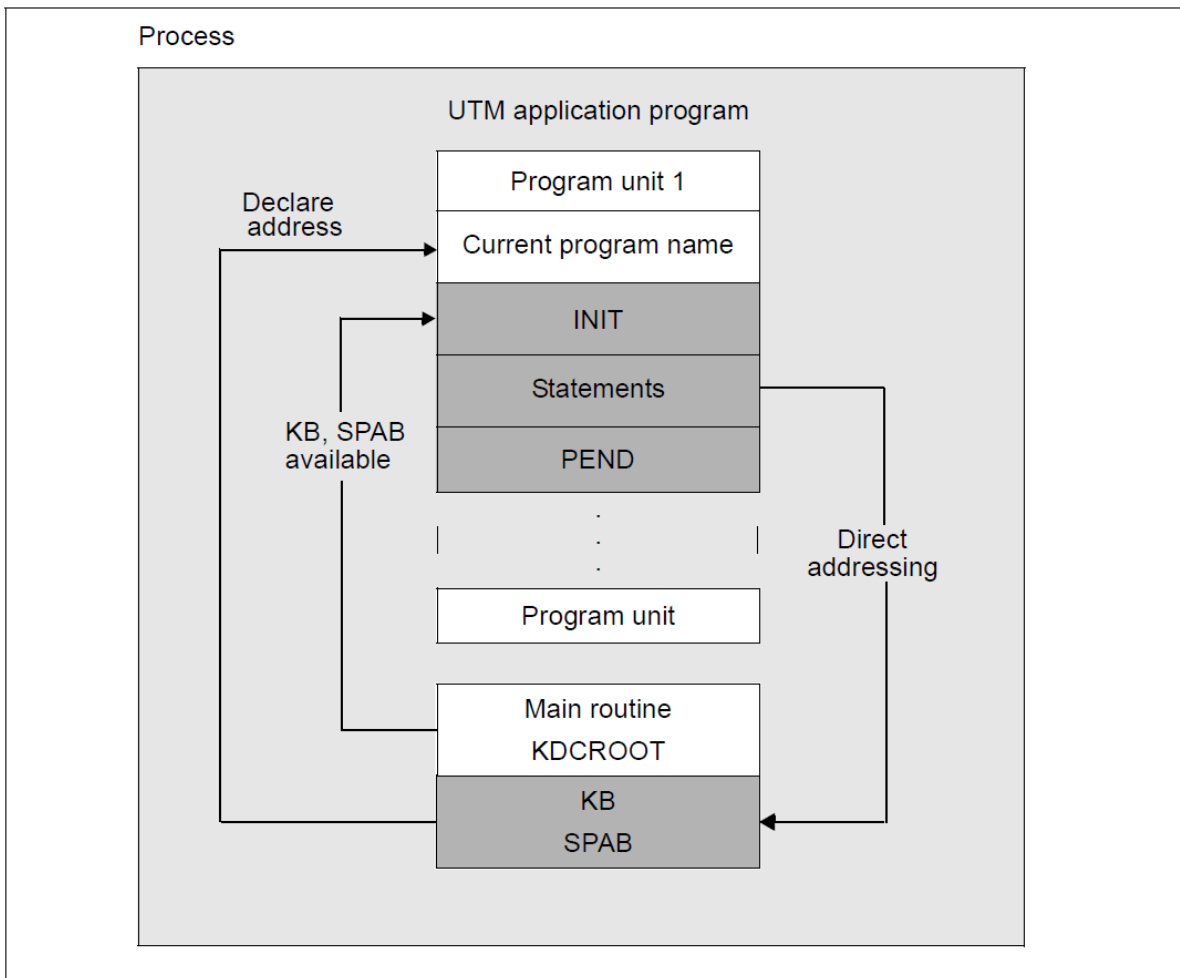


Figure: Use of primary storage areas (SPAB, KB)

2.5.2 Communication area (KB)

openUTM creates the KB when a new service is started. The KB is retained until the service is terminated. The contents of the KB are transferred to the program currently being executed. The size of the KB can be adapted to the data to be transferred, i.e. it can be increased or decreased for individual processing steps.

There are two areas of fixed lengths at the beginning of each KB. These are used for communication between openUTM and the program:

- the KB header
- the KB return area.

Language-specific data structures are available for structuring these areas: for COBOL in the KCKBC COPY element, and for C/C++ in the *kcca.h* include file.

In the **KB header** you can find current information about the service, program unit and communication partner after calling INIT, and after each subsequent call.

In the **KB return area**, openUTM transfers its return data to the program after each call (except PEND). The evaluation, in particular of the return code, provides information about whether or not a call has been executed successfully and can be used for specific control measures in the program (see also section “[Programming error routines](#)”).

Additionally, you can define an area of variable length in the KB, the **KB program area**, whose structure you can determine freely. While the KB header and the KB return area are always present, you can select whether or not you want to use a KB program area. It can be used to transfer and store service-specific data of any type.

The maximum length of this area is specified when the application is generated (KB operand in the MAX statement). In the program, you use INIT to specify the length which the program currently expects. This length may not be longer than the value you generated with the KB operand. When the next synchronization point is reached the KB is saved in the length specified by INIT. Therefore only enter the absolutely necessary minimum length for the KB when calling INIT. In this way you avoid unnecessary information being saved.

If multiple programs with KB program areas of differing length process the same service, length conflicts may occur during data transfer between programs. A program always receives data in the length specified in the KCLKBPRGE field by the predecessor program when INIT was called. If the receiving program provides longer data fields, then the remaining area is undefined. If the receiving program defines a shorter KB, it nevertheless receives the data in its full length. The truncation only takes effect when the data is passed on again (see diagram next page).

Freely selectable fill characters

When you generate a UTM application you can specify a fill character of your choice (in the CLRCH operand of the KDCDEF statement MAX). openUTM then overwrites the SPAB with this character at the end of the service. After the start of the application program the area is filled with the specified character in the generated length.

This function is important for program testing because it facilitates the discovery of certain errors in single-process mode; additionally, you can use this function for data protection.

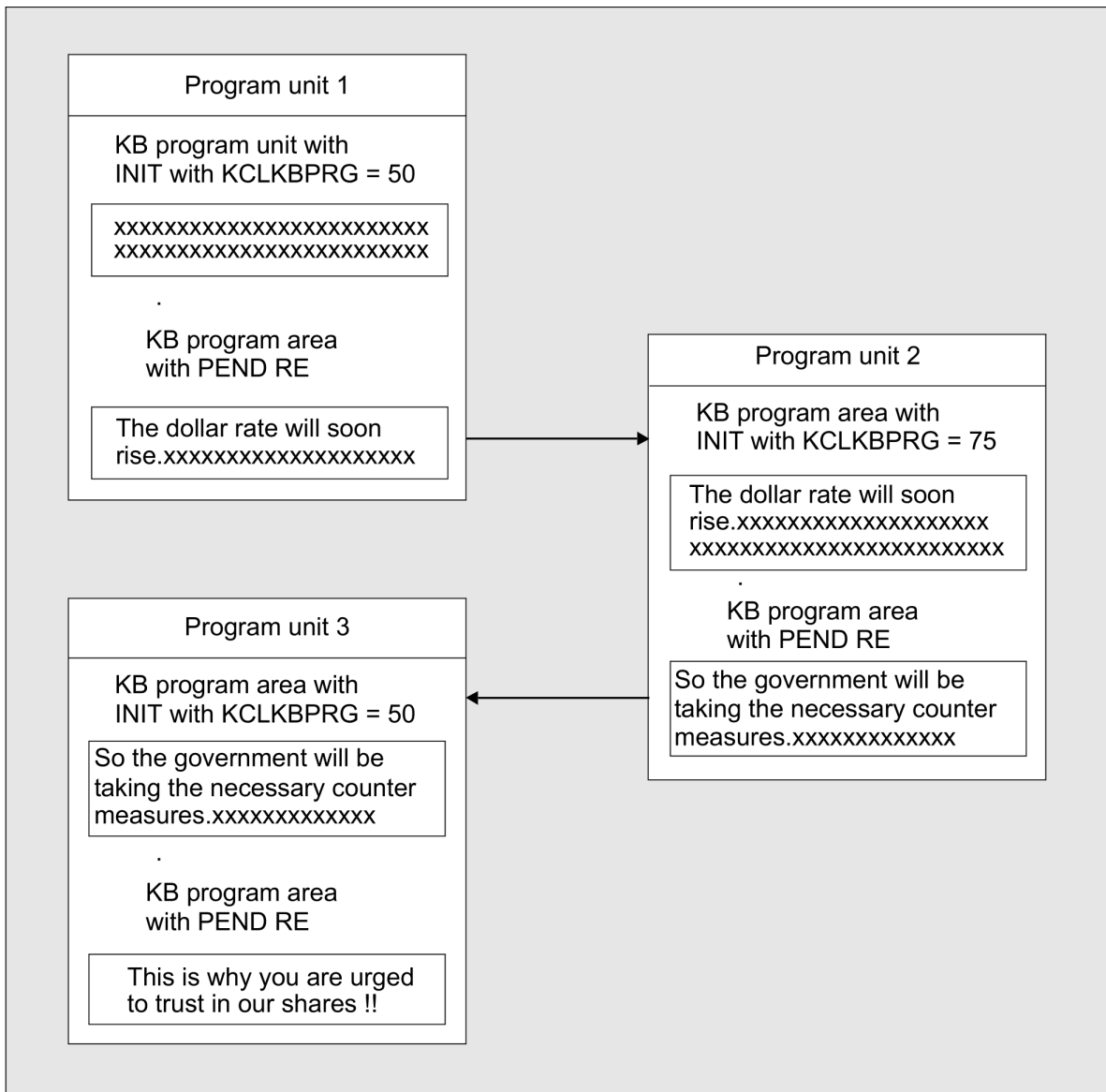


Figure: KB program area for data transfer

2.5.3 Local secondary storage area (LSSB)

LSSBs are service-specific background storage areas which are used to forward data between program units within a service. In standalone applications their contents are stored externally in the KDCFILE, see [“Storage location for user data” \(KDCS storage areas in openUTM\)](#). While openUTM automatically makes the communication area available for each program unit and then saves it, the LSSB is only accessed when necessary. It is therefore particularly useful for data which is accessed for reading only or if multiple program units are present which do not require the data between the point when the data is written and the time it is read.

For example, you can use LSSBs in the following cases:

- creation of a "browse function" for dialog outputs
- "temporary" data storage

You can use the SPUT call to write to a LSSB. To do this, enter the name of the area you want to write to. This name is only valid for the local service; if two services have the same name, then the names designate two different LSSBs. The LSSB is set up on the first write access within a service. Here the programmer defines the length of the LSSB. An LSSB can have a maximum length of 32767 bytes.

You use the SGET call to read from the area. If the storage is not required after the SGET call, it can be simultaneously released. You can also use the SREL call to release an LSSB. As soon as the associated services has terminated, any unreleased LSSBs are released.

The maximum number of LSSBs that you can create within a service is determined when the application is generated (MAX statement, LSSBS operand, see also the openUTM manual “Generating Applications”).

Unix, Linux and Windows systems

In UTM cluster applications LSSB contents are stored externally in the cluster page pool, see [“Storage location for user data” \(KDCS storage areas in openUTM\)](#).

2.5.4 Global secondary storage area (GSSB)

GSSBs are background storage areas just like LSSBs. The GSSB differs from the LSSB in its function, lifetime and application. The GSSB permits the transfer of data from one service to another. Data transfer is also possible after the end of an application run in UTM-S applications, i.e. data remains available to the application after restart.

You can, for example, use a GSSP to transfer data between dialog and asynchronous services if you do not use service-controlled queues (see "[Messages to service-controlled queues](#)").

It is open to all services. You must therefore define an unambiguous name in all the program units of an application. A GSSB is reserved for a service from an SPUT, SGET or SREL call until the end of the transaction. This prevents multiple accesses. A call from another service to the reserved GSSB waits until this is free again. openUTM locks the GSSB from the time of access to the end of a transaction (see also the section "[Action with locked storage areas \(TLS, ULS and GSSB\)](#)").

You define the maximum wait period at generation time (KDCDEF statement MAX, operand RESWAIT, value time1). The UNLK call explicitly unlocks a GSSB, i.e. releases it prematurely for a waiting service, provided that the GSSB has only been read.

You call SPUT to create a GSSB (and its name).

The contents of a GSSB are maintained until it is released in a program unit by means of the SREL call. Its life is not limited. It is thus again made available to a UTM application after an interruption of operation provided that, in the case of a standalone application, the same KDCFILE is used as before the interruption or if the user data has been transferred to a new KDCFILE using the KDCUPD tool.

In a program unit, you can use the KDCADMI call KC_GET_OBJECT (object type: KC_GSSB) to ascertain the names of all currently existing GSSBs.

You define the maximum number of GSSBs which can be generated when you generate the application (MAX statement, operand GSSBS=, see also the openUTM manual "Generating Applications").

Unix, Linux and Windows systems

In UTM cluster applications, GSSBs are supported throughout the cluster. I.e. they are stored in the cluster page pool and are therefore available for all users in all node applications. This means that all the node applications have the same view of the data in the storage area, see also "[Storage location for user data](#)" ([KDCS storage areas in openUTM](#)).

The contents of a GSSB are maintained until it is released in a program unit by means of the SREL call. Its life is not limited. It is thus again made available to a UTM application after an interruption of operation provided that, in the case of a UTM cluster application, the same cluster page pool is used as before the interruption or if the user data has been transferred to the new cluster page pool using the KDCUPD tool.

2.5.5 Terminal-specific long-term storage area (TLS)

The TLS is assigned to a connection point (LTERM, LPAP or OSI-LPAP partner) and is used to store information that is to be available independently of the life of the services and the operating time of the application. This long-term storage may consist of multiple blocks whose names you define in the TLS statements. A separate TLS statement is used to define each TLS block name. You can specify multiple TLS statements. The defined block names are the same for all LTERM/LPAP/OSI-LPAP partners. A particular block can be identified by its block name and the names of its LTERM/LPAP/OSI-LPAP partners (see the openUTM manual "Generating Applications").

For example, you can use a TLS

- to generate statistics for an LTERM, LPAP or OSI-LPAP partner or
- to log access violations, for a example for an MSGTAC exit, see ["Example of a MSGTAC program unit" \(Asynchronous service MSGTAC\)](#).

A program unit of a dialog service can only access blocks belonging to its "own" TLS, i.e. only the TLS of the LTERM, LPAP or OSI-LPAP partner via which the service was started.

A program unit run of an asynchronous service can read blocks from all the LTERM, LPAP or OSI-LPAP partners of the UTM application.

You use GTDA to read and PTDA to write a TLS block. openUTM locks a TLS block from the time of access to the end of the transaction. You can specify the maximum wait period at generation (KDCDEF statement MAX, Operand RESWAIT, value time1). If a TLS has only been read, you can use the UNLK call to *explicitly unlock the* TLS (see also the section ["Action with locked storage areas \(TLS, ULS and GSSB\)"](#)).

The TLS is used to store information that has to be available independently of the life of the services and the operating time of the application. It is thus again made available to the UTM application after an interruption of operation provided that the same KDCFILE as before is used or if the KDCUPD tool is used to transfer the user data to a new KDCFILE.

Unix, Linux and Windows systems

In UTM cluster applications TLSs are only supported locally in the nodes , i.e. each node application has its own TLSs.

2.5.6 User-specific long-term storage area (ULS)

The ULS is a long-term storage area which is assigned to each user ID (USER), LU6.1 session (LSES) and OSI-TP association (ASSOCIATION-NAMES of the OSI-LPAP statement). This long-term storage may consist of multiple blocks whose names you define in the ULS statements. A separate ULS statement is used to define each ULS block name. The defined block names are the same for all user IDs. A particular block can be identified by its block name and the name of the associated user ID (see the openUTM manual “Generating Applications”).

You can, for example, use the ULS to record statistics about user IDs.

Without administrator privileges, a program unit can only access the ULS blocks of the user ID under which it was started. To access ULS blocks of other user IDs, the program unit must have administrator privileges.

You use the SGET call to read and the SPUT call to write a ULS block. openUTM locks a ULS block from the time of access to the end of a transaction. You can specify the maximum wait period at generation (KDCDEF statement MAX, Operand RESWAIT, value time1). If a ULS block has only been read, you can use the UNLK call to unlock the block explicitly (see also section “[Action with locked storage areas \(TLS, ULS and GSSB\)](#)”).

The ULS is used for storing information that has to be available independently of the life of the services and the operating time of the application. It is thus again made available to a UTM application after an interruption of operation, provided that, in the case of a standalone application, the same KDCFILE is used as before the interruption or if the user data has been transferred to a new KDCFILE using the KDCUPD tool.

Unix, Linux and Windows systems

In UTM cluster applications, user-specific, long-term storage is supported throughout the cluster. I.e. the data is stored in the cluster page pool and is therefore available for all users in all node applications. This means that all the node applications have the same view of the data in the storage area, see also “[Storage location for user data](#)” ([KDCS storage areas in openUTM](#)).

The ULS is used for storing information that has to be available independently of the life of the services and the operating time of the application. It is thus again made available to a UTM application after an interruption of operation, provided that, in the case of a UTM cluster application, the same cluster page pool is used as before the interruption or if the user data has been transferred to the new cluster page pool using the KDCUPD tool.

2.5.7 User log file

The user log file (USLOG file) is used for recording user-specific data.

Unix, Linux and Windows systems

User log files are only supported locally in a node in a UTM cluster application, i.e. every node application writes to its own USLOG file.

It has the following record structure:

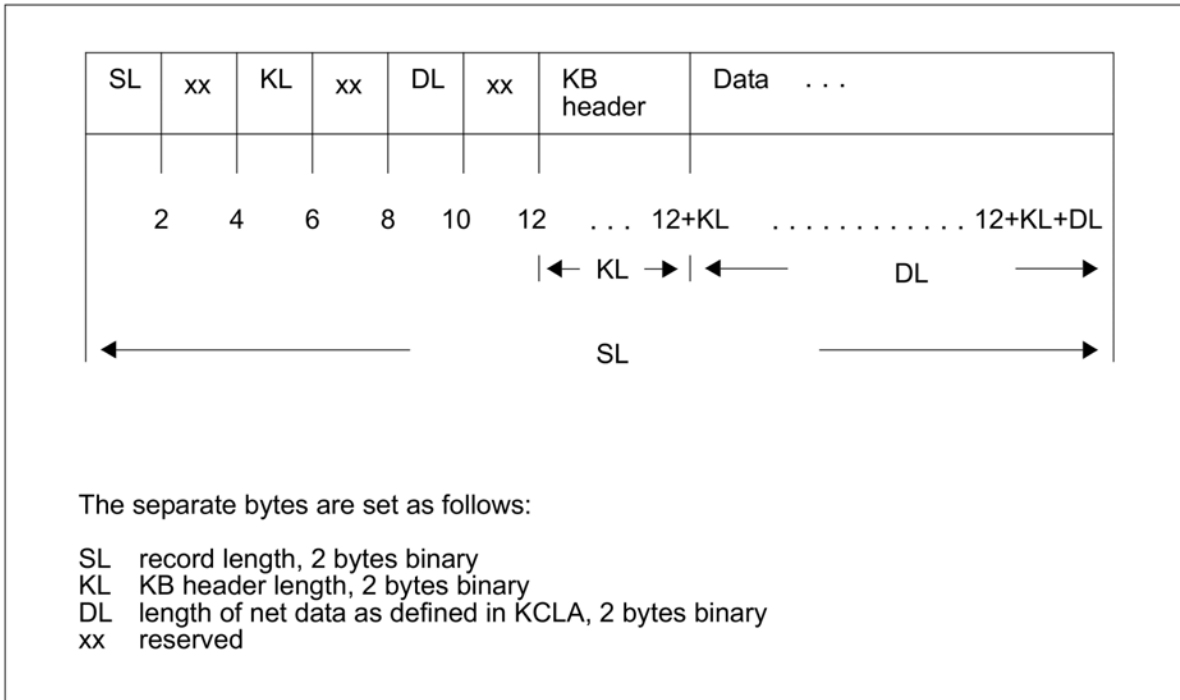


Figure: Record structure of the user log file

Each data record is generated with an LPUT call. openUTM additionally enters the contents of the KB header in the prefix of the data record. These contents are the same as at the time of the INIT call. You simply have to provide the data area containing the data which you want to log.

For more details on the user log file see the corresponding openUTM manual "Using UTM Applications".

2.5.8 Other areas

A program unit can use up to 99 other areas, which you define with the KDCDEF statement AREA (see the openUTM manual “Generating Applications”). AREAs are shared storage areas available to the UTM application. The structure of these areas is not predefined by openUTM and you can define them as you wish.

The addresses of such storage areas are passed along with SPAB and KB as additional parameters at the start of the program. These areas are **not** subject to the transaction concept: openUTM does not save these areas, nor does it roll back them with an RSET or lock them. This means that the application program alone is responsible for managing these storage areas.

For information about how you define such an area in your programming language, refer to "[Other data areas \(AREAs\)](#)" for C/C++ and "[COBOL program units as subroutines](#)" for COBOL.

i When program units which use AREAs are transferred from one application to another, the use of AREAs may cause problems, for example because of differences in parameters. Alternatives to the use of AREAs are described on "[Other data areas \(AREAs\)](#)" for the C/C++ programming language and "[COBOL program units as subroutines](#)" for COBOL.

Unix, Linux and Windows systems

AREAs in a UTM cluster application are always node-specific, i.e. one node cannot access the AREAs in another node.

2.5.9 Action with locked storage areas (TLS, ULS and GSSB)

If multiple UTM transactions attempt to access GSSB, TLS or ULS storage areas simultaneously, openUTM synchronizes these accesses.

Each access (for reading, writing or deleting) to a TLS, ULS or GSSB causes openUTM to lock this area for other transactions:

- until the next synchronization point (PGWT CM, PEND RE, FI, SP or FC) or
- until the next roll back operation (PGWT RB, RSET, PEND RS or PEND ER/FR) or
- until release with the UNLK call if the area has only been read.

If a transaction attempts to access the locked area, openUTM places it in a queue until

- the lock has been released
- or the maximum wait period has elapsed.
- or the transaction responsible for the locking of the area uses PEND KP or PEND PA/PR with TAC class change or wait for DGET message or with PGWT KP/PR/CM to set itself to a wait state of undefined length.

The process remains blocked and cannot take on other tasks during the wait period.

This maximum wait period is defined by the value time1 of the RESWAIT operand in the KDCDEF statement MAX (default: 60 seconds, see also the openUTM manual “Generating Applications”). If a transaction waits longer than the time defined by RESWAIT (time1), openUTM rejects the access attempt with the return codes KCRCCC = 40Z and KCRCDC = K810.

UTM rejects such an access attempt **immediately**

- if the area has been locked by another transaction which has just used PEND KP or PEND PA/PR with TAC class change or wait for DGET message or PGWT KP/PR to set itself to a wait state of undefined length (KCRCCC = 40Z and KCRCDC = K810), or
- if waiting would lead to a deadlock in GSSB, TLS and ULS areas (KCRCCC = 40Z and KCRCDC = K820).

Unix, Linux and Windows systems

In cluster applications, deadlock detection must be enabled explicitly for this purpose (see also KDCDEF statement CLUSTER DEADLOCK-PREVENTION in the openUTM manual “Generating Applications”).

If a transaction accesses a GSSB, ULS or TLS for reading only, it is advisable to release this area again as quickly as possible - in particular before database calls or PEND PA/PR with TAC class change or wait for DGET message or before PGWT KP/PR - in order to shorten the waiting times of other transactions.

No such locks can occur during access to LSSBs, since it is not possible to access LSSBs across services.

2.6 Programming error routines

openUTM returns the following return codes in the return area of the communication area after KDCS calls: in the KCRCCC field, after each call a KDCS return code in accordance with DIN 66 265 (compatible return code) and possibly a UTM-specific return code in the KCRCDC field (KCRCDC). These return codes inform you whether openUTM was able to execute the KDCS call or why openUTM could not execute it.

For each KDCS call there is a description of the error codes that may occur with that call. For a list of error codes refer to the openUTM manual "Messages, Debugging and Diagnostics".

If control is returned to the program unit after a call, it therefore has to check:

- whether the call was executed without errors; this is the case if the program unit recognizes that the KDCS return code has the value "000" (in the KCRCCC field).
- which errors have occurred on the basis of the specified error code.

Additional information that may be relevant for the measures which are to be implemented include the actual transferred length (KCRLM field) and the employed format character (KCRMF/kcrfn field) etc.

In the event of serious errors, the program unit does not get control back. In such cases, openUTM rolls back the transaction, terminates the service and creates a PEND ER dump; the error code that led to the abortion of the service can be obtained from the UTM Diagarea of the PEND ER dump. You will find more information on the analysis of a PEND ER dump in the openUTM manual "Messages, Debugging and Diagnostics".

On Unix and Linux systems, you have the option of keeping control in certain cases by performing a user-specific error handling, see "[User-specific error handling \(Unix and Linux systems\)](#)".

i Control is not returned to the program unit after a PEND call. The return area cannot therefore be subsequently evaluated in the program unit. If errors occur during PEND processing, UTM responds as described above.

The program unit can use RSET, PGWT RB or PEND RS/ER/FR to roll back the transaction: a PEND ER causes a dump to be requested.

It might also happen that openUTM returns an error message because it has received an error message from one of the components involved (e.g. the formatting system).

In the case of such errors openUTM executes an internal error handling routine, thus relieving the program unit of this task. Where possible, openUTM corrects the error, otherwise the service is aborted by PEND ER and the appropriate UTM error code is set.

For examples of error routines, refer to the sample programs, for C/C++ "[Programming examples in C/C++](#)", for COBOL "[Programming examples in COBOL](#)".

2.7 Message segments

The KDCS interface enables you to process message segments. In this way, you can combine message components in order to forward them to the communication partner as a complete message.

The use of message segments has the following advantages:

- message areas only have to be as large as the largest message segment
- message segments can be processed separately
- formats can be made up of partial formats.

You use the MPUT NT, FPUT NT, DPUT NT or DPUT QT call to send message segments to openUTM.

Message segments may be addressed to a terminal, a client program, a queue, a printer, a follow-up program unit, a local asynchronous service or, with distributed processing, a remote partner.

In all cases where multiple message segments are addressed to a program unit, you must read each of these message segments with a separate DGET, MGET or FGET.

On BS200 systems, the following applies: If you use formats then you can send formatted message segments in messages to terminals and printers. In the case of dialog messages to terminals you must then use partial formats (see "[Using partial formats \(BS2000 systems\)](#)"). In the case of formatted asynchronous messages to terminals, each message segment is treated as a separate message. In the case of formatted asynchronous messages to printers, the message segments are combined to form a logical unit.

Messages with format identifiers can also be sent to UPIC clients as well as to LU6.1 partners. Formats are not used to prepare the messages for these partners, but more precisely to describe the structure of the user data. openUTM does not call a formatting routine when sending formatted messages to these partners, rather the format name is sent to the UPIC client or LU6.1 partner instead.

Note on the diagram below

If, in the first program unit (TAC1), FPUT is written as FPUT NT, it will again produce an asynchronous message of its own since openUTM terminated the message with PEND PR.

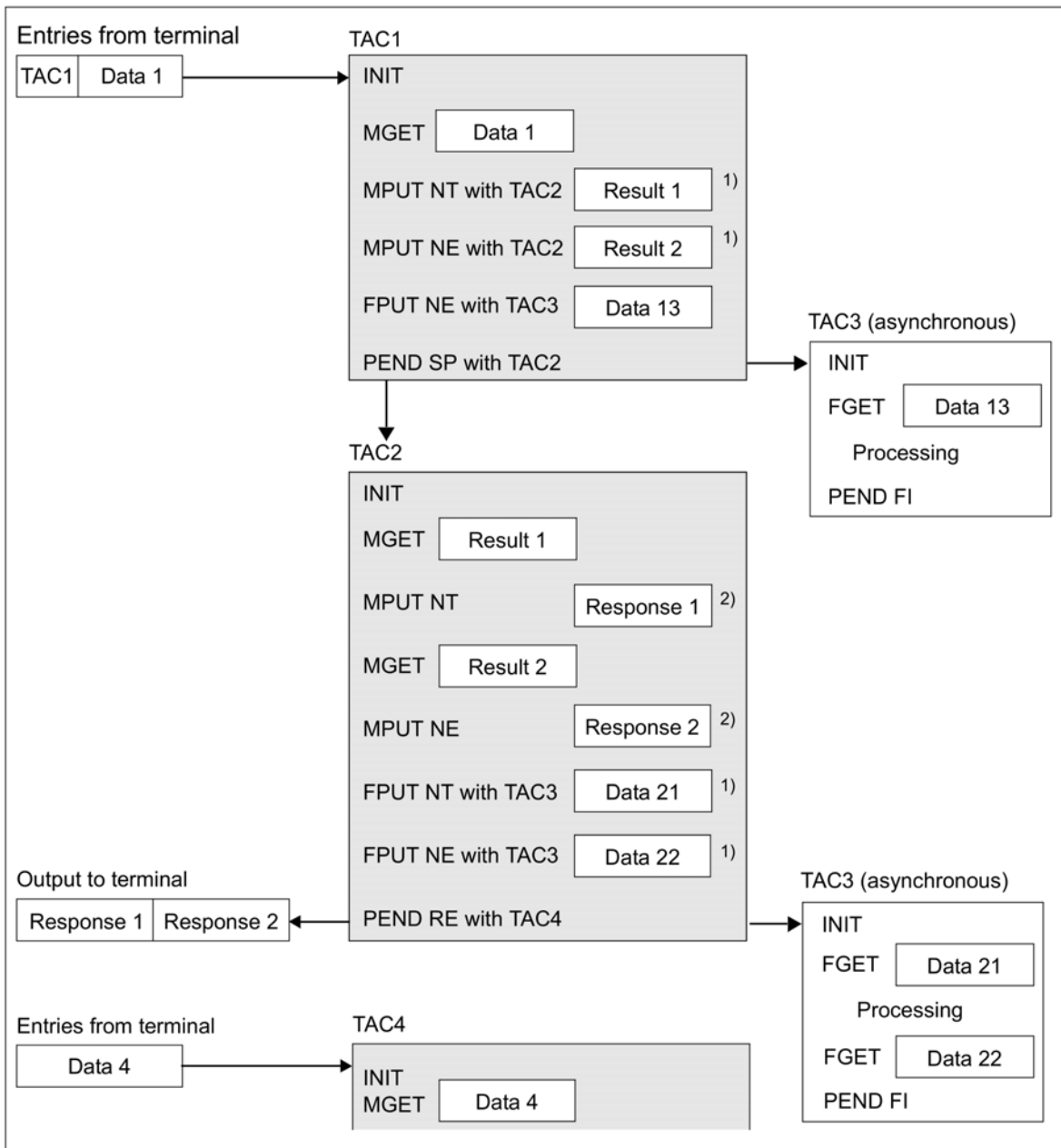


Figure: Message segments

- 1) If message segments are sent from one program unit to another, each message segment must be read with its own MGET NT or FGET.
- 2) Message segments to a terminal are combined by openUTM into a single message.

2.8 Communication partners of a UTM application

A UTM application can communicate with a variety of partners. Communication partners of an openUTM application are for example:

- Terminals
The KDCS interface enables you to connect character-oriented terminals directly. You can use these terminals in line mode or - in openUTM on BS2000 systems - you can use screen forms (masks).
- UPIC clients
UPIC clients are programs that use the CPI-C interface with the UPIC carrier system to communicate with the UTM application.
- Transport system (TS) application
Transport system applications are programs that use the transport system interface directly to communicate with the UTM application, e.g. sockets. TS applications can also be other UTM applications.
- HTTP clients
HTTP clients are programs that use the HTTP protocol to communicate with the UTM application via the socket interface.
- Printers
You can create output jobs for printers from openUTM services (see section "[Programming error routines](#)"). Print jobs are also part of the transaction concept.
- OSI TP, LU6.2 or LU6.1 partners
The partner may be another openUTM application or a UTM-Client application with the OpenCPIC carrier system, or it may be an application that uses a transaction system from a different manufacturer.
- Message queues
In UTM services, messages can be written to message queues, from where they can be retrieved by the recipient at any time. These queues are also included in the transaction concept.

You use the same KDCS calls for communication with all these partners:

MPUT	to send a dialog message to the partner
FPUT/DPUT	to send an asynchronous message to the partner or a message queue
MGET	to receive a dialog message from the partner
DGET	to read an asynchronous message from a message queue
FGET	to receive an asynchronous message from the partner

The following calls can also be used for communication within a UTM application:

- You can use MPUT to send a message to a follow-up program unit which then can use MGET to read this message. However, you can also use service-specific storage areas to exchange information between program units of a service (KB and LSSB, see section "[KDCS storage areas in openUTM](#)").
- You can use FPUT/DPUT to send asynchronous messages to local asynchronous services or message queues. The messages can then be read with FGET/DGET.

2.9 Output to printers

You can output to printers in two different ways:

- hardcopy to a central or local printer
- output jobs to printers (print jobs), also called spooling

Transaction-oriented output to printers is not supported on Windows systems.

2.9.1 Hardcopy mode with openUTM on BS2000 systems

You can activate automatic hardcopy mode using the screen function KCREPR in the KCDF field of the KDCS parameter area. If you use #formats control is performed via global attributes.

You can also activate the hardcopy function using edit profiles (specifications in KCMF/kcfn). To do this, you have to set the operand HCOPY=Y in the KDCDEF statement EDIT when you define the edit profile (see the openUTM manual "Generating Applications").

In hardcopy mode you have to use MPUT, FPUT or DPUT to send the message to the terminal. This initiates the printout, i.e. if you use MPUT, blanks are entered in KCRN and if you use FPUT/DPUT, the LTERM name of the terminal is used.

The terminal user can also press the key to print the current screen contents to the selected, assigned printer.

2.9.2 Print jobs

You use the FPUT or DPUT message queuing calls to create print jobs (see section “[Messages to UTM-controlled queues](#)” and chapter “[KDCS calls](#)”). Here you have to specify the LTERM name of the printer in the KCRN field. openUTM enters the job in the corresponding queue.

You can

- use a single FPUT or DPUT call (NE in KCOM field) to generate a print job or
- construct print jobs using multiple FPUT or DPUT calls (for message segments): NT in KCOM field and NE for the last FPUT or DPUT call.

openUTM handles the message segments of a print job as one entity when determining print sequences or for error handling. With printer pools, openUTM sends all the message segments of a job to **one** printer.

You can either print out in line mode.

On BS2000 systems you can output print jobs in format mode.

On BS2000 systems it is also possible with RSO printers to pass a parameter list to RSO using FPUT RP or DPUT RP. RSO changes the parameter settings depending on the particular printer type.

Administering message queues and printer control

You use the KDCS call DADM (see “[DADM Administer message queues](#)”) to administer the UTM-controlled message queues which contain the print jobs and are assigned to the LTERM partner.

With the DADM (delayed free message administration) call, you can:

- read information about jobs of a message queue into the message area
- change the processing sequence of jobs of a message queue
- delete individual jobs or an entire message queue
- move defective messages from the dead letter queue

You can use the KDCS call PADM for printer control.

With PADM (printer administration) you can:

- activate or deactivate the confirmation mode for a printer control LTERM
- confirm or repeat a print out
- modify the assignment of the printer to an LTERM partner
- change the printer status, i.e. lock and release the printer, establish or cancel connection to a printer
- read information about a printer into the message area
- read information about print outs to be confirmed

For detailed information about the administration of message queues, the execution of print outs and printer control options refer to the openUTM manual “Administering Applications”.

Avoiding bottlenecks during high volume printing

The message queues are stored in the Pagepool of the KDCFILE. To avoid bottleneck situations when printing high volumes and to avoid a Pagepool overflow, you can make the following provisions in the program unit or at generation.

- In the program unit:
 - Evaluate the return code 40Z/K701 after FPUT/DPUT calls to printers or the "K041 warning level # for PAGEPOOL exceeded" message in an MSGTAC program unit and, for example:
 - establish a connection to the printer for which there are many messages available so that the messages can be printed and then deleted by openUTM
 - or delete FPUT via the DADM administration, or block TACs that send FPUTs to the printer.
- For each generation:
 - use QLEV= (LTERM statement) to establish the maximum number of messages which openUTM can temporarily store in a message queue. Print jobs are not taken into account until end of transaction. openUTM rejects further messages to this printer with 40Z.
 - use QAMSG= (LTERM statement) to determine whether messages to a printer which is not connected to the application are to be buffered.
 - estimate the necessary, additional space for printer messages in Pagepool and enter a sufficiently high value in the PGPOOL operand of the MAX statement, for recommendations see the openUTM manual "Generating Applications".

2.10 Support for ID card readers on BS2000 systems

UTM supports ID card readers at data display terminals.

You can use the ID card reader in two ways:

- access protection through ID card control at sign-on
- data input via ID card

You cannot use the ID card reader both ways simultaneously: after signing on with the ID card reader, the terminal user cannot then use the ID card to enter data.

2.10.1 Signing on to the application via ID card reader (BS2000 systems)

You can configure user IDs for a UTM application in such a way that access to the application via a user ID is only possible with a special ID card (magnetic strip card): This can be done either via the KDCDEF statement USER Operand CARD at generation or through dynamic configuration (KC_CREATE_OBJECT, object type KC_USER).

If a user signs on via a user ID for which an ID card check is configured, the user is requested to insert the ID card in the reader. openUTM checks the ID card information. If this information agrees with the information generated in the configuration for this user ID, the user is allowed to work with this application

If an ID card is in the reader during dialog input, openUTM enters the identifier "A" in the KCAUSWEIS/kccard field of the KB header.

The user must leave the ID card in the reader until he or she has signed off from the application with KDCOFF, otherwise openUTM disconnects the connection to the terminal.

You can call the ID card information in the program units, for example using the KDCS call INFO with the "CD" (CARD) operation modifier.

2.10.2 Data input via ID card (BS2000 systems)

If you do not use the card reader for sign-on check, you can enter data via the card reader in the following way on BS2000 systems:

If you use the screen function KCCARD or an edit profile with SPECIN=I to output a dialog message (MPUT), the keyboard is locked and the user is requested to insert the magnetic strip card into the ID card reader (this should be made clear in the text for the dialog message).

The follow-up program unit can then use **MGET** to read the data of the magnetic strip card like a normal screen input.

If no magnetic strip card is available to the user, he or she can unlock the keyboard by pressing either the key (or together with). In this case, when MGET is called, the follow-up program receives the return code which you assigned to the key with the KDCDEF statement **SFUNC** during generation.

If you remove the magnetic strip card from the card reader, openUTM repeats the last dialog output (internal KDCDISP).

Checking availability

- You can check whether the ID card is available in the KCAUSWEIS/kccard field in the KB header. In this case openUTM sets the character "A" if the ID card was inserted at the last input.
- You can check the availability of an IID card reader by means of an INFO CK call: the return code of the INFO CK call tells you whether or not there is an ID card reader at the terminal. It makes sense to call INFO CK *before* an MPUT call with KCCARD. In the case of an MPUT with KCCARD to a terminal which does not have a card reader, UTM terminates the service abnormally.

3 Interaction with databases

openUTM supports coordinated interaction with database systems. openUTM uses **two-phase-commits** to synchronize the UTM transactions and the transactions of the database system (see the openUTM manual “Concepts and Functions”).

A UTM application can interact in coordination with multiple database systems. This means that a UTM transaction can contain calls to **different** database systems.

If a UTM program unit terminates a dialog or processing step with PEND KP, the transaction is normally continued in a different process. If the program unit run is terminated with PEND PA/PR, it is also possible that the processing step will be continued in a different process. In distributed OSI TP transactions, a transaction is normally also terminated in a different process after the KDCS calls PEND SP, RE, FI or PGWT CM. In this kind of environment, all database systems involved in the transaction must support the change of process.

Furthermore, it is possible in distributed transaction processing to process data from a number of different database systems on different computers in a single distributed transaction.

Rolling back transactions

If an error occurs, openUTM rolls back all the databases of a transaction to a common synchronization point. There is no need for the programmer to coordinate openUTM and the database systems.

The database system can also roll back DB transactions itself, e.g. to release long-term locks. In this case the transactions are again synchronized and the program unit is informed by the corresponding DB system return code.

Internal interface between openUTM and database systems

openUTM employs a uniform and neutral interface to control the interaction with database systems. In this way openUTM is independent of any implementation-specific features of the various database systems.

On Unix, Linux and Windows systems, this is the XA interface standardized by X/Open, on BS2000 systems the XA interface is offered and the functionally equivalent IUTMDB interface.

Supported database systems

openUTM on BS2000 systems supports coordination with the following database systems:

- UDS/SQL
- SESAM/SQL
- Oracle
- LEASY (the LEASY file system behaves like a database system with openUTM).

On Unix, Linux and Windows systems openUTM supports coordination with the database system Oracle.

Connecting openUTM with database systems

The database systems with which a UTM application is to coordinate and interact are specified in the KDCDEF statement during generation of the UTM application: on Unix, Linux and Windows systems you use the RMXA statement, for BS2000 systems the DATABASE statement (see the openUTM manual “Generating Applications”).

Note for BS2000 systems

Some database systems provide various call interfaces for the application program. These may be implemented as CALL interfaces or language elements in the programming language (e.g. in COBOL). You use the KDCDEF statement DATABASE to specify the interfaces which the program units of a UTM application use for communication.

Note for Unix, Linux and Windows systems and for XA-capable databases on BS2000 systems

No interface is specified for the application program at generation of a XA-capable database. The interface depends on the resource manager used.

Note on using XA

As a rule, there is a static and dynamic XA switch. A database can provide one or both variants. If the database provides a dynamic XA switch, you should use this. This minimizes the resources occupied in the database system.

3.1 UTM transaction and DB transaction

A service is constructed of one or more UTM transactions. The structure is determined by the program units of the service. A program unit opens a DB transaction when required, i.e. if it is necessary to read or modify the database.

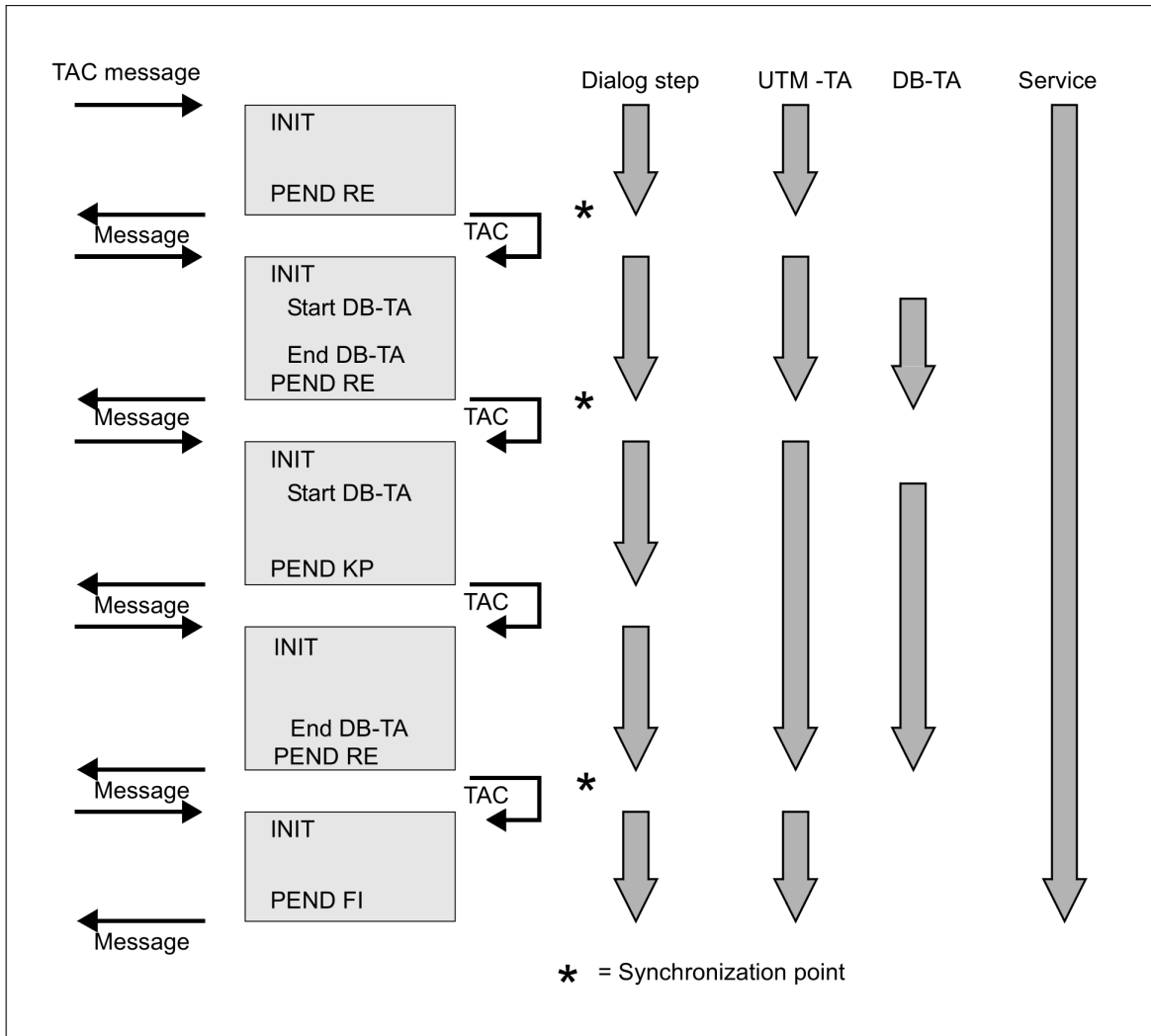


Figure: UTM transactions and DB transactions in a service

i With regard to database transactions the PGWT CM call behaves in the same way as PEND SP or PEND RE.

Multi-step transactions

A multi-step transaction consists of several UTM dialog steps within a transaction. It is often impossible to modify the data records of a dialog in a single processing step. You need a first processing step to display the data and a second to enter the modifications. By locking the data records for both processing steps you can extend the lock to a multi-step transaction.

The time between the processing steps is monitored by a timer which you specify with the KDCDEF generation tool at generation. After the timer has expired the transaction is rolled back and the locked data released.

The database systems also manage the locking period themselves and roll back the DB transactions to release the locks. The service is informed at the next DB call.

When using multi-step transactions you should note that each rollback may result in the repetition of multiple processing steps, depending on how recent the last synchronization point is.

3.2 Programming ESQL program units

A UTM-ESQL program unit is structured like a normal UTM program unit.

To communicate with databases you can use all the facilities of the ESQL interface.

However, for transaction logging you may only use KDCS calls.

ESQL calls such as `BEGIN WORK`, `COMMIT WORK` and `ROLLBACK WORK` are not permitted during the coordinated interaction of openUTM with databases. For further details refer to the manual for your database system.

i Currently, Oracle cannot migrate open cursors when connected via XA, i.e. you have to open them explicitly at the start of every program unit and close them explicitly at the end of every program unit. If you require this position in a follow-up program unit, you must program your application to save its value (e.g. in the KB or LSSB) and then set it in the follow-up program unit.

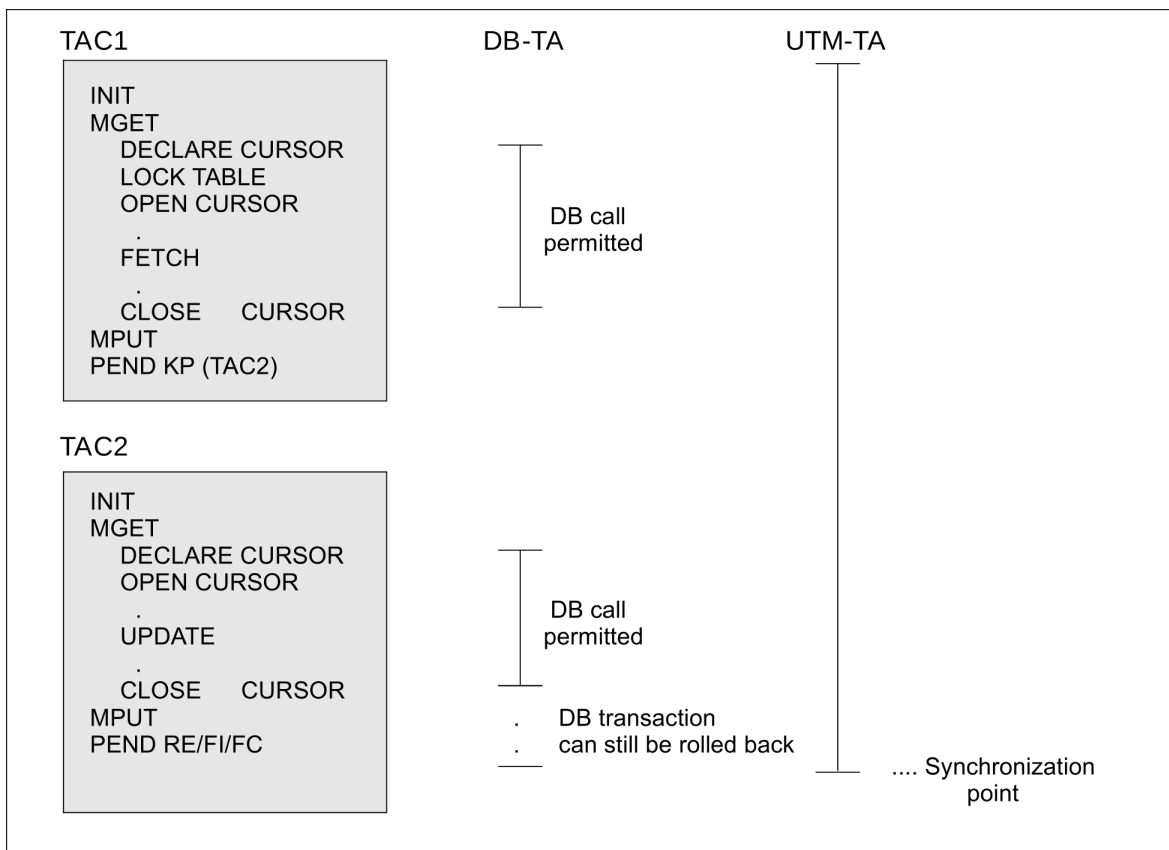


Figure: Example for use of `CLOSE CURSOR`

3.3 Error processing with connected databases

If errors occur in the interaction with database systems, openUTM processes the errors - the programmer does not need to take any special precautions.

BS2000 databases without XA

The database system informs openUTM about whether it has been able to execute a call successfully. If an error has occurred, openUTM checks the severity of the error and reacts accordingly: openUTM rolls back the transactions to the last synchronization point and outputs messages that contain information on the causes of the error. If a serious error occurs as a result of interaction with the database then openUTM generates the message K071. This message contains database status information together with a specific return code, see openUTM manual "Messages, Debugging and Diagnostics".

Database connection via XA

In this case, openUTM additionally uses XA messages (K201 - K232) to provide information about the status of the connection, irregular rollbacks, commits and errors when using XA calls (see also the openUTM manual "Messages, Debugging and Diagnostics").

A special area for further diagnosis is available in the UTM dump, the UTM Diagarea. openUTM enters trace information in this area. Alongside the KDACS calls, this area also logs all the calls to the database system. These calls can be seen after the DBCL string (see the openUTM manual "Messages, Debugging and Diagnostics").

Behavior after a system crash

After an operating system crash and abortion of the UTM application, the database should be started before the UTM application at restart. If the UTM application was generated for the UTM-S variant (default setting), then openUTM executes a joint recovery phase with the database system/database systems at the start of the application.

4 Screen functions

In this chapter, you will find all the required information about the screen functions made available by openUTM. These include the use of formats as well as the possibility of influencing screen output in line mode. The chapter also describes the cases in which openUTM performs an automatic screen restart for terminals and how format names are handled during message exchange with UPIC clients.

Note on programming

In order to simplify programming, when INIT is called, openUTM indicates the name of the format or edit profile that must be specified when reading the message with MGET or FGET in the KCRMF/kcrfn.

If a format consists of multiple partial formats you have to read each partial format with a separate MGET/FGET. Here the preceding MGET/FGET provides the format identifier in KCRMF/kcrfn. This format identifier must be entered in KCMF/kcfn in the following MGET/FGET call.

i A formatting system is not supported on Unix, Linux and Windows systems, although format names can still be sent to UPIC clients and LU6.1 partners.

4.1 Use of formats in openUTM on BS2000 systems

A format (also called a mask) is simply a form displayed at a terminal or output to a printer. Like any other form, a format consists of fields which you can fill in (input fields) and texts belonging to the form (text fields). This means that formats are forms which are stored in a computer and output at a terminal or printer when necessary (see also section [“Output to printers”](#)).

A format also contains information on how a field is represented on the screen (e.g. flashing), what you can enter in a field (e.g. numeric values only), or where the cursor should be found in the format display.

Interaction with the formatting system

openUTM cooperates with the format handler FHS (format handling system) via IUTMFORM interface.

You can use the format generator IFG (Interactive Format Generator) to create FHS formats simply and quickly within a guided dialog. Addressing aids are automatically generated which you can use in the program units to structure the message areas. The finished formats are stored in under in libraries.

If you want to perform input/output in program units, you have to set the required format identifier in the KCMF/kcfn field. Interacting with the format handling system, openUTM then automatically formats the messages.

The format identifier consists of:

- the prefix (*, + or #) which determines the type of the format (see next section).
You can also use the "-" character.
- the format name (up to a maximum of 7 characters).

Format types

openUTM distinguishes between *formats, +formats and #formats:

*formats	use these formats if you do not want to change the attributes of the format fields (e.g. display attributes) in the program. If you use *formats only the data fields are transferred in inputs/outputs.
+formats	are formats in which you are allowed to change the attributes of individual format fields in the program. For example, you can return an incorrect entry back to the terminal in flashing mode. Each data field is prefixed with a 2-byte attribute field which you can use to insert the required attribute combination in the program. If you enter binary zero, the attribute combination which was defined when the format was generated applies. openUTM provides you with all the permissible attribute combinations in language-specific data structures, in the KCATC element in COBOL and in the <i>kcat.c</i> include file in C/C++.
#formats	are formats in which you are allowed to change both the attributes of the format fields and the global attributes of the format in the program. For input/output, the attribute fields and data fields are divided into separate blocks. For further information refer to the formatting system manual.

You can also use -formats. -formats are not formatted by the formatting system, but by the event exit FORMAT, see [“Event exit FORMAT \(BS2000 systems\)”](#). If the format identifier starts with the "-" character, openUTM branches to this user-defined formatting routine.

Positioning the cursor

When formatting output with +formats and *formats, it is possible to control the position of the cursor in a program (function KDSCUR).

When setting the cursor, you have to specify the address of either the attribute field or the data field. Which is required depends on what is specified in the FHS start parameter ATTR or NOATTR:

- ATTR (only permissible with +formats): the address of the attribute field is specified
- NOATTR (for *formats and +formats): the address of the data field is specified

The cursor can be placed at the beginning of the assigned data field by correspondingly marking the attribute field. The position of the corresponding screen field is known from the format description. If several attribute fields of an output message are marked at the same time in the program run, then only the first entry is used.

The cursor can be placed on a specific field by calling the KDCSCUR() function. The field at which the cursor is to be placed the next time something is output is specified in the message area as an argument of the function.

Setting the cursor in COBOL program units:

```
CALL "KDCSCUR" USING FNAME.
```

Setting the cursor in C/C++ program units:

```
KDCSCUR (field name); (The result of the function is of type void)
```

The following arrangement is valid regarding the KDCS attribute functions (+formats and *formats):

The cursor can be positioned at the beginning of a message field F(i) by calling the "KDCSCUR" subroutine with the i-th attribute field AF(i) as a parameter. The subroutine contains the cursor identifier as a constant and adds this constant to the attributes already specified in the attribute field passed as a parameter.

Example:

```
CALL "KDCSCUR" USING AF1.
```

The program unit run would like to place the cursor at the beginning of the message field F1 in addition to the field attribute already defined.

Changing format between input and output

If openUTM outputs a message with a particular format identifier, you have to specify the same format name in the KCMF/kcfn field with MGET for the next input.

Exception:

If you do not use partial formats, openUTM tolerates for MGET an incorrect format identifier in KCMF/kcfn: the message is nevertheless formatted in accordance with the last screen format, the 05Z return code is set and the format identifier of the last employed format is displayed in KCRMF/kcrfn.

If an incorrect format identifier is specified in the KCMF/kcfn field when reading partial formats, openUTM sets return code 03Z, returns the correct format identifier in KCRMF/kcrfn and sets KCRLM to 0. There is no entry in the message area.

4.1.1 Screen output functions in format mode (BS2000 systems)

openUTM enables you to request specific screen functions together with the message output when using +formats and *formats. To do this, you enter one of the predefined values for your programming language in the KCDF (device function) field in the KDCS parameter area. For C/C++ these values are in the kcdf.h include file and for COBOL in the COPY element KCDFC.

With "#" formats, KDCF must be set to binary zero. The screen functions are controlled using global attributes.

You can use the following functions in +formats and *formats:

KCREPL	(replace)	
		Clear and rewrite screen
KCERAS	(erase)	
		If KCLM = 0, all variable fields are erased, the format is retained. If KCLM > 0, new field contents are output in the same format, other variable fields are erased
KCALARM	(alarm)	
		An audible alarm sounds at output
KCREPR	(reproduce)	
		Screen output to printer
KCRESTRT	(restart)	
		screen restart after PEND RS
KCNODF	(no device feature)	
		No screen function, KCDF is set to binary zero

If you are working with message segments, only the entry for the first message segment applies. All subsequent message segments must have binary zero in the KCDF field.

You can combine two or more screen output functions, for example with the statement:

COBOL: `KCDF = KCREPL + KCREPR + KCALARM`

C/C++: `kcdf = KCREPL | KCREPR | KCALARM`

For performance reasons, however, you should use the KCREPL function sparingly.

The effect of KCERAS and KCREPL depends on the selection of the FHS start parameters, see the "FHS User Guide".

For information on error processing when formatting errors occur, refer to the openUTM manual "Messages, Debugging and Diagnostics".

4.1.2 Starting services using basic formats (BS2000 systems)

If necessary, you can make formats available before service start in order to simplify the entry of the data required by the service.

These formats are called basis formats. You can use basic formats in the following ways:

- **Define start formats**

In the configuration of the UTM application you can define a specific start format for each LTERM partner. In applications with the SIGNON event exit (see "[The SIGNON service](#)") the exit can read this start format if no user is logged on to this LTERM. In applications without the SIGNON event exit and without user IDs, this start format is output after the terminal connection is established through this LTERM partner.

In the configuration of the UTM application, you can define a user-specific start format for each user ID. After the user has signed on to UTM under this user ID, UTM outputs this format on screen. In applications without a SIGNON event exit, openUTM outputs this format after the user has signed on to openUTM under this user ID. In applications with a SIGNON event exit, the exit can read this start format if a user has signed on under this user ID. *formats, +formats and #formats can be used as start formats. #formats can only be used as start formats, however, when the SIGNON event service is used.
- **Format output at end of service**

At the end of a dialog service you can output a format from a program unit This format can be used by the terminal user at the start of the next service.
- **Format request using KDCFOR**

The user at the terminal can use the KDCFOR user command to request a basic format. openUTM will then output the desired format. You cannot use KDCFOR for #formats.

In order to start a service by entering a format you have to transfer the desired transaction code together with the message. You can do this in the following ways:

- In the format, the first input field is an 8-character field into which the user enters the desired transaction code. Note that this field (in +formats including attributes) is not transferred to the message area. (Exceptions: #formats, BADTACS event service or if the INPUT exit was used to make other specifications). If the transaction code field contains blanks, the string up to the first blank is interpreted as the transaction code. If you use addressing aids to structure the input area, you must take account of this truncation of the transaction code.
- The format permits the transaction code to be entered at any other specified location. The input is evaluated using the input exit and the transaction code is extracted.
- The transaction code is assigned to a function key at generation, see KDCDEF statement SFUNC in the openUTM manual "Generating Applications", and the user presses this function key.
- The function key must be an F-key because messages are not passed when the K-keys are used (see also the KDCDEF statement SFUNC).
- The format contains one or more UTM control fields. In a control field, the transaction code is either entered by the user or is already preset. The "UTM control field" attribute is assigned when the format is created.

i If you use basic formats to start the service, you must always check the KCRMF/kcrfn field in the first program unit in order to determine whether the intended format was used to start the service.

4.1.3 Using partial formats (BS2000 systems)

A screen display may consist of multiple partial formats. A partial format normally occupies a part of the screen only. You must enter a separate MPUT NT call for each partial format. If the screen is to be read again, a separate MGET call is required for each partial format.

4.1.3.1 Output formatting with partial formats (BS2000 systems)

If a new screen is constructed of two or more partial formats, you must also specify the value KCREPL in the KCDF field of the first MPUT NT. In all subsequent MPUT calls KCDF must contain a binary zero. Otherwise, openUTM terminates the conversation abnormally, setting KCRCCC = 70Z and KCRCDC = K606.

You cannot mix format mode and line mode within a dialog message: If the format changes from line mode to format mode or vice versa within a partial message, the service is terminated with KCRCCC=75Z.

You may switch between *formats and +formats.

Updating a screen

You can update a screen with one or more MPUT NT calls. In the first MPUT call you can specify any value except KCREPL in the KCDF field since KCREPL is used to erase the entire screen. In subsequent MPUT NT calls KCDF must be set to binary zero as for setting up a new screen.

If the format is changed, openUTM only erases those old partial formats which are overlapped by new ones.

You can use the screen output function KCERAS to erase the variable fields when outputting a partial format.

Outputting partial formats with FPUT/DPUT NT

You can use FPUT/DPUT NT to output individual partial formats. However, you cannot construct a screen with multiple FPUT/DPUT NT calls, since openUTM transfers each partial format sent using FPUT/DPUT NT as a separate message when outputting to the screen. You may switch between format mode and line mode.

Before a formatted asynchronous message is output the screen is automatically cleared. It is therefore not possible to use FPUT/DPUT NT to update the displayed format.

openUTM responds with an automatic screen restart to inputs from asynchronously output formats - with the exception of command entries (see section [“Screen restart”](#)).

If you output to printers, all message segments sent with FPUT/DPUT NT are combined and output as one message, even when you change between format mode and line mode.

4.1.3.2 Input formatting with partial formats (BS2000 systems)

The terminal user can enter data in the partial formats, but is not required to enter data in every one.

Since openUTM passes all variable fields, after the INIT call the KCRMF/kcrfn field contains the name of the first partial format containing variable fields. After the MGET call KCRMF/kcrfn contains the name of the next partial format with variable fields. After the last partial format with variable fields has been read KCMF = KCRMF (kcrfn=kcrfn). If you try to read another partial format, although the message has already been entirely read, openUTM responds with the return code 10Z.

Example

In the preceding program unit run there was an MPUT output with the 3 partial formats: PARFOR1, PARFOR2, PARFOR3; variable fields are present only in PARFOR1, PARFOR2

KDCS call:		Returned by openUTM:
INIT		KCRMF = PARFOR1
MGET	KCMF = PARFOR1 KCLA = ...	KCRMF = PARFOR2 KCRCCC = 000 KCRLM = ... Data in message area
MGET	KCMF = PARFOR3 KCLA = ...	KCRMF = PARFOR2 KCRCCC = 03Z (as KCMF contains a value other than that returned in KCRMF by the preceding MGET) KCRLM = 0
MGET	KCMF = PARFOR2 KCLA = ...	KCRMF = PARFOR2 KCRCCC = 000 KCRLM = ... Data in message area
MGET	KCMF = ... KCLA = ...	KCRMF = PARFORF2 KCRCCC = 10Z KCRLM = 0

Entering a format consisting of multiple partial formats to start a service

If you want to start a service by entering a format consisting of multiple partial formats you can use the first variable field of the first partial format to specify the transaction code (for other options, see "[Using partial formats \(BS2000 systems\)](#)").

openUTM then automatically separates the field with the transaction code from the message: for *formats the first 8 characters (transaction code) are removed in the first partial format, for +formats the first 10 characters (attribute field and transaction code). The other partial formats remain unchanged.

An asynchronous service can also be started using a format consisting of multiple partial formats which was output at the end of a dialog service. The asynchronous program must be written in the same way as the dialog version: the INIT call provides the name of the first partial formats with variable fields in KCRMF/kcrfn. Using FGET the program can retrieve the input data from this partial format. In the case of an empty input message (transaction code without data), the FGET call returns 10Z to the program unit.

4.1.4 Message flow for formatted messages (BS2000 systems)

The following diagram displays the message flow in the event of an MPUT call to a terminal:

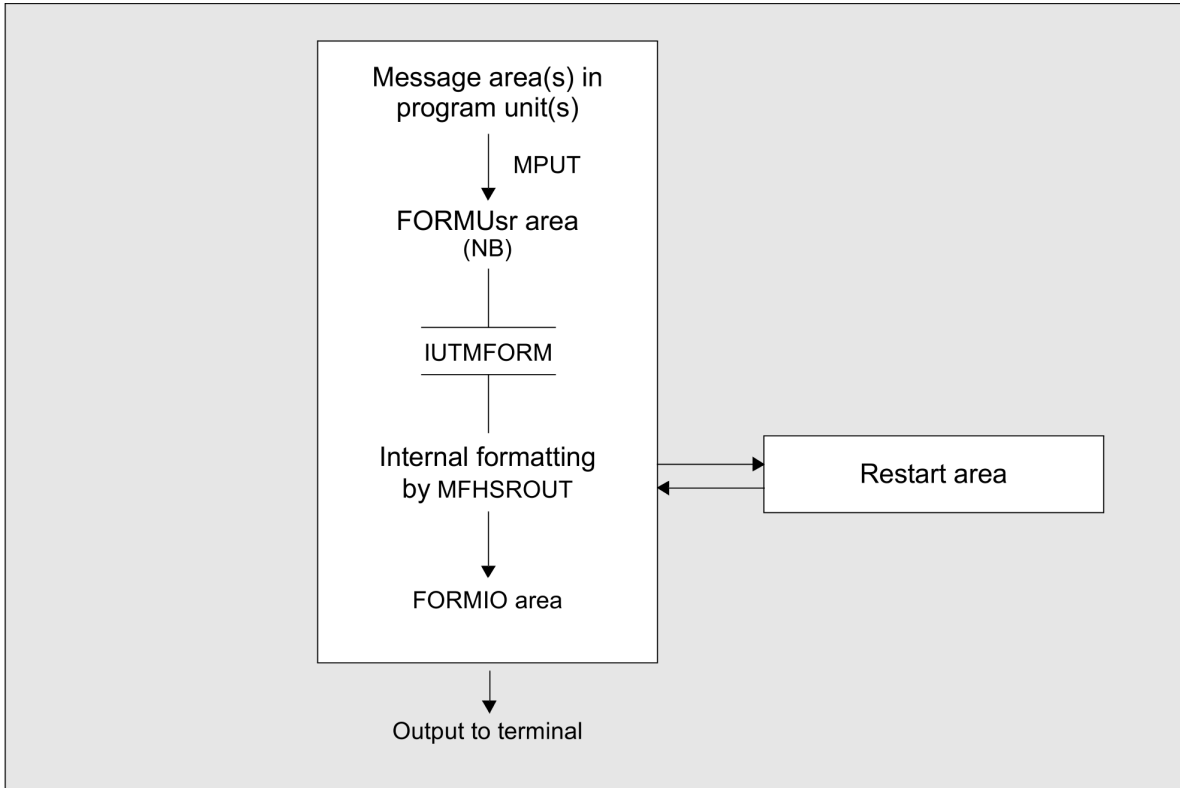


Figure: Message flow for MPUT to terminal

The messages from the program units enter the FORMUSR area via UTM buffers at MPUT time. The size of this area, which must be able to contain the entire logical message, is defined in the NB parameter of the MAX statement (see the openUTM manual “Generating Applications”). This message is formatted by the FHS formatting system MFHSROUT and stored in the FORMIO area. This message is sent to the terminal.

If partial formats are used, you have to make sure that the FORMUSER area is always able to store the entire message.

Input formatting

With input formatting, the message stream runs in the opposite direction, using the same areas.

4.1.5 Outputs on printers in format mode (BS2000 systems)

Formats can also be output at printers. Refer to the manual for your formatting system for information about the supported printer functions.

In the KCMF/kcfn field of the KDCS parameter area, you enter for the FPUT/DPUT call:

*format_name | +format_name | #format_name

where:

- * Formatting without the option of changing the attribute
- + Formatting with the option of changing the attributes of individual format fields
- # Formatting with the option of both changing the characteristics of individual format fields and changing the global characteristics of the format fields

The formatting system must support the printer models as they are known in the VTSU-B or as they were generated for RSO (for PTYPE=*RSO).

If you use the FORMAT event exit for printouts, you have to consider the following:

- you do not have to set the restart area
- you have to request the print out confirmation in the message header
- you have to enter the confirmation bytes transferred by openUTM in the message header
- you ascertain the formatting specifications, such as format name, device type, etc. from the KB header and the parameter area of the FORMAT event service.

For the structure of the message header, refer to your printer manual.

Form feed

Whenever FPUT/DPUT is called, including in the case of message segments with FPUT/DPUT NT, the form feed depends on the contents of the KCDF field in the KDCS parameter area (exception: when #Formats are used):

KCREPL Form feed before printing, i.e. the format is printed starting at the basic form setting specified at the printer.

other No form feed, i.e. the format is printed starting at the next line (also for the first FPUT/DPUT).

This allows you to concatenate formats in order to print large forms, independent of any length limitations. However, the physical message segment must be shorter than:

- the BCAM letter length (see TRANSDATA manual "Generating a Data Communication System"), and
- the device-specific length that is supplied by VTSU-B when a connection is established.

4.2 Controlling the output in line mode (BS2000 systems)

openUTM operates in line mode whenever the name specified in KCMF/kcfn starts with a blank. In line mode, openUTM also enables you to use the following options to control the screen output:

- use logical control codes to structure the output
- In addition to the screen output functions KCALARM, KCREPR and KCRESTRT that can be used in format mode (see "[Screen output functions in format mode \(BS2000 systems\)](#)"), in line mode it is also possible to use the screen output functions KCCARD and KCEXTEND (extended line mode).
- use of edit profiles

For a description of how to prepare messages for printing, refer to section "[Output to printers](#)".

Using logical control codes for structuring

In line mode you can use logical control codes to structure the output. The VTSU (Virtual Terminal Support) terminal support facility then converts the control codes into the physical control codes necessary for the addressed device. You can use all logical control codes permitted by the TIAM access method, see the "TIAM User Guide". In some programming languages data structures are available which you can copy into the program (see the "TIAM User Guide").

KCCARD screen function

You can use the KCCARD screen function to input data via magnetic strip cards:

If you use the KCCARD screen function to output a dialog message, the keyboard is locked and the terminal user is requested to insert a magnetic strip card into the ID card reader.

KCEXTEND screen function

If you use this screen function the output fields are set to a particular, predefined value which is equivalent to the macro WRTRD, ... EXTEND=YES. All output fields are displayed in half video and protected by default, see the "TIAM User Guide" for further information.

Edit profiles

An edit profile is a set of attributes used for output in line mode. Using edit profiles you can, for example, specify that characters entered at the terminal are not to be displayed (password entry) or request lower case to upper case conversion. Alongside the KCCARD screen function edit profiles are another way of requesting input from ID card readers. You can also perform other screen functions such as, for example, KCREPR.

You use the KDCDEF statement EDIT to specify the name and attributes of edit profiles at generation (see the openUTM manual "Generating Applications"). The length of the name can be up to 7 characters. You can use the MPUT/FPUT/DPUT calls to address an edit profile in a program unit. To do this, enter a blank in the first byte of the KCMF/kcfn field and the name of the edit profile in the remaining seven bytes.

Edit profiles are handled like format names, i.e. the name of the edit profile of the last output message is returned in the KCRMF/kcrfn field after INIT (as with format identifiers). If you use MGET/FGET calls the name is entered in the KCMF/kcfn field.

Note the following points when edit profiles:

- When using MPUT, FPUT or DPUT calls with edit profiles, no screen function may be specified (KCDF must be set to binary zero) as otherwise openUTM responds to MPUT with 70Z or to FPUT/DPUT with 40Z.

-
- As soon as edit profiles are generated for an application, you must use 8 blanks in KCMF/kcfn to identify messages in line mode (without edit profile); it is not sufficient to fill set the first byte with blanks, since openUTM interprets this as an incorrect format identifier and sets the corresponding error code in KCRCCC.
 - If you use MPUT NT, FPUT NT or DPUT NT to issue multiple message segments to a terminal, the name of the edit profile must not change, otherwise openUTM responds to MPUT with 75Z and to FPUT/DPUT with 45Z. When issuing partial messages to printers edit profile names may change.
 - If the screen was overwritten by the output of an asynchronous message, openUTM performs an automatic KDCCDISP on the next input when using edit profiles.
 - For messages to UPIC clients the names of the edit profiles are treated like format identifiers, i.e. they are also passed (therefore they also appear in the UTM program unit in KCRMF/kcrfn), although they do not have any effect.
 - For messages via distributed processing the names of the edit profiles are processed like format identifiers:
 - In distributed processing via LU6.1 the names of the edit profiles are transferred (i.e. they appear in KCRMF/kcfn). However, they have no effect.
 - In distributed processing using OSI TP, no edit profile must be specified in KCMF/kcfn, since openUTM uses field of the the format identifier to transfer the abstract syntax.

4.3 Output on printers in line mode

If you want to output in line mode, the first byte in the KCMF/kcfn field of the KDCS parameter area must be a blank.

In line mode, the message may contain all logical control characters, e.g. for form feed or line feed. You can define these control characters yourself in the program unit and in this way structure the text for the print-out yourself.

On BS2000 systems you can also use edit profiles to present/prepare the messages (see also section [“Controlling the output in line mode \(BS2000 systems\)”](#)). You enter the name of the edit profile in KCMF/kcfn starting at the second byte.

i A message terminated by FPUT/DPUT NE is always printed as a separate message. In the case of cut sheet printers, the program must allow users to change sheets themselves for output in line mode (form feed) since the device cannot recognize the end of sheet itself.

4.4 Screen restart

openUTM automatically restarts the screen for terminals in the following cases:

- If a screen output took place at the last synchronization point in a service and the user has signed on at the application again following the interruption to the service, e.g. after:
 - the application has been terminated normally without terminating the service
 - the application has terminated abnormally
 - KDCOFF within a service
 - connection loss

This screen restart is only performed when the user signs on again if the user ID or, in applications without user IDs, the LTERM partner, was generated with restart.

To do this, you set the operand RESTART=YES in the USER or LTERM statements at generation (see openUTM manual "Generating Applications").

Following the end of an application then, **in the case of standalone UTM applications**, a screen restart is only possible in UTM-S applications.

- during a service, an asynchronous message was output to the screen and the user did not issue a KDCDISP command to continue the dialog, i.e. the user attempts to input the message into the asynchronously output screen content (only command entries are possible).
- within a service, after a follow-up transaction has been rolled back by MPUT RM, KCDF = KCRESTRT and PEND RS and screen output has taken place at the last synchronization point in the service.
- when certain operating errors occur on BS2000 systems (e.g. terminal switched on or off, AM key).

Screen restart is only possible because openUTM stores the data on the last screen structure, initially in a buffer in the process-specific system storage area. At the end of the transaction, openUTM writes this information to the restart area in the page pool of the KDCFILE, see also the openUTM manual "Generating Applications".

When formatting output on BS2000 systems, openUTM writes the entire screen contents to the restart area if the entire screen is to be restructured (KCDF= REPLACE, change of format). During a screen update, only the fields which are also overwritten at the terminal are updated in the restart area. Similarly, during input formatting only the fields received from the terminal are updated in the restart area.

If you use a formatting system on a BS2000 system, openUTM automatically performs the setup, modification and storage of the restart area in interaction with the formatting system. However, if you use -formats and write the formatting routine yourself, openUTM will save the restart area, but the setup and modification of the area are the responsibility of the formatting routine programmed by you (see chapter "[Event exit FORMAT \(BS2000 systems\)](#)").

4.5 Format names for message exchange with UPIC clients

Program units that are written for the formatted dialog with terminals can also be used for the dialog with UPIC clients without any changes. In this case, however, a formatting system is not called. Net messages or message segments and format names are exchanged between openUTM and the UPIC client. openUTM functions in the same manner when reading the message as when reading segment formats, i.e. if an incorrect format identifier was specified for MGET, then openUTM sets the return code to 03Z, returns the correct format identifier in KCRMF/kcrfn and sets KCRLM to 0. Nothing is entered in the message area.

The UPIC client can then set up the screen interface based, for example, on the format name.

It is also possible to position the cursor in a program using "KDCSCUR" when outputting a message to the UPIC client.

A UPIC client can pass the value of a function key to a UTM application so that the return code generated for this function key is triggered when an MGET is executed in the program unit (see the SFUNC statement generation, RET parameter).

See the manual „openUTM-Client for the UPIC Carrier System” for more detailed information.

5 Program structure in distributed processing

The term "distributed processing" applies to all types of processing where server applications with the same authorization levels interact (server/server communication). openUTM supports distributed processing via the OSI TP, LU6.1 and LU6.2 protocols. Partners of a UTM application for distributed processing can be other UTM applications, OpenCPIC applications or applications that are based on transaction systems from other manufacturers.

The program interfaces for the communication via LU6.2 are identical to those for the communication via OSI TP. You will need the openUTM-LU6.2 product to communicate via the LU6.2 protocol; .

When using the OSI TP protocol you can decide whether or not openUTM is to operate with global transaction management.

openUTM is designed to operate with global transaction management when the LU6.1 is used, i.e. the transactions of all participating partners are synchronized.

Client/server communication is not regarded as distributed processing, despite the fact that the client performs processing tasks in client/server communication, e.g. plausibility checks. However, fixed client and server roles are assigned. The client does not make services available which could be used by other applications.

Communication with UTM client applications with OpenCPIC carrier system is done via the OSI TP protocol; this means that all statements and rules that are agreed upon in this manual for the communication with OSI TP partners are valid for these partners, even when a client of a UTM application is implemented with an OpenCPIC application.

5.1 Addressing remote services

Before you can send a message to a remote service, you must first address this remote service. To do this, use the **APRO** (Address **PRO**gram) call.

In distributed processing you can use the functions of both remote services and, by using openUTM's message queuing functionality, asynchronous services. You use **APRO DM** (Dialog **M**essage) to address remote dialog services. and **APRO AM** (**A**synchronous **M**essage) to address asynchronous services.

If a remote service is addressed in a transaction with APRO AM/DM, then a message must also be sent to the remote service in the same transaction.

Under certain circumstances you can also use APRO AM to address a dialog service via OSI TP, i.e. to address an asynchronous job to a dialog service (see "[Job receiver side](#)").

The following APRO call parameters are of relevance when a remote service is addressed:

- In the **KCRN** (**R**eferenced **N**ame) field, enter the LTAC name of the remote service. The LTAC name (Local TransAction Code) is the name under which the remote service is known in the configuration of the local application. The LTAC name is assigned at generation.

If this LTAC name is already associated with a fixed partner application in the configuration you only have to specify the name for the APRO call to unambiguously determine the remote service. This is called single-step addressing. Single-step addressing is always advisable in cases where there are no alternative partner applications, e.g. because the requested service is only available from one partner application.

In two-step addressing, the partner application is specified explicitly when calling APRO:

- The **KCPA** (**P**artner **A**pplication) field is used to specify the (OSI-)LPAP name of the partner application in two-step addressing. The (OSI-)LPAP (Logical Partner APplication) name is the name by which the partner application is known in the configuration of the local application. The (OSI-)LPAP name is assigned at generation. The name of a MASTER-LU61-LPAP or a MASTER-OSI-LPAP can also be specified in the KCPA field.

Two-step addressing is always advisable in cases when the requested service is available from multiple partner applications. Which partner application is selected depends on the particular situation.

If you specify the (OSI-)LPAP name of a partner application in KCPA, although the LTAC name specified in KCRN is already assigned to a partner application in the configuration, then the specification in KCPA takes precedence over the configuration assignment.

-
- In the **KCPI** (Partner Identification) field, you assign an identification to the remote service for the duration of the interaction. This identification, also called the service ID, is freely selectable. However, the first character must be ">". The scope of the validity of the service ID is the local service; in other words, if two services use the same service ID at the same time, they are thus addressing different remote services. You have to specify this identification in the KCRN field for all communication calls to the addressed service. When interaction with the remote service terminates, you can use the service ID in further APRO calls to identify the same service or other services.

For the following calls you have to specify the service ID in the KCRN field:

- MPUT calls to send dialog messages to the remote service
- FPUT/DPUT calls to send asynchronous messages to the remote service
- MGET calls to read dialog messages or status information from the remote service
- MCOM BC calls to start a job complex whose basic job is directed to the remote service
- CTRL calls to control OSI TP dialogs

5.2 Distributed dialogs

The rule of strict dialog also applies to distributed processing, i.e. in communications between two partners, after a message to the partner you have to receive a response before you can send another message to this partner.

The period between receiving a dialog message and sending the next dialog message is called a **processing step**. The next message may either be a response, in which case the processing step is equivalent to a **dialog step**, or a message to another partner.

A job submitter can simultaneously interact with multiple job receivers. The next programming step in the job submitter only starts when all the responses have been received from the job receivers. A separate program unit run is generally started for each processing step (exception: PGWT).

The job-submitting service can be either a dialog service or an asynchronous service.

Exchange of dialog messages

You use MPUT to send and MGET to receive dialog messages between partner services in the same way as with dialog messages without distributed processing.

If a job-receiving service exchanges messages with a job submitter it behaves as if it were communicating with a terminal: you have to enter blanks in the KCRN field when using MGET and MPUT.

When exchanging messages with a job receiver, a job-submitter service must specify the service ID of the job receiver in the KCRN field (see "[Addressing remote services](#)").

5.2.1 Controlling communication in the program

In distributed processing, multiple program units in various partner applications are used to process a job. A program unit can be addressed by a client (terminals or client programs), from the application's own programs or from other applications. The program unit has therefore to decide independently from the partner which task to process, to whom it sends a message, and whether or not it has to terminate a distributed processing.

For this reason, openUTM provides a range of information about the communication partner and the current communication status. This information can be evaluated and used for communication control. For a description of this information refer to the sections "[Programming aids](#)" for LU6.1 and "[Programming aids](#)" for OSI TP.

5.2.2 Error handling by the program unit

There are two situations in which a program unit can respond to errors:

- In the case of less serious errors:
The program unit retains control and can react with a programmed rollback (see below).
- After a service restart:
The program unit is restarted, receives status information and possibly a rollback message and can respond to the error situation.

5.2.2.1 Programmed rollback

If less serious errors occur, the program unit retains control and can roll back the distributed transaction with PENDING RS or PENDING ER/FR, or the local transaction with RSET. If communication is via OSI TP transactions can also be rolled back using PGWT RB, see "[Particularities of rollback and restart](#)".

The comments below apply to distributed processing with global transaction management, i.e. for LU 6.1 and for OSI TP with functional unit commit. The effect of these calls in the case of OSI TP without functional unit commit is described on "[Particularities of rollback and restart](#)".

PENDING RS

PENDING RS can be called in a job-submitting or job-receiving service.

In a distributed transaction, a PENDING RS has the following effect:

With PENDING RS, all the services participating in a distributed transaction are rolled back to the last synchronization point. As opposed to the PENDING ER/FR call, with PENDING RS a service remains open if it has already reached a synchronization point. Services which have not yet reached a synchronization point are terminated.

The following situations are possible:

- PENDING RS in the first transaction of the uppermost job-submitting service.
All participating services are terminated without any service restart. Chained services are restarted after the rollback.
- PENDING RS in the first transaction of a job-receiving service
The job-receiving service is terminated. If the uppermost job-submitting service has already reached a synchronization point, openUTM executes a service restart (with the message K034 to the terminal). The job-submitting service receives status information (service status "R" / "Z" and transaction status "R") which you read using MGET NT.

-
- PENDING RS in a follow-up transaction of the job-submitting service or job-receiving service.

In this case a rollback message has to be sent with MPUT RM prior to the PENDING RS, otherwise openUTM aborts the service with KCRCCC = 83Z. The rollback message goes to the follow-up program unit specified at the last synchronization point of the (local) service. After the rollback openUTM executes a service restart. The form this takes depends on the destination of the output message at the last synchronization point and on who called PENDING RS:

- In the case of an **output message to the client** the service restart begins in the job-submitting service.
 - If PENDING RS was issued in the uppermost job-submitting service, then a screen restart is executed (as without distributed processing).
 - If PENDING RS was issued in a job-receiving service, then a screen restart is executed and the message K034 output. The next entry from the client is read by the follow-up program unit of the last synchronization point. If a follow-up program unit sends a new message to the job receiver (which executed PENDING RS), then this job receiver first reads the rollback message and then the message sent to it. If job-receiving services are terminated by the rollback (i.e. the job receiver was also a job submitter), then you also have to read the associated status information using MGET NT.

In the case of LU6.1, follow-up processing in the job-receiving service does not start until a message is present for this service. If the job receiver is not included in the next transaction after the rollback, this may not take place until a later follow-up transaction.

In the case of OSI TP, the follow-up program unit runs from the last synchronization point in the job-receiving service which called PENDING RS and always runs in the next transaction: The program is started if a message is received from the job submitter or if the job submitter has requested end of transaction.

- With an **output message to a service**, openUTM starts the follow-up program unit specified at the last synchronization point. This program unit has to read the rollback message; subsequently the output message can be read; status information from the job-receiving services may be present, too. If the (uppermost) job-submitting service participated in the rolled back transaction, then openUTM issues message K034.

Programmed PENDING ER/FR

In distributed transactions, the effects of the PENDING ER and PENDING FR calls are identical; however PENDING FR does not, in contrast to PENDING ER, generate a DUMP. PENDING FR enables you to respond to errors other than programming errors (e.g. meaningless data).

The effect of PENDING ER or PENDING FR differs in the job-submitting and the job-receiving services:

- If PENDING ER/FR is issued in the job-submitting service, this and all job-receiving services are terminated with PENDING ER/FR.
- If issued in the job-receiving service, only this service is terminated and the distributed transaction is rolled back to the last synchronization point. The service restart then begins at this synchronization point and the next program started receives status information from the job-receiving service which called PENDING ER/FR. If the job-submitting service has not yet reached a synchronization point, it is also terminated by a PENDING ER/FR.

If the preceding distributed transaction was terminated in the job-receiving service, the follow-up program unit specified at the last synchronization point is started in the job-submitting service.

If the job-receiving service wishes to terminate with PENDING ER/FR, it first has to execute an MPUT, otherwise PENDING causes it to be terminated by the system with KCRCCC = 83Z (service status Z instead of E). Exceptions to this rule are dialogs via OSI TP in which an MPUT to the job submitter is not permitted (KCSSEND=N). The job-submitting service always receives status information which has to be read with MGET NT.

RSET

The effect of the RSET call is the same in job-submitting and job-receiving service.

After a RSET call in a program unit run belonging to a distributed transaction, the behavior of openUTM depends on the RSET generation parameter of the UTMD statement.

- If RSET = LOCAL is generated, openUTM allows the RSET call merely to roll back the local transaction. Please note that the data environment (GSSBs, LSSBs, TLSs, ULS,...), with the exception of the SPAB, is rolled back to the last synchronization point. The following applies to job-receiving services addressed within the transaction: if a message was sent to a job-receiving service in a preceding dialog step terminated with PEND KP or PGWT KP, then this service remains addressed, otherwise the service identifier is deleted.
- If RSET = GLOBAL is generated, the program unit run must be terminated with PEND FR/ER/RS. This then causes the distributed transaction to be rolled back.

5.2.2.2 Error handling after service restart

If the distributed transaction has to be rolled back, service restart tries as far as possible to restart the program for which there was a message at the end of the last distributed transaction, or to which the next input from the client is directed. The programming rules (see "[Programming rules and recommendations](#)" for LU6.1 and "[Programming rules for dialogs without the functional unit commit](#)" for OSI TP) ensure that one and only one message exists for the client or for a program in a service at the end of a distributed transaction.

The program unit can tell from the service ID in the KCKNZVG/ kccv_status field in the KB header if a service restart has occurred: after a service restart this field has the value "R".

If the service restart occurs in the job-submitting service, the program unit normally receives **status information** from the job-receiving service if the job-receiving service caused the rollback and is or was consequently terminated. Such status information is read with **MGET NT**; it is a message of length 0 and provides the service and transaction status of the job-receiving service in the KCVGST/kcpcv_state and KCTAST/kcpta_state fields in the KB return area (see "[Programming aids](#)").

There are 3 different cases with service restart:

1. There was a message for the client at the last synchronization point.
The follow-up program unit in the job-submitting service can now read the new input from the client with MGET and receives as status information the service status O and the transaction status C.
If the rollback of the transaction was caused by an error in a job-receiving service and the job-receiving service was subsequently terminated, the KCRPI field receives the service ID of the service which caused the rollback. Status information from this service can then be read with MGET NT and KCRN = service ID.
2. There was a message at the last synchronization point from a job-receiving service to a job-submitting service.
The follow-up program unit in the job-submitting service can now use MGET as usual to read the message, and additionally receives the service and transaction status of this job-receiving service.
If this job-receiving service was rolled back and terminated by an error, you only receive the corresponding status information. If the rollback was caused by another job-receiving service, you receive the transaction status C as status information with the first MGET. Subsequently more status information can be read, as in case 1.
If the message cannot be sent by the job-receiver (see next section), then you just receive status information from the job-receiving service.
3. There was a message at the last synchronization point from a job-submitting service to a job-receiving service.
If possible, the follow-up program unit is then started in the job-receiving service.
If the follow-up program unit cannot be started (e.g. because the application was terminated and not restarted within the generated wait time or because the service terminated with PEND ER), then the follow-up program unit in the job-submitting service is started and receives status information.

There is status information from all job-receiving services which caused rollback of the distributed transaction and which were or are being terminated.

If, after a service restart of the job-submitting service, a job-receiving service is addressed again and an error recurs, the job-submitting service can be rolled back more than once to the same synchronization point. Since the status information from the preceding rollback is retained, it is possible to have multiple status information.

If there is multiple status information, then with each MGET you receive the service ID of the next service with status information. Status information from several job-receiving services has to be read in the order proposed by openUTM (KCRPI). The KCMF/kcfn field is to be set with blanks when reading the status information.

If a remote service in the rolled back transaction is newly created by the APRO call, then there is likely to be status information from it although this service does not actually exist at the synchronization point from which the restart begins.

No message from job receiver

There are two reasons why a job-receiving service cannot send a result to the job submitter service:

1. The job receiver was not started for one of the following reasons:
 - no logical connection to the application of the job receiver exists and no connection could be established during the generated wait period
 - no session or association to the application of the job receiver could be reserved during the generated wait period
 - the job was sent to the application of the job receiver. However, the transmitted transaction code is unknown or locked
 - The application of the job submitter is terminated using KDCSHUT W
2. The job-receiving service was started, but errors have occurred during processing of the job-receiving service or the communication path was disturbed. For this reason the transaction was rolled back in the job-receiving service and the job-receiving service has been terminated. Additionally, the session/association to the job-receiving service which terminated through error has been released. The following error situations can occur:
 - no response has been received by the application of the job submitter from the job-receiving service within the generated wait period
 - the application of the job receiver has been terminated abnormally because of a severe error
 - the job-receiving service has terminated using PEND ER or was terminated because of a severe program error.

5.2.3 Load distribution using LPAP bundles

openUTM provides the LPAP bundle function for the OSI TP and the LU6.1 protocols.

LPAP bundles allow load distribution and the use of alternative connections to a partner application. If a UTM application has to exchange a very large number of messages with a partner application then load distribution may be improved by starting multiple instances of the partner application and distributing the messages across the individual instances. In an LPAP bundle, openUTM is responsible for distributing the messages to the partner application instances. An LPAP bundle consists of a master LPAP and multiple slave LPAPs.

The slave LPAPs are assigned to the master LPAP on generation. In normal circumstances, the physical connections (CONs) of the individual slave LPAPs address different partner applications.

Operating an application

To allow openUTM to distribute the messages to the slave LPAPs, you address the messages to the master LPAP in the program units.

openUTM distributes these messages to the slave LPAPs in sequence. The system always attempts to find a slave LPAP via which the message can also be sent, i.e. to which a connection is established and for which, for instance, the queue level has not yet been exceeded.

For more details on this, refer to the description of the APRO call on "[APRO Address job-receiving service](#)".

Administration

The "Master LPAP" and "Slave LPAP" properties are displayed via the administration interface.

All the slave LPAPs are displayed for a master LPAP and the master LPAP is displayed for a slave LPAP.

Using the administration facilities, you can set the status of master LPAPs to ON or OFF. If you change the status of a Master LPAP, this causes the status to be changed accordingly on all slave LPAPs.

5.3 Distributed dialogs via LU6.1

The LU6.1 protocol (**Logical Unit 6.1**) is a SNA protocol defined by IBM. It has been continuously developed and has become the industry standard. Communication is performed with transaction management over multiple applications.

In addition to using LU6.1 to connect UTM applications, you can also connect UTM applications with CICS and IMS applications running on IBM computers.

The sections below explain the programming aids provided by openUTM for distributed processing, the rules for these dialogs and how you can use existing program units as an LU6.1- job submitter.

5.3.1 Programming aids

openUTM makes a range of information available to program units. You can evaluate and use this for communication control:

- after the INIT call
- after using MGET to read the dialog message

After the INIT call, you can ascertain the following from the communication area:

- the user ID or session name under which the program unit was started (KCBENID/kcuserid field)
- the communication protocol used by the partner (1 is entered in KCVGST/kcpcv if LU6.1 is used)
- whether it is a service restart (KCKNZVG/kccv_status is then set to "R").

After the MGET call, openUTM returns the status of the partner service in the KCVGST/kcpcv_state field and the status of the partner transaction in the KCTAST/kcpta_state field.

For COBOL, a higher-ranking status field KCRST is defined which contains the KCVGST and KCTAST fields.

Using these stati you can, for example, ascertain whether the partner service has already requested end of transaction and is waiting for the termination of distributed processing. This feature can be used to control the program run and ensure that the programming rules are observed, even in situations where the exact security processes used by the partner are not known. On the other hand, it also allows the job-submitting service to react to errors in the job-receiving services.

Service status of the partner

KCVGST/ kcpcv_state	Meaning
I	(inactive): The service is inactive, i.e. it has not yet been started or it has not been possible to start it, e.g. because the TAC is unknown in the partner application.
O	(open): The service is open.
C	(closed): The service terminated with PEND FI.
R	(rolled back): The service has been terminated by the program with PEND RS.
E	(error): The service has been terminated by the program with PEND ER/FR.
Z	The service has been terminated by openUTM because of an error.
T	(timeout): The service has been or is terminated incorrectly, as no response has been received within the specified wait period or it has not been possible to reserve a free session within the specified wait period.

Transaction status of the partners

KCTAST/ kcpta_state	Meaning
I	(inactive): There is no transaction because no service exists.
O	(open): The transaction is open; the last dialog step has been terminated with PEND KP.
P	(prepare to commit): The service has requested end of transaction, but the distributed transaction has not yet terminated. In this situation the service waits for an acknowledgment which it receives as soon as the distributed transaction is terminated. Just as with PEND KP, the resources (GSSB, TLS) remain locked until that point.
C	(closed): The last distributed transaction in which the service participated is terminated.
R	(rolled back): The distributed transaction and thus also the local transaction have been rolled back.
M	(mismatch): The services participating in a distributed transaction cannot agree on a common synchronization point for service restart. This can only occur with a timeout or after termination and start of a UTM-F application.

5.3.2 Programming rules and recommendations

The following sections explain the rules which have to be observed when using distributed dialogs via LU6.1. If you follow the suggested "[programming recommendations](#)" in the final section the presented rules are automatically observed.

i Note that PGWT CM and PGWT RB calls are not permitted in distributed dialogs via LU6.1.

Effect of PEND calls and rules for usage

The PEND calls in job-submitting **and** job-receiving services control the distributed transaction, i.e. they decide when the **common** synchronization point of the two transactions is to be set.

Which PEND calls a service may use and their effect depends on the service and transaction status of the partner service.

The following table describes the effect of the PEND calls in the job-receiving and job-submitting services and the rules for how to use them:

Variant	Effect / rule of usage
PEND KP PGWT KP	<p>No synchronization point is requested and no synchronization point is set. The service remains in transaction status "0" and in service status "0". An open DB transaction remains open. The follow-up program unit specified in KCRN is started in the job-submitting service as soon as all results from the job-receiving services have been received.</p> <p>This is permissible if the program unit sends a message to the terminal or the client (LTERM partner) or if the message is addressed to a partner service and this does not have transaction status "P".</p>
PEND RE	<p>End of transaction (synchronization point) is requested. End of transaction (synchronization point) is requested. If all partner services already have transaction status "P" (i.e. they have already requested end of transaction), then the end of transaction is executed by all participating services, i.e. a common synchronization point is set. If a partner service is not in transaction status "P", the local service passes to transaction status "P" and waits for the partner service to request end of transaction, too. The follow-up program unit specified in KCRN is started in the job-submitting service as soon as all results have been received from the job-receiving services.</p> <p>Permissible in the two cases below:</p> <ul style="list-style-type: none">• no partner service with an open transaction exists.• there is exactly one partner service with an open transaction. The program unit sends a message to this partner. <p>If multiple partner services with open transactions exist then PEND RE is forbidden.</p>

Variant	Effect / rule of usage
PEND FI	<p>The effect is the same as with PEND RE, except that end of service is requested simultaneously. The service is terminated at the next synchronization point.</p> <p>This is permissible if no job-receiving services are open any longer, i.e. all job receivers must have issued PEND FI before the job submitter is permitted to issue PEND FI.</p>
PEND FC	<p>The effect is the same as with PEND FI, except that after end of service, the chained follow-up service is started immediately.</p> <p>This is permissible in job-submitting services only (never permitted in job receivers), and only if no further job-receiving services are open, i.e. all job receivers must have issued PEND FI before the job submitter is permitted to issue PEND FC.</p>
PEND PR PEND PA	No effect on the transaction.
PEND SP	The transaction is closed, i.e. a synchronization point is set and the dialog step is continued. Not allowed if there are partner services with open transactions.
PEND RS	With PEND RS all the services participating in the distributed transaction are rolled back to the last synchronization point. All services created in the distributed transaction are terminated by the rollback. Services which have reached at least one synchronization point remain open.

Programming rules

A set of rules has to be adhered to when programming distributed transactions. Violation of these rules leads to abortion of the service with (internal) PEND ER and KCRCCC=87Z.

These rules determine:

- how transactions and services have to be terminated when using distributed processing and
- where the output message may be sent.

Program unit runs, transactions and services are terminated as usual via the various PEND variants; of particular importance here are the PEND variants KP, RE, SP, FI and FC, and for error handling RS, ER and FR.

Using the variants KP, RE and SP you have to specify the follow-up program unit in KCRN, which is used to continue the service. You start this follow-up program unit with PEND KP/RE after all results from the job receivers have been received, or, if the message was addressed to the job submitter, after the next message is received from the job submitter. If you use PEND SP the follow-up program unit is started immediately.

The PGWT KP call may be used whenever a PEND KP is allowed.

The following rules hold for correct programming of a distributed transaction:

- **Service rule:**
 - a job-submitting service may only be terminated once all the associated job-receiving services have been terminated (with PEND FI). PEND FC is prohibited in job-receiving services.
 - After the PEND FI of the job-receiving service, the job-submitting service can terminate the subsequent dialog step with PEND KP, RE, SP, FI or FC. It may not send any more messages to this job-receiver service.

- **Transaction rule (single-level):**

a job-submitting or job-receiving service can terminate a dialog step either with or without end of transaction subject to the following restrictions:

- a job-submitting service **may not request end of transaction** if the transaction is open in the job-receiving service, and the output message is directed to the client
- a service **must request end of transaction** if the output message is directed to a partner service which has requested end of transaction.

With multi-level distributed transactions, i.e. when a job-receiving service is itself a job-submitting service or when a job-submitting service addresses several job-receiving services in one transaction, then the transaction rule is generalized as follows:

- **Transaction rule (multi-level):**

a service can terminate a processing step either with or without end of transaction subject to the following restrictions:

- a service **may not request end of transaction** if there is a partner service with an open transaction and the output message is not directed to this partner service. If multiple partner services with open transactions exist, it is never permitted to request end of transaction.
- a service **must request end of transaction** if the output message is directed to a partner service which has requested end of transaction

If a service has multiple partner services with open transactions, PEND RE, PEND FI and PEND SP are never permitted.

The tables "[Effect of PEND calls and rules for usage](#)", "[PEND variants in the job submitter](#)" and "[PEND variants in job-receiving service](#)" illustrate the situations when you can use the PEND call.

If you follow the "bottom-up strategy" described below, then the programming rules are adhered to automatically.

Programming recommendation: Bottom-up strategy

The bottom-up strategy is such that distributed transactions are always terminated from the bottom up, i.e.

- a job-receiving service always requests end of transaction before its job-submitting service and sends its output message to its job-submitting service, and
- a job-submitting service only requests end of transaction once all its job-receiving services have requested end of transaction. The output message then goes to its own job submitter.

PEND variants depending on the partner status

When using the PEND call must always consider the service status and transaction status of the partner service. Following MGET, openUTM returns the status information in the KCVGST/kcpcv_state and KCTAST/kcpta_state fields.

The cases illustrated in the following tables contain no new rules. They illustrate the rules described in the preceding sections.

PEND variants in the job submitter

The calls PEND PA and PEND PR are not included because they have no special features for distributed processing.

Partner status		PEND variants in the job-submitting service	
KCVGST/ kcpcv_state	KCTAST/ kcpta_state	permitted variants and their effect and limitations	
"O"	"O"	KP:	transactions in the job-receiving and job-submitting services remain open - default.
		RE:	requests end of transaction. Only permitted if the output message is addressed to this job receiver and no further partner with open transactions exist.
		RS:	rolls back the job-submitting and job-receiving transaction to the last synchronization point. Services in this transaction are terminated.
		ER /FR:	rolls back the distributed transaction; the job-receiving service is terminated.
"O"	"P"	KP:	only permitted if the output message is addressed to another partner service or another client; the transactions remain open (not recommended because of PTC state)
		RE:	terminates the distributed transaction.
		SP:	terminates the distributed transaction.
		RS:	rolls back the job submitter and job receiver transaction to the last synchronization point. Services in this transaction are terminated.
		ER /FR:	rolls back the distributed transaction; the job-receiving and job-submitting service are terminated

Partner status		PEND variants in the job-submitting service	
KCVGST/ kcpcv_state	KCTAST/ kcpta_state	permitted variants and their effect and limitations	
"O"	"C"	KP:	transaction in job-submitting service remains open.
		RE:	transaction in job-submitting service is terminated if the output message is addressed to the client, otherwise the service passes to transaction status "P".
		SP:	terminates the job submitter transaction.
		RS:	rolls back the transaction in the job-submitting service to the last synchronization point; services which started in this transaction are terminated.
		ER /FR:	terminates job-submitting and job-receiving service and rolls back the local transaction.
"C"	"P"	The output message must be addressed to another partner or the client or (with PEND SP/FC) to a follow-up program unit!	
		KP:	not recommended, since the job-receiving service waits in state PTC.
		RE:	terminates the distributed transaction and the job-receiving service.
		SP:	as RE
		FI:	terminates the distributed transaction as well as the job-receiving service and job-submitting service.
		FC:	as FI
		RS:	rolls back job-submitting and job-receiving service to the last synchronization point. Services which started in this transaction are terminated.
ER /FR:	terminates job-submitting and job-receiving service and rolls back the distributed transaction.		

Partner status		PEND variants in the job-submitting service
KCVGST/ kcpcv_state	KCTAST/ kcpta_state	permitted variants and their effect and limitations
"C"	"C"	the output message must be addressed to another partner or to the client or (with PEND SP/FC) to the follow-up program unit!
		KP: keep transaction in job submitter open.
		RE: terminates the transaction in the job submitter.
		SP: terminates the transaction in the job submitter.
		FI: terminates transaction and job-submitting service.
		FC: terminates transaction and job-submitting service.
		RS: rolls back the job submitter transaction to the last synchronization point.
		ER /FR: rolls back the transaction in the job-submitting service and terminates the job-submitting service. the job-receiving service is already terminated.

The combinations "KCVGST=O, KCTAST=C" and "KCVGST=C, KCTAST=C" cannot occur if you follow the "[bottom-up strategy](#)".

PEND variants in job-receiving service

The calls PEND PA and PEND PR are not included because they have no special features for distributed processing. The variant PEND FC is not permitted in job-receiving services.

Partner status		PEND variants in job-receiving service	
KCVGST/ kcpcv_state	KCTAST/ kcpta_state	permitted variants and their effects and limitations	
"O"	"O"	KP:	transactions in the job-receiving and job-submitting services remain open.
		RE:	job-receiving services passes to transaction status P.
		FI:	the job-receiving service changes to transaction status P. The service is terminated at the next synchronization point (=end of the distributed transaction).
		RS:	rolls back the distributed transaction to the last synchronization point. Services in this transaction are terminated.
		ER /FR:	rolls back the distributed transaction; the job-receiving service is terminated.
"O"	"P"	RE:	terminates the distributed transaction.
		SP:	terminates the distributed transaction.
		FI:	terminates the distributed transaction and the job-receiving service.
		RS:	rolls back the distributed transaction to the last synchronization point. Services in this transaction are terminated.
		ER /FR:	rolls back the distributed transaction; the job-receiving service is terminated.
"O"	"C"	KP:	permitted
		RE:	job-receiving service passes to transaction status P.
		SP:	job-receiving service passes to transaction status P.
		FI:	The service is terminated at the next synchronization point (= end of the distributed transaction).
		RS:	rolls back the distributed transaction to the last synchronization point.
		ER /FR:	rolls back the distributed transaction; the job-receiving service is terminated.

If the bottom-up strategy is adhered to, only the combination "O"/"O" can occur, see ["bottom-up strategy"](#).
Prior to a PEND RS in a follow-up transaction, you have to send a rollback message with MPUT RM, otherwise openUTM aborts the job-receiving service with 83Z.

5.3.3 Existing program units as LU6.1 job receivers

Provided that certain conditions are satisfied, you can use UTM program units, which were designed to communicate with terminals, unchanged as program units in a job-receiving service (see list below). Existing asynchronous programs can also be used as job receivers without any adaptations.

The same service can thus be used by terminals and client programs as well as by other services. In this way openUTM gives you considerable flexibility in application distribution.

If you want to use existing program units as job-receiving program units unchanged, or want to develop program units which can be used by terminals and client programs as well as by other services, you have to take account of the following points:

- Different return information in KB header

The communication partner of the job-receiving service is not the user at the terminal, but the job-submitting service. This is why the job-receiving service receives neither the ID of the terminal user nor the name of the LTERM partner in the KB header. (It is possible that neither are even generated in the application of the job-receiving service). Instead it receives the local session name (LSES name) and the local name of the partner application (LPAP name).
- Different assignments of TLS and ULS

Write and read calls for TLS in the job-receiving service refer to the TLS of the LPAP partner and not to a TLS of an LTERM partner. Similarly, calls for a ULS refer to the ULS of the session.
- Function keys are not supported in distributed processing

The job-submitting service cannot send a message corresponding to the function key to the job-receiving service. When using MGET the job-receiving service can therefore never receive the corresponding KDCS return code (19Z to 39Z).
- The card reader is not supported in distributed processing.

In a job-receiving service, the KCAUSWEIS/kccard field always contains blanks.
- No formatting in distributed processing via LU6.1

It is usually unimportant to a service whether it receives the dialog message from a terminal, an openUTM client program or from an LU6.1 partner. In the case of distributed processing via LU6.1, openUTM transfers the format ID specified in the job-submitting service with the MPUT call, but does not perform any formatting. The format identifier is also transferred with all message segments.

If you specify an incorrect format identifier in MGET, then openUTM operates when distributed processing via LU6.1 is used just like it does when segment formats are used for terminals: openUTM acknowledges an incorrect format identifier in MGET with the KDCS return code 03Z, and no messages or message segments are passed in the message area.
- Special structure of the job-submitting service (with distributed dialogs)

If existing program units of an application are to be used as program units in a job-receiving service, or if the job-receiving programs are programmed in such a way that they cannot evaluate the status indicators in the MGET call, the job-submitting service has to let itself be controlled by the job-receiving service with regard to transaction management. This means the bottom up strategy (see "[Programming rules and recommendations](#)") must be observed. To ensure this the job-submitting service must take account of the transaction status of the job-receiving service: end of transaction (PEND RE/SP) may not be set in the job submitter until all job receivers have transaction status "P".

5.3.4 Example: distributed dialog via LU6.1

The following simple example shows the sequence of calls in distributed dialogs via LU6.1. In each case there are indications as to which fields can or have to be set or evaluated. The field names are specified using COBOL notation.

In this example the job-submitting program consists of two program units: in the first unit, the subjob is submitted to the job-receiving service; in the second unit, the response of the job-receiving service is read and the response is output to the terminal, if necessary.

As explained in section “[Error handling by the program unit](#)” a job-submitting program unit which follows after a synchronization point is started not only in a normal run, but also after rolling back a distributed transaction with service restart. This is why a check is made in the first unit of the job-submitting program whether status information is available. Such a service restart only occurs, however, if the job-submitting service has set a synchronization point prior to the start of this program unit (with or without participation of a job-receiving service).

1. Job-submitting program, first unit

INIT

```
Evaluate:
KCKNZVG    -->  R  service restart,
                status information might be available.
```

MGET Input message from terminal. If the job-submitting service has already reached a synchronization point, status information may be present as well.

Evaluate:

```
KCRPI      -->  Return information from the job receiver
blanks     there is no status information present
>svid      there is status information from the
            job-receiving service with the specified service ID. In this case
            the status information is to be read with a 2nd MGET.
```

2. MGET

Read the status information after which error handling is necessary.

Set:

```
KCOM       <--  with NT
KCLA       <--  with the length 0
KCRN       <--  with the service ID (>svid)
KCMF       <--  with blanks
```

Evaluate:

```
KCVGST     -->  service status:
I          job-receiving service inactive
E          job-receiving service terminated with PEND ER/FR
Z          job-receiving service terminated by openUTM with PEND ER
R          job-receiving service terminated with PEND RS
T          time has expired (timer)
```

KCTAST --> transaction status:

```
I          transaction in job-receiving service inactive
R          transaction in job-receiving service rolled back
M          mismatch
```

If there is no status information present:

APRO Address the job-receiving service (if not already done)

Set:

```
KCOM       <--  with DM for dialog service
KCRN       <--  with the LTAC of the job-receiving service
KCPA       <--  with double-step addressing:
                with the name of the partner application
KCPI       <--  with a self-selected service ID (>svid)
```



```

KCLM      ,    0
MPUT      to job-receiving service
Set:
KCOM      <-- NT or NE
KCRN      <-- with the service ID (>svid)
KCMF      <-- possible format ID for job-receiver
KCDF      <-- binary 0
KCLM      <-- length
PEND      (end of first unit)
Set:
KCOM      <-- PEND call variant:
          KP      normally recommended in the job-submitting
                   service
          RE      end of transaction is requested
          FI      not allowed because job-receiver still open
          ER/FR   also aborts job-receiving service
          PA      prohibited after MPUT to job-receiving service
          PR      prohibited after MPUT to job-receiving service
          SP      prohibited after MPUT to job-receiving service
          FC      prohibited after MPUT to job-receiving service
KCRN      <-- name of follow-up program unit of job submitter
          (second unit of the job-submitting program)

```

2. Job-receiving program

```
INIT
  Evaluate:
  KCBENID    --> name of the session
  KCLOGTER   --> name of the partner application
  KCTERMN    --> ID of the partner application
  KCCP       --> ID of the protocol used, '1' is entered for LU6.1
  KCRMF      --> format ID from first MPUT of the job submitter
MGET  Read message from job-submitting service
  Evaluate:
  KCRCCC     --> KDCS error code 19Z through 39Z cannot occur
  KCRMLM     --> length from MPUT of the job submitter (KCLM)
  KCRST Byte1 --> service status of job-submitting service:
                    O  job-submitting service is open
  KCRST Byte2 --> transaction status of job-submitting service
                    O  transaction is open (PEND KP for job submitter)
                    P  end of transaction initiated (PEND RE)
                    C  transaction with job submitter terminated
  KCRMF      if more message segments still present:
                    format ID of the next segment, otherwise:
                    format ID of segment read.
MPUT  unchanged
  Set:
  KCOM       <-- with NT or NE
  KCMF       <-- format ID or blanks
  KCLM       <-- length of the message
  KCRN       <-- with blanks to send the message to the job submitter
  KCDF       <-- any value which the job submitter receives
                    with MGET
PEND  End of job-receiving program UNIT
  Set:
  KCOM       <-- depending on the transaction status:
  KP         only allowed with KCTAST=O or C
  RE         terminates the transaction with KCTAST=P or initiates end of
                    transaction with KCTAST=O or C
  FI         end of the job-receiving service, otherwise as PEND RE
  ER/FR     end of the job-receiving service, transaction is rolled back, job
                    submitter is informed
  PA/PR     no special points, cannot be used to send a message to the job
                    submitter
  KCRN       <-- if necessary (with PEND KP or PEND RE), name of the follow-up
                    program unit of job-receiving service
```

3. Follow-up program unit of the job-submitting program (second unit)

```
INIT
  Evaluate:
  KCRPI      <--  service ID of the job-receiving service
  KCRMF      <--  format ID from 1st MPUT of the job receiver
MGET  Read message from the job receiver
  Set:
  KCOM       <--  NT
  KCLA       <--  length of the message area
  KCRN       <--  service ID from KCRPI of the INIT call
  KCMF       <--  format ID from KCRMF of the INIT call
  Evaluate:
  KCRLM      -->  actual length of the input message
  KCRMF      -->  if more message segments present:
                  format ID of next segment, otherwise:
                  format ID of segment read.
  KCRDF      -->  value from the relevant MPUT of the
                  job-receiving service.
  KCRPI      -->  service ID if further message
                  segments present
  KCRST Byte1 -->  service status of job-receiving service:
                  O  job-receiving service is open
                  C  job-receiving service is terminated (PEND FI)
  KCRST Byte2 -->  transaction status of job-receiving service:
                  O  transaction is open (PEND KP)
                  P  job receiver has requested end of transaction (with PEND RE or
                  FI, PTC status)
                  C  transaction is terminated (PEND RE or FI)
MPUT  to the terminal
  Set:
  KCRN       <--  with blanks
  KCOM       <--  with NT or NE
  KCLM       <--  with the length of the message
  KCMF       <--  with the format ID or blanks
  KCDF       <--  if necessary, with a screen function
PEND  end of the follow-up program unit of the job-receiving service
  Set:
  KCOM       <--  depending on status indicators in KCRST
  FI         only allowed with KCVGST=C, terminates service and transaction
  RE         terminates the transaction with KCTAST=P, not allowed with
             KCTAST=O (because message directed to terminal)
  ER/FR      rolls back transaction, job-receiving service is also rolled back
             and terminated;
             only exception: KCTAST=C and KCVGST=C.
  KP         not recommended if KCTAST=P
  PA/PR      prohibited since message was sent to terminal.
  KCRN       <--  if necessary (with PEND KP or PEND RE), name of the follow-up
                  program unit of the job-submitting service
```

5.4 Distributed dialogs via OSI TP

For distributed processing between applications the ISO (International Organization for Standardization) defined the OSI TP protocol (**O**pen **S**ystems **I**nterconnection **T**ransaction **P**rocessing).

OSI TP is part of level 7 of the OSI reference model and was accepted as an international standard under the identification ISO/IEC 10026 in July 1992. In particular, OSI TP allows you to control the processing of distributed, i.e. inter-system, transactions. However, you can also use this protocol in cases where two applications simply exchange data without any transaction management. These types of application are often used in client/server communication.

5.4.1 Functional units

The OSI TP functions are divided into so called functional units (FU). Depending on the requirements placed on communication with a partner application, individual functions can be selected for the communication. openUTM supports the following functional units:

Dialogue

The functional unit Dialogue is required whenever you communicate via the OSI TP protocol. It contains functions for the establishment and disconnection of dialogs and as well as for sending error messages.

You use the KDCS call APRO to establish dialogs. In the APRO call you select the OSI TP function combinations which are used for the dialog. Dialogs are normally terminated with a PEND FI call. Dialogs are abnormally terminated by the PEND ER or CTRL AB call. MPUT EM triggers the protocol element TP-U-ERROR, CTRL AB or PEND ER the protocol element TP-ABORT.

Polarized Control

You use the functional unit Polarized Control to manage the send authorization for a dialog. Each dialog is assigned a send authorization which only one of the communication partners can possess at any one time.

In UTM services, send authorization for a dialog changes at the end of the processing step when a message is sent to the dialog partner: openUTM creates the protocol element TP-GRANT-CONTROL implicitly.

Handshake

The handshake functions can be used by the communication partners to coordinate the processing of a dialog at application level. This function makes it possible to request processing confirmations and send positive or negative confirmations. No inter-application transaction management is linked to this function.

You can create a handshake request by calling MPUT HM. Handshake requests from the partner application are displayed by calling MGET. When the KDCS interface is used the messages are not sent until the send authorization is transferred. For this reason openUTM only creates the OSI TP protocol element TP-HANDSHAKE-AND-GRANT-CONTROL, and not TP-HANDSHAKE.

UTM implicitly sends a positive confirmation of a handshake request before the next message to the partner from which the request has been received. However, the confirmation is sent at the next end of transaction at the latest.

You use MPUT EM to send a negative confirmation of a handshake request.

The requesting service can read the result of a handshake request with an MGET call.

Commit and Chained Transactions

The Commit functional unit provides the functions necessary to create distributed transactions. These are, in particular, functions to commit or roll back distributed transactions. If you use these functions you must always select the functional unit Chained Transactions. If processing is to be performed with global transaction management, then only distributed transactions are processed for this dialog.

The MPUT, CTRL and PEND/PGWT calls are used in connection with these function groups.

The operation modifiers of the PEND/PGWT calls, in combination with the target of the MPUT messages created during the last processing step, determine whether a TP-PREPARE is sent and, if this is the case, whether it is sent with DATA-PERMITTED=TRUE or FALSE. However, you can also use the CTRL PR call to create a TP-PREPARE.

The OSI TP protocol elements TP-DEFER(GRANT-CONTROL) and TP-DEFER(END-DIALOGUE) are triggered in the same way. The latter can also be created on its own using the CTRL PE call.

You use the PEND call with the appropriate operation modifiers or the PGWT CM call to request an end of transaction. openUTM negotiates the protocol for the processing of the two-phase commit without the participation of the application program unit. A distributed transaction can be rolled back using PEND RS or PGWT RB. PGWT RB **must** be used if the previous transaction was terminated with PGWT CM.

openUTM handles the protocol for rolling back the distributed transaction without the participation of the application program unit.

Following an MGET call, heuristic decisions by communication partners are shown in the transaction status.

Recovery

The Recovery functional unit provides the services which are necessary for resynchronization of the interrupted transaction after a communication failure. This functional unit ensures global data consistency in such cases. However, OSI TP does not permit the continuation of an interrupted connection (dialog restart).

UTM uses the services of the Recovery functional unit internally. They cannot be directly accessed by the application program.

5.4.2 Programming aids

A program unit receives information about its communication partners via different displays. This information enables the program unit to react selectively to special situations. openUTM makes the information available after an INIT or MGET call.

After INIT, the job receiver is informed about being called by an OSI TP partner and the OSI TP functions used by the job submitter for the dialog. Further displays after the INIT call inform the job receiver of whether the job submitter has requested end of transaction or dialog and whether another message has to be sent to the job submitter in the current transaction.

After an INIT or MGET call, the program unit run is informed about the communication partner for which a message is present for reading and about the abstract syntax which was used when sending the message. When receiving the messages, the program unit has to adhere to the predefined order of messages specified by openUTM. Through the MGET call, the program unit is informed of the type of message received and receives information about the service and transaction status of the communication partner.

The information available after INIT or MGET is explained in more detail below.

Displaying the selected OSI TP functions for the dialog

During the INIT call, important information is entered in the KCCP and KCOF1 fields in KBKOPF (the KB header).

KCCP contains the communication protocol used by the partner: in the case of OSI TP, '2' is entered here. This tells the program unit that it has been called by an OSI TP job submitter.

KCOF1 contains information about the OSI TP functions available for the dialog with the job submitter. The values in the KCOF1 field have the following meanings:

B Basic functions

The functional units Dialogue and Polarized Control are selected for the dialog with the job submitter.

H Basic and handshake functions

The functional units Dialogue, Polarized Control and Handshake are selected for the dialog with the job submitter.

C Basic and Commit functions with Chained Transactions

The functional units Dialogue, Polarized Control, Commit and Chained Transactions are selected for the dialog with the job submitter.

O (other combination)

A standard combination was not selected for the dialog with the job submitter. If INIT PU was called and OSI TP information requested, the available OSI TPI functions are displayed in the message area.

Requesting end of transaction or service by job submitter

After an INIT PU call, the KCENDTA field in the message area for the job-receiving service indicates whether the local service has been requested by its job submitter to terminate the transaction and which variant of the PEND call is to be used. The local service must respond to the request to terminate the transaction or dialog at the latest by the end of the processing step in which it next sends a message to the job submitter.

The following values are possible:

- ' ' no instructions concerning the termination of the processing step.
- O no end of transaction may be requested at the end of the processing step.
- R the transaction and the dialog step must be concluded, the service may not be terminated (PEND RE or PGWT CM with a preceding MPUT to the job submitter).

At the end of transaction, the job submitter possesses the send authorization in the job submitter dialog. The local service possesses the end-of-transaction send authorization in all other dialogs.

- S the transaction must be concluded, the dialog step must not be terminated (PEND SP or PGWT CM without a preceding MPUT to the job submitter).

The local service possesses the send authorization in the dialog with the job submitter at the end of the transaction.

- C the transaction must be concluded, the service may not be terminated (PEND RE/SP or PGWT CM). The local service has end-of-transaction send authorization for the dialog to the job submitter. In another dialog, end-of-transaction send authorization may be passed to the job receiver. This is performed by issuing an MPUT to a job receiver, followed by PEND RE or PGWT CM.

- F both the transaction and the service must be concluded (PEND FI).

Displaying the send authorization for the dialog with the job submitter

After an INIT PU call, the KCSEND field indicates in the message area in the local service whether the local service may send a message to the job submitter in the current processing step. The following values are possible.

- Y It is necessary to send a message to the job submitter at the end of the dialog step.

If KCENDTA has the value "S", in this case it is also necessary to send a message to the job submitter at the end of transaction. This combination (KCENDTA=S and KCSEND=Y) can only occur in the case of heterogeneous coupling.

- N No messages are permitted to be sent to the job submitter. However, messages may be sent to job receivers in which case the transaction must remain open after the end of the processing step.

Displaying the type of message received

After an MGET call, the type of message received is displayed in the KCRMGT field of the return area. The following values are possible:

C (confirm)

A positive handshake confirmation has been received.

E (error)

An error message or negative handshake confirmation has been received.

H (handshake)

A handshake request has been received.

M (message)

A normal user message has been received.

Service status

Following an MGET call, the service status of the communication partner from which a message has been received is displayed in the KCVGST/kcpcv_state field of the return area. The local service can use this display to draw conclusions about the dialog with this partner.

The following values are possible:

C (closed)

The job submitter has terminated the service.

D (disconnected)

The communication with the job submitter has been terminated because of loss of connection.

I (inactive)

The job-receiving service could not be started because, for example, the TAC is unknown.

O (open)

The partner service is open, i.e. end of dialog has not yet been requested.

P (pending end dialogue)

This status can only occur in the case of heterogeneous links and in dialogs for which the Commit functionality has not been selected.

The job receiver wants to end the communication. If the job submitter does not agree, it can continue the communication using MPUT EM.

T (time out)

No connection could be utilized in the generated wait time or the job receiver sent no message in the generated wait time; the dialog with the job receiver is terminated.

Z (error)

The dialog with the job receiver has been terminated because of an error.

In the case of the service stati D, I, and T no message is transferred. The service status in the job-receiving service is always O.

Transaction status

Following an MGET call, the transaction status of the communication partner from which a message has been received is indicated in the KCVGST/kcpta_state field of the return area. The local service can use this display to draw conclusions about the dialog with this partner.

The following values are possible:

H (heuristic hazard)

The result of a transaction is undetermined since communication with at least one communication partner has been interrupted. The possibility that one of the communication partners involved in the last transaction has made a heuristic decision which conflicts with the actual result of the last transaction cannot be excluded.

I (inactive)

The transaction is inactive at the job receiver, e.g. because the TAC is invalid or no connection could be established in the generated wait period.

M (mismatch)

It was not possible to synchronize the transaction in the remote service with the transaction in the local service. This may occur after a timeout.

A mismatch can also occur if at least one of the communication partners involved in the transaction has made a heuristic decision which conflicts with the actual result of the transaction.

O (open)

The transaction is open in the remote service.

P (prepare to commit)

The partner service has either initiated the end of transaction itself or is requesting the local service to initiate the end of transaction.

R (rolled back)

The transaction in the remote service has been rolled back.

U (unknown)

The transaction status is unknown. This value is only possible in dialogs for which the Commit functionality has not been selected.

In the job-receiving service, only the following transaction statuses are possible:

with functional unit commit: O, P

without functional unit commit: U

5.4.3 Programming rules for dialogs without the functional unit commit

End of transaction

In a communication which complies with Cooperative Processing, the communication partners may request end of transaction independently of each other. In this type of processing only local transactions occur, i.e. end of transaction in a service has no effect on the transaction in the partner service.

End of service

A job-receiving service may terminate its service at any time.

A job-submitting service may not terminate until all dialogs with its job-receiving services are terminated.

PEND FC (chained services) in job-receiving services is not permitted.

5.4.4 Programming rules with the functional unit commit

Before explaining the rules which a service must respect in a distributed transaction, it is first necessary to explain certain terms.

Explanation of terms

Data transfer phase

A service is in the data transfer phase until it has either been requested to end the transaction or has requested its job receivers to end the transaction.

Send authorization

During the data transfer phase, a send authorization exists for each dialog. This is assigned to one or other of the communication partners at any given time.

The service which has send authorization in a dialog may use MPUT to send a message to the partner service. When the message is sent, the send authorization passes to the communication partner unless the partner has explicitly prohibited this with a CTRL call (CTRL PR or PE and KCNORPLY=Y).

In a processing step, a service can pass the send authorization for the dialog with the job submitter or pass one or more send authorizations for dialogs with job receivers.

End-of-transaction send authorization

The end-of-transaction send authorization controls which of the communication partners owns the send authorization after the current transaction is finished.

Usually the job-submitting service owns the end-of-transaction send authorization. However, the job-submitting service can use an MPUT message followed by PEND RE to pass this send authorization to the job-receiving service.

Here you have to remember that a service can only pass on send authorization for a maximum of one dialog at the end of the transaction.

End of transaction

A service may request end of transaction if it has been requested to do so by its job-submitting service, and it does not possess end-of-transaction send authorization for more than one dialog.

End of service

A service may request end of service if it has been requested to do so by its job-submitting service, and the service has not sent a message to a job receiver in the current processing step.

Other programming rules

- In the data transfer phase, the local service possesses the send authorization for all dialogs during a program unit run.
- In a processing step, a service cannot simultaneously send messages to its job submitter and to job receivers.
- If the transaction remains open at the end of the processing step, then the local service may send messages to multiple job receivers simultaneously in this processing step.

-
- A service may pass the end-of-transaction send authorization to no more than one partner. The consequences of this rule are:
 - In a processing step which is terminated by a request to end a transaction, a message may be sent to only one partner.
 - An intermediate node may only transfer the end-of-transaction send authorization in a dialog with a job receiver if it possesses the end-of-transaction send authorization in the dialog with the job submitter.
 - A job receiver may only request end of transaction if it has been requested to do so by its job submitter.

Rules for using the different PEND variants

- You can use PEND KP if, in the processing step, messages are only sent to partners which have not yet requested end of transaction.
- You can use PEND RE if, in the processing step,
 - messages have been sent to no more than one partner.
 - no request for end of transaction or dialog has simultaneously been sent to this partner.
 - the local service has already received a request for end of transaction or the local service itself is the root in the transaction tree.
- You can use PEND SP if, in the processing step,
 - the local service has already received a request for end of transaction or the local service itself is the root in the transaction tree and
 - the local service possesses the end-of-transaction send authorization for the dialog with the job submitter and
 - no message has been sent to a job receiver and
 - no message has been sent to the client.
- You can use PEND FI if, in the processing step,
 - the local service has already received a request for end of dialog or the local service itself is the root of the transaction tree and
 - no job receiver has received a request (using CTRL PR) for end of transaction, but not for end of service.
 - no message has been sent to a job receiver.

Rules for using PGWT variants

- A PGWT KP is possible if PEND KP is allowed.
- A PGWT CM is possible
 - with output of a dialog message if PEND RE is allowed.
 - without output of a dialog message if PEND SP is allowed.
- PGWT RB must be used if a transaction in which the last synchronization point was set with PGWT CM is to be rolled back without terminating the OSI TP dialog.

Programming recommendations

In distributed transaction processing via OSI TP protocol, you should preferably terminate the distributed transaction in the following way:

If the uppermost job submitter in the transaction tree wants to terminate the distributed transaction, it issues a CTRL PR and an MPUT call to each of its job receivers and subsequently uses PEND/PGWT KP to terminate the processing step. The uppermost job submitter terminates the transaction after the responses from its job receivers have been received.

If an intermediate node in the transaction tree receives a request to end the transaction, it issues a CTRL PR and an MPUT call to each of its job receivers and subsequently uses PEND/PGWT KP to terminate the processing step. After the responses from its job receivers have been received, the intermediate node sends a response to its job submitter and terminates the dialog step and the transaction.

If the lowest job receiver in the transaction tree receives a request to end the transaction, it sends a response to its job submitter and terminates the dialog step and the transaction.

If you follow this rule, the next transaction starts at the uppermost job-submitting service in a program unit run.

5.4.5 Programming rules for communications with BeanConnect

If openUTM calls an OLTP message driven bean via BeanConnect at an J2EE server, then you should note the following:

- The handshake functional units must not be selected.
- Only single-step dialogs are permitted, i.e. in the case of dialogs without functional unit commit, the job receiver terminates the dialog after sending the response.
- In the case of dialogs with functional unit commit, the job submitter must request the receiver to terminate the dialog either immediately on sending the message or on receiving the response. If the job submitter does not request dialog termination until receiving the response then, if an error occurs, the job receiver is still able to send an (error) message to the submitter and the submitter itself can roll back the transaction.

5.4.6 Particularities of rollback and restart

The OSI TP protocol enables you to work either with global transaction management (functional unit commit) or without global transaction management (Cooperative Processing).

OSI TP with functional unit commit

If you select the functional unit commit for OSI TP, the rollback of transactions with PEND RS is performed in the same way as in LU6.1.

When a service is restarted after PEND RS, the behavior is the same as with LU6.1, with one exception: when using the OSI TP protocol it is not possible to restart an interrupted dialog.

A synchronization point can also be set with PGWT CM when using OSI TP. The next transaction may then be rolled back with PGWT RB only. In this case a return is always made to the program unit that issued the PGWT RB. No service restart is performed.

OSI TP without functional unit commit

If you do not select this functional unit, the job-submitting service is **not** automatically rolled back when an error occurs in the job-receiver service or if the connection is lost. The job-submitting service is continued with the program unit specified in the last PEND. However, if it waits for a result from the job receiver, it receives an error message (with service status "Z" and transaction status "U") and can also react with a rollback.

If an error occurs in the job-submitter service, openUTM rolls back the transactions in the job-submitting service and job receiving services and terminates the job-receiving service. If the job-submitting service has already reached a synchronization point, a service restart is performed after the rollback of the transaction. The follow-up program unit receives an error message with service status "Z" and transaction status "U".

A global service restart is not possible, since no common synchronization points exist.

If you use calls for programmed rollbacks, you have to take the following into account:

- PEND RS

For a call in the job-submitting service:

All job-receiving services with which the job-submitting service communicates without functional unit commit are terminated.

For a call in the job-receiving service:

- If PEND SP has been used to terminate the preceding transaction, then PEND RS rolls back the local transaction and the service is continued with the follow-up program unit specified with PEND SP.
 - If PEND SP has **not** been used to terminate the preceding transaction **and the service** is running under a user ID without the restart property, then the service is rolled back to the last synchronization point and the dialog with the job submitter is terminated.
 - In all other cases, openUTM terminates the service with PEND FR.
- PGWT RB
- PGWT RB rolls back the current transaction and the program unit continues.

- PENDING/FR

No special considerations apply when this call is used in the job-submitter service: The transactions in the job submitter and all its job receivers are rolled back and the job receivers terminated.

If called in the job-receiver service, the job receiver is rolled back and terminated. However, the job-submitter service is continued in the program unit specified with the last PENDING. The job-submitter service can read the messages which have been sent by the job receiver with MPUT.

i To ensure consistent operation even when a transaction is rolled back, it is advisable to use only PGWT or only PENDING calls within a distributed transaction.

- RSET

The RSET call always applies only to the local service. The RSET=GLOBAL setting in the KDCDEF statement UTMD has no effect. This setting only has an effect in distributed processing with global transaction management (see "[Programmed rollback](#)").

5.4.7 Using existing program units for OSI TP communication

Existing UTM program units which were not specifically designed for communication via OSI TP can be used unchanged for OSI TP communication given certain restrictions (see below). The same service can, for example, be used by clients as well as other services. In this way openUTM gives you considerable flexibility when distributing applications.

The various cases which may arise when using existing program units for OSI TP communication are identified and described in the following sections.

Program units for communication with clients as OSI TP job receiver

Program units which have been designed for communication with clients can be used unchanged by the job receiver for communication with an OSI TP partner. You must observe the following points:

- Different return information in KB header

The communication partner of the job-receiving service is the job-submitting service, not the user at the terminal. This is why the job-receiving service does not receive the name of the LTERM partner in the KB header. Instead, it receives the name of the OSI-LPAP partner. The entry in the KCBENID/kcuserid field depends on the security type used. You use the APRO call to select the security type in the job submitter (in the KCSECTYP field):

 - With security type "N" (None), no user ID is transferred to the job receiver. KCBENID/kcuserid contains the name of the association instead of the user ID.
 - With security type "P" (Program), KCBENID/kcuserid contains the user ID which was specified through APRO in the job submitter.
 - With security type "S" (Same), KCBENID/kcuserid contains the user ID under which the job submitter was started.
- Different TLS and ULS assignments

Write and read calls for TLS in the job-receiving service refer to the TLS of the OSI-LPAP partner and not to a TLS of an LTERM partner. Similarly, calls for a ULS refer to the ULS of the user ID only if security type P/S is present. If security type N is present it refers to the ULS of the association.
- Function keys are not supported in distributed processing

The job-submitting service cannot send a message corresponding to the function key to the job-receiving service. When MGET is used, the job-receiving service can therefore never receive the corresponding KDCS return code (19Z to 39Z).
- The card reader cannot be used in the job-receiving service.

In a job-receiving service, the KCAUSWEIS/kccard field always contains blanks.
- Abstract syntax for distributed processing via OSI TP

In distributed processing via OSI TP, the format identifier is used to transfer the name of the abstract syntax. Job receiver programs designed for communication with clients can only be used unchanged for distributed processing via OSI TP if you use UDT Octet String Mapping exclusively as the abstract syntax. Using any other abstract syntax you would have to perform adaptations for the encoding or decoding of messages. The KCMF /kcfn field must therefore always contain blanks.

LU6.1 job receiver as OSI TP job receiver

Job receiver program units written for communication via LU6.1 can only be used unchanged as OSI TP job receivers when the commit functional unit has **not** been selected and the when the following conditions are fulfilled:

-
- You use UDT Octet String Mapping exclusively as abstract syntax for communication via OSI TP. The KCMF /kcfn field must therefore always contain blanks when exchanging messages.
 - The transaction and service status in the job receiver programs are not evaluated.

If the commit functional unit is selected, then the job submitter must be the first to request the end of the transaction and the end of the service, and must also always issue the request when the job receiver expects it.

LU6.1 job submitter as OSI TP job submitter

Job submitter program units written for communication via LU6.1 cannot be used as OSI TP job submitters unchanged. At the very minimum, you will have to adapt the APRO call (selection of OSI function in KCOF field and possible changes in the 2nd parameter area). No adaptations are necessary for distributed processing without global transaction management (Cooperative Processing).

In distributed processing with global transaction management, i.e. when the functional unit commit is selected, the programs must always be extended to take account of end-of-dialog requests (e.g. by inserting CTRL PE).

5.4.8 Particularities with heterogeneous coupling

If you want to use OSI TP to connect your UTM applications with transaction applications of other manufacturers you have to consider the following points:

- User data when establishing associations:
When the connection is being established, only the user data necessary for OSI TP and CCR is exchanged. Other user data is not sent and is ignored when received.
- User syntaxes and CCR association setup:
openUTM does not permit syntaxes generated by openUTM to be rejected by the Additionally, these syntaxes must be offered with the association setup request. In such cases, openUTM rejects the association setup.
- Disconnection with A-ABORT:
openUTM uses A-ABORT to disconnect, not A-RELEASE.
- Channels:
"Two-way-recovery" channels are not supported by openUTM.
- User data for TP-BEGIN-DIALOGUE-RI:
You can only use TP-BEGIN-DIALOGUE-RI to exchange user data necessary for UTMSEC. Application programs have no direct access to this user data. Other user data is not sent and is ignored when received.
- No user data for TP-BEGIN-DIALOGUE-RC, TP-ABORT-RI:
openUTM does not send user data with the protocol elements. Received user data is ignored.
- No Shared Control functional unit:
openUTM does not support the Shared Control functional unit (i.e. does not support the profiles ATP12, ATP22, ATP32).
- Unchained Transactions functional unit:
openUTM does not support this functional unit as a job submitter. Conversely, you can select the functional unit in a partner application if the partner application acts as job submitter. However, the partner application has to start the distributed transaction before the first send authorization transfer in the dialog. The dialog must terminate with the first transaction, as otherwise openUTM terminates the dialog abnormally.
- Recipient TPSU-Title:
A Recipient TPSU-Title is always necessary when using TP-BEGIN-DIALOGUE-RI. If openUTM is the receiver, the title must not exceed 8 characters in length and cannot be of the type "integer".
- REQUEST-CONTROL-RI, HANDSHAKE-RI:
openUTM does not send the protocol elements. If a dialog service receives TP-HANDSHAKE-RI it is terminated abnormally.
- maximum user data length: 32767 octets:
openUTM sends a maximum of 32767 octets of user data in a protocol element. If user data with a length of more than 32767 octets is received, openUTM disconnects the link.
- End of dialog without Commit:
No TP-END-DIALOGUE-RI should be sent to a dialog job-receiving service (end of dialog from "above"), as otherwise openUTM terminates the service abnormally. openUTM only uses "Confirmed End Dialogue" for the transfer of asynchronous messages.

5.4.9 Examples: distributed dialogs via OSI TP

This section contains examples describing the different programming interface possibilities when you use the Commit functionality and Chained Transactions.

First the simplest case is considered. Here, a job submitter communicates with a job receiver. Secondly, the scenario is extended to describe communication with multiple job receivers and finally the more complicated cases are illustrated in which a service communicates with both a job receiver and a job receiver via the OSI TP protocol.

The data transfer phase, end of transaction, and end of dialog are considered separately.

At the end of the section you can find examples which illustrate the ["abnormal termination of job-receiving services with CTRL AB"](#).

Comments on the following diagrams

The following diagrams illustrate the communication flow in distributed OSI TP dialogs. In these services, only those KDCS calls which are relevant for communication are shown, other KDCS calls and processing statements are omitted.

The service and transaction stati, displayed to the program unit after the MGET call, are shown to the right of the MGET calls. In the examples, the COBOL field names are used, i.e. KCVGST for the service status and KCTAST for the transaction status. For C/C++ the corresponding fields are called *kcpcv_state* and *kcpta_state*.

In the job-receiving services, the KCENDTA and KSEND are shown to the right of the INIT calls. These can be evaluated by a program unit after an INIT PU call.

In the case of MPUT calls addressed to a job receiver and CRTL calls, the name of the addressed job-receiving service is shown. The format used is ">x", where x represents the job receiver. MPUT calls without this specification are always addressed to either the job submitter or the client.

The arrows between job submitters and job receivers symbolize for the message exchange and protocol flow.

Synchronization points are represented by bold, unbroken lines.

Any PEND KP calls shown in these examples can be replaced by PGWT KP calls. Similarly, a PGWT CM with a preceding MPUT message can be used instead of PEND RE, and a PGWT CM without a preceding MPUT message can be used instead of PEND SP.

5.4.9.1 One job receiver

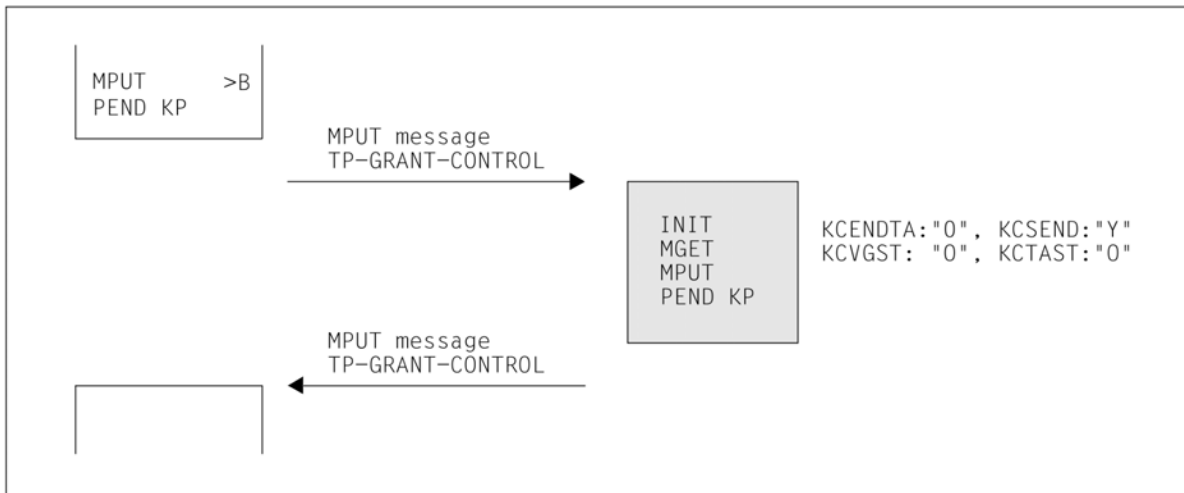
The simplest case possible is where one job submitter (A) has exactly one job receiver (B). This section explains all possible uses for this type of application.

Data transfer phase

The message transfer phase is the period in which neither of the two partners requests an end of transaction. For the job receiver, this option is only available if it has been requested explicitly by the job submitter.

Send authorization changes with each message sent to the partner. Displaying the service status "O" and transaction status "O" informs the job receiver that neither end of transaction nor end of service has been requested.

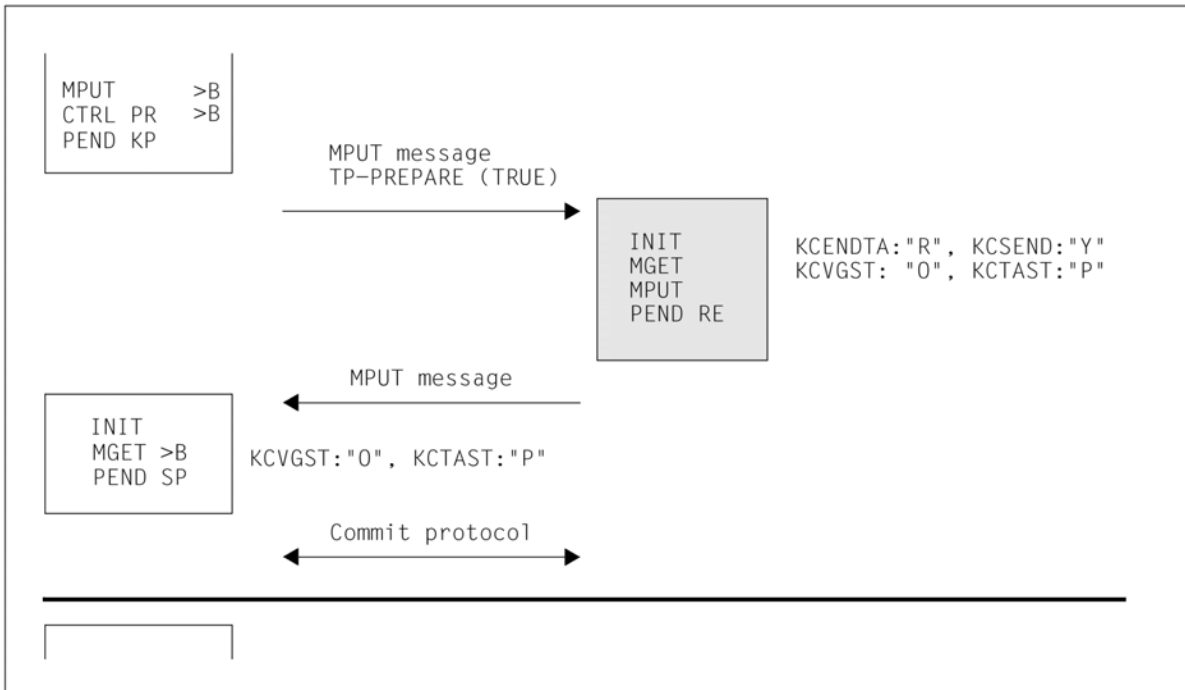
Example 1: Message to job receiver and PEND KP



End of transaction

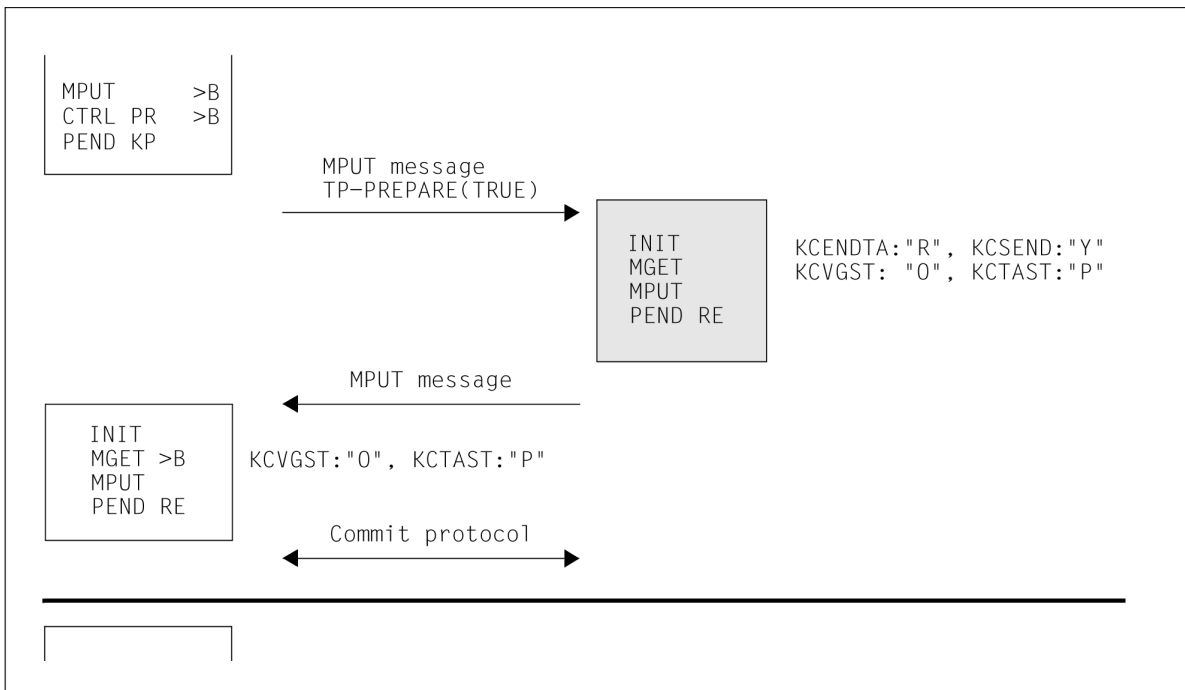
A job receiver may only issue an end of transaction call if this has been requested to do so by the job submitter. The job receiver can read this information from the transaction status after the MGET call.

Example 2: Message and Prepare to job receiver and PEND KP

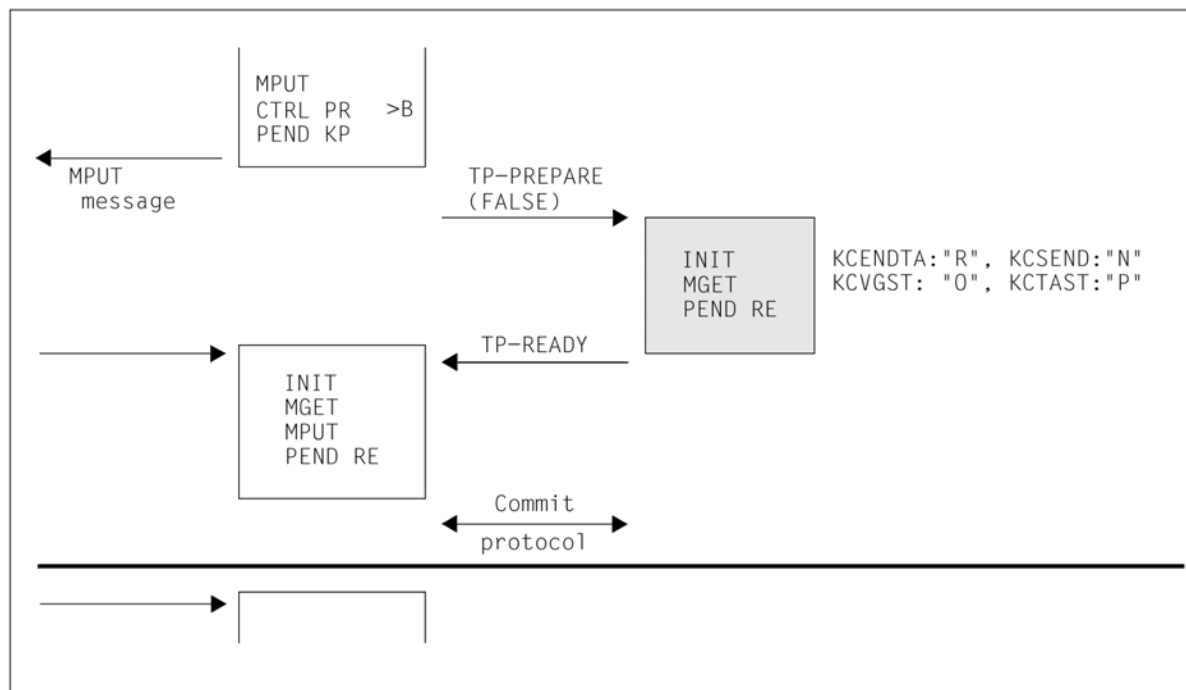


This should be regarded as the normal case when communicating via the OSI TP protocol, since the order of KDCS calls best corresponds to the protocol flow. Additionally, the job-submitting service has control after end of transaction and this simplifies service restart.

In the second job submitter program unit run you can also issue an MPUT to the client and a PEND RE in a dialog service instead of PEND SP. In this case, the command sequence is as follows:



Example 3: No message to the job receiver and CTRL PR



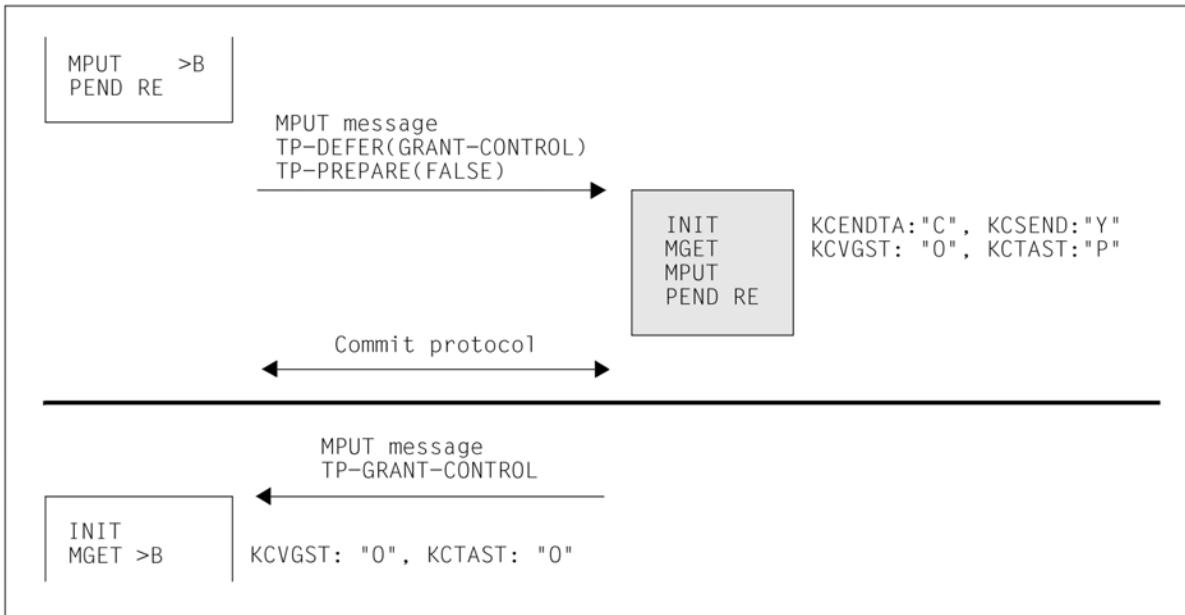
In this case the job receiver simply receives a request for end of transaction, but no message from the job submitter. Send authorization therefore does not pass to the job receiver (DATA-PERMITTED=FALSE). The job submitter possesses the send authorization at end of transaction - as in example 2.

It is also only possible to issue a PEND PA/PR in place of the MPUT, PEND KP the first time the program unit is run. If the job-submitting service is an asynchronous service, only this second variant is possible.

You should note that at the start of the program unit run, after the PEND KP, the system waits only for the message from the client but not for the TP-READY from the job receiver. I.e., after a PEND PA/PR the follow-up program unit is started immediately unless the system is waiting for a DGET message.

It is also only possible to issue a PEND SP in place of the MPUT, PEND KP the second time the program unit is run. If the job-submitting service is an asynchronous service, only this second variant is possible.

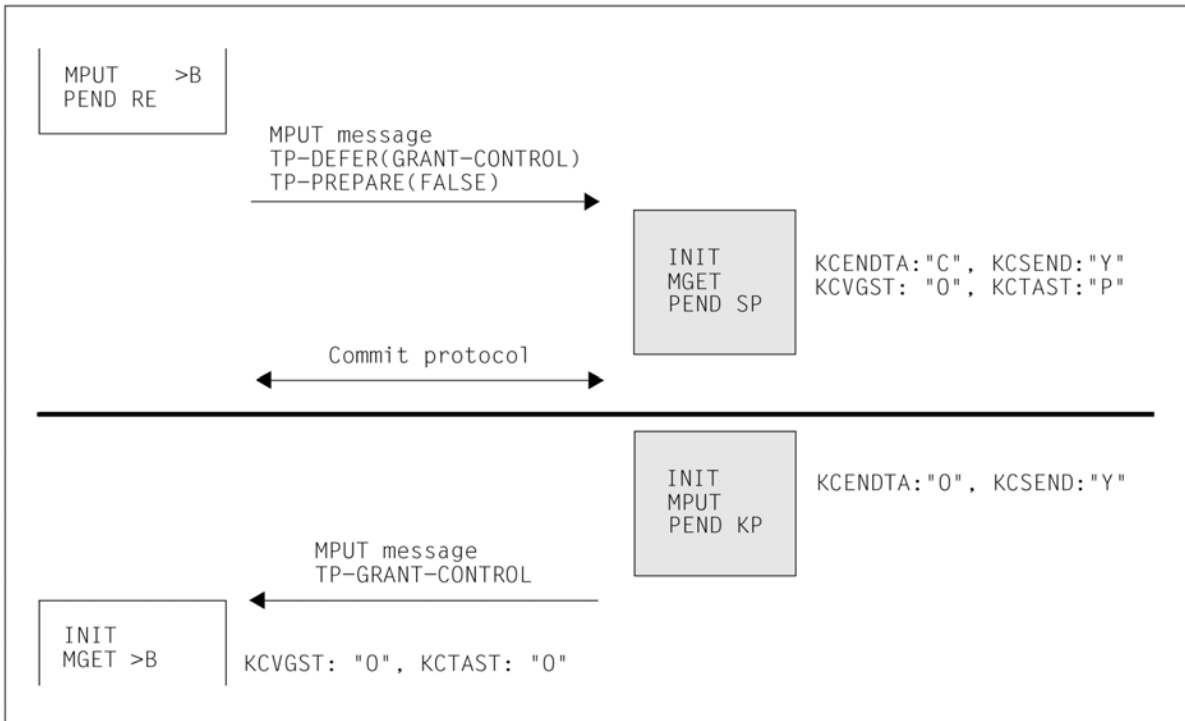
Example 4: Message to job receiver and PEND RE



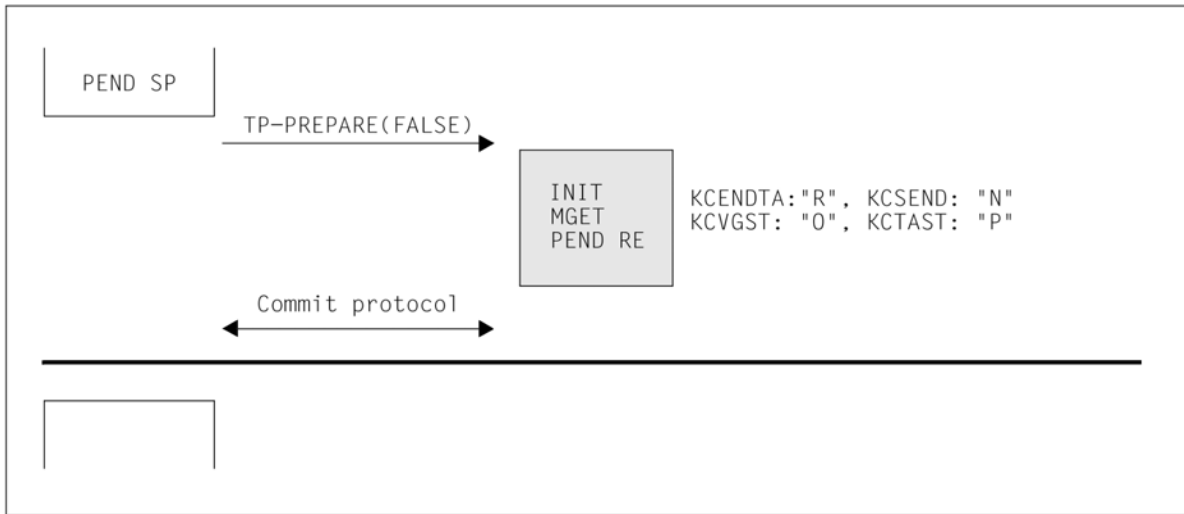
This case most closely resembles the situation when using the LU6.1 protocol. In particular, the service and transaction stati are identical to those for communication via the LU6.1 protocol. This means that you can reuse these programs unchanged. However, you should remember that these programs do not adhere to the bottom up strategy recommended for LU6.1 communication.

In this example, the job receiver possesses control of end-of-transaction send authorization.

In this case, the job receiver can also use a PEND SP instead of the PEND RE call. The command sequence is then as follows:



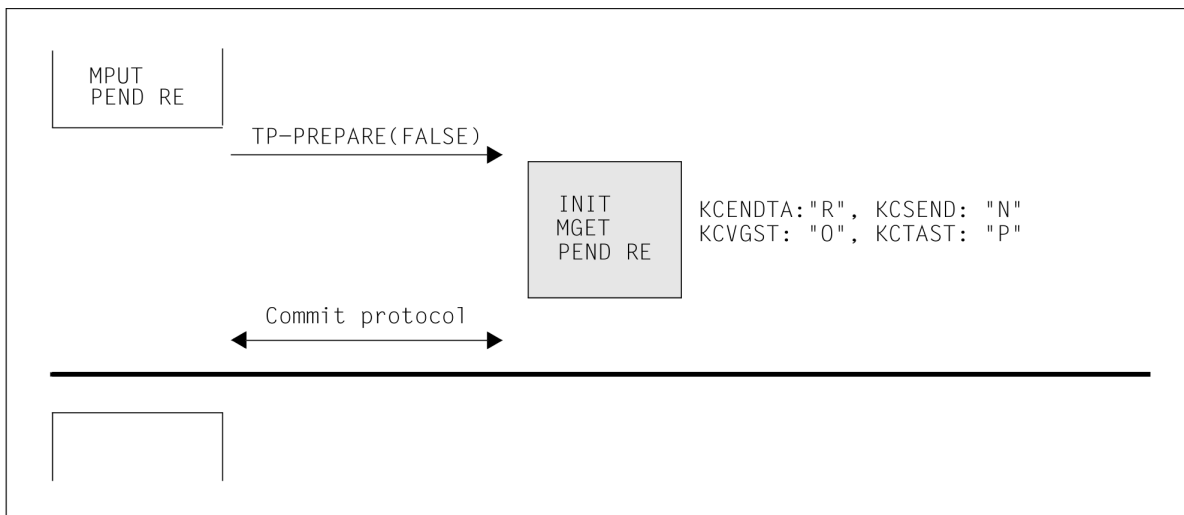
Example 5: No message to job receiver and PEND SP/RE



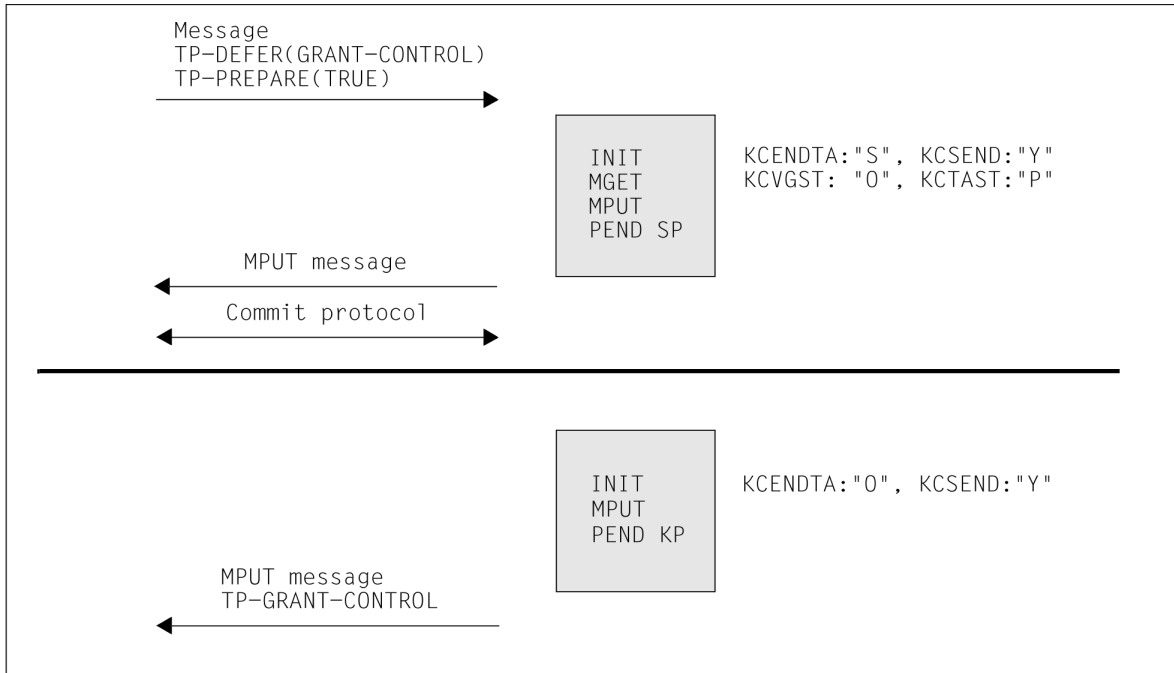
This example illustrates that the job-receiving services are included in all transactions, even if the job submitter and job receiver have not communicated in the last transaction.

There are no so-called local transactions when using the OSI TP protocol with Chained Transactions. This has to be taken into account when you design your distributed applications.

The job submitter can issue an MPUT to the client and a PEND RE instead of PEND SP. The command sequence is then as follows:



Example 6: Defer-Grant-Control and Prepare(True)



This is an 'exotic' case which can only occur with heterogeneous coupling. The job receiver has to send two messages in sequence to the job submitter. The first message has to be sent within the first current transaction. Send authorization remains with the job receiver after the end of transaction, which means that the job receiver issues the first message in the follow-up transaction.

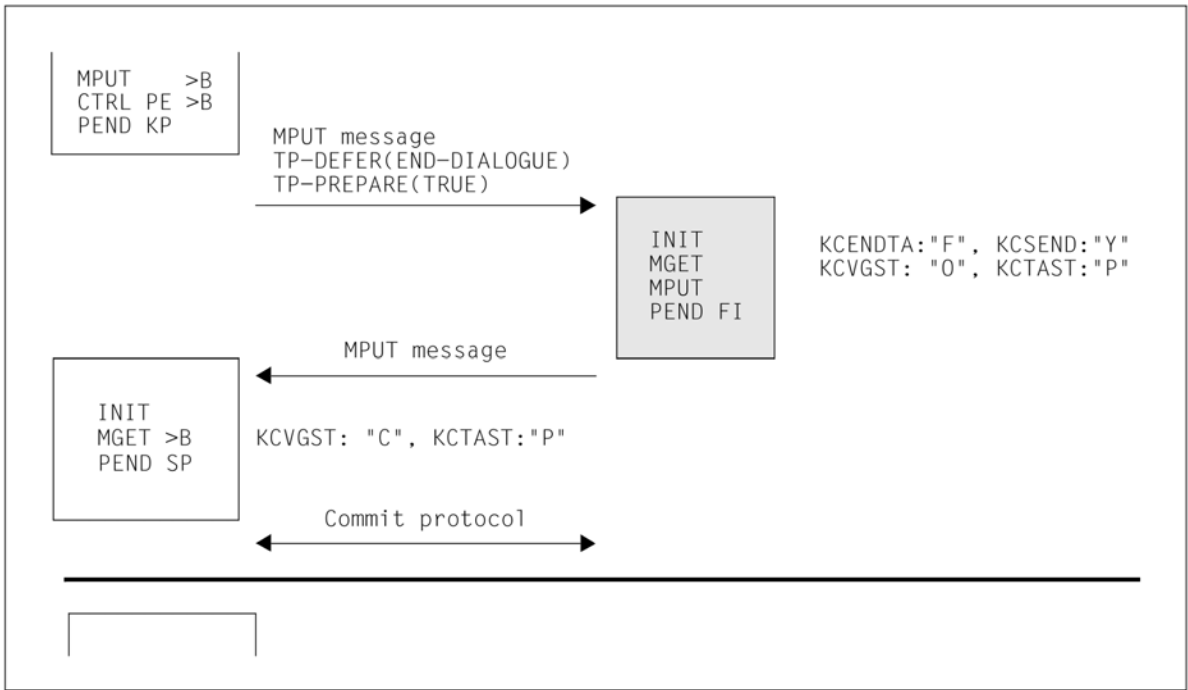
End of dialog

If the Commit functionality is used, the job receiver can only terminate the service if requested to do so by the job submitter.

Normally the job-receiving services are terminated first and the job-submitting service can terminate afterwards. It is also possible to terminate the job-submitting and job-receiving service simultaneously.

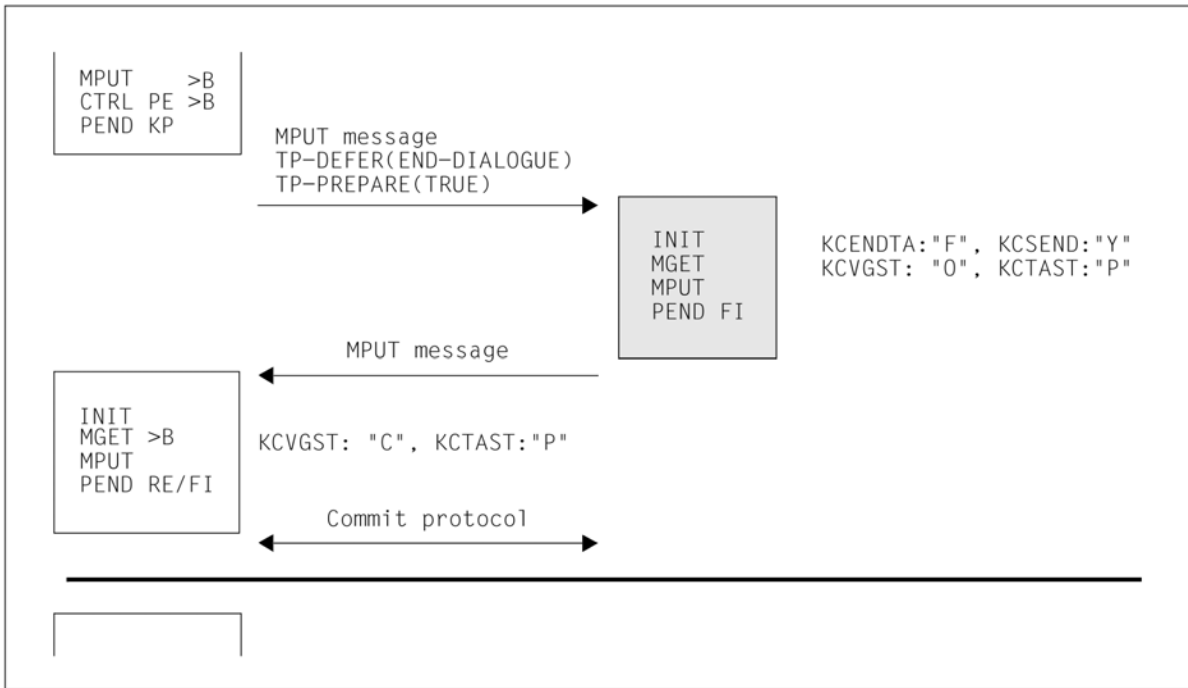
If the job-submitting service is to be continued, then the job receiver must use the CTRL PE call to request the job receiver to end the service.

Example 7: Message and end dialog to job receiver and PEND KP

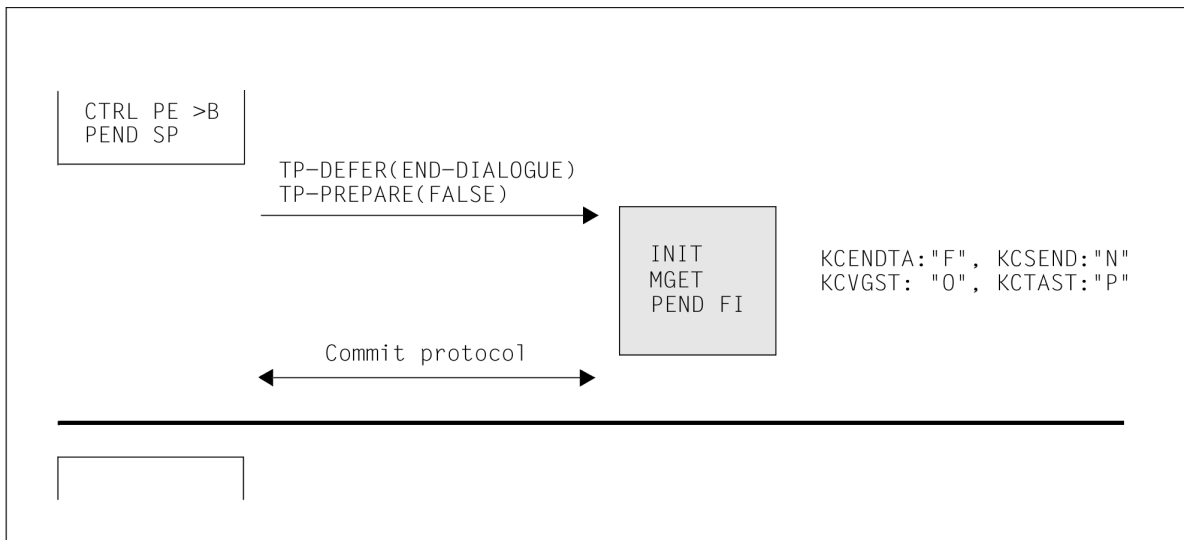


In this example, the job receiver can send a last message to the job submitter before the job receiver terminates the service.

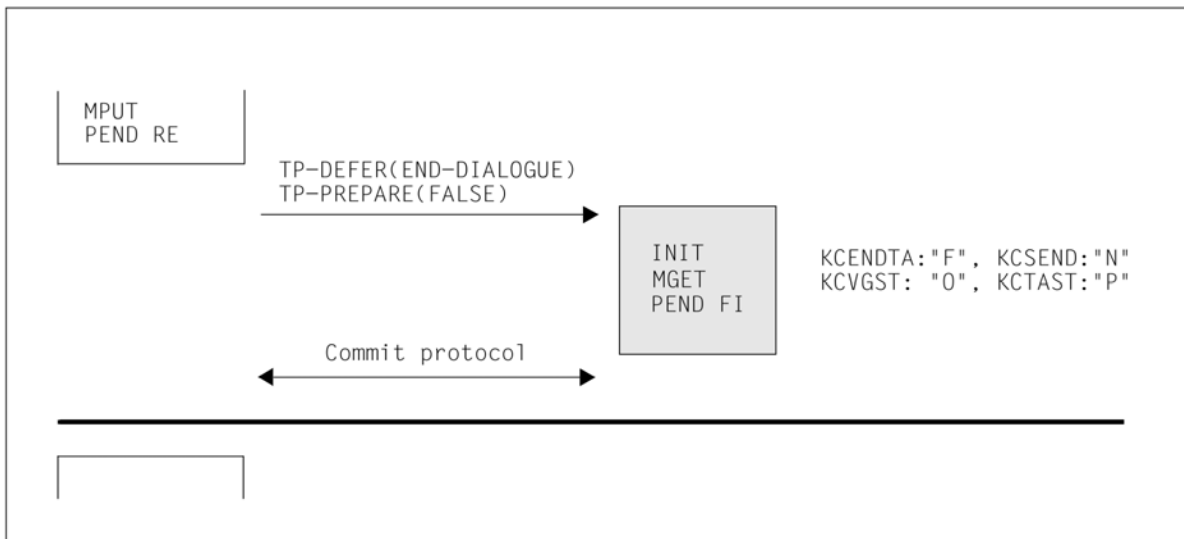
In the second job submitter program unit run, instead of PEND SP, you can issue an MPUT to the client and another PEND call to request end of service or end of transaction. The command sequence is then as follows:



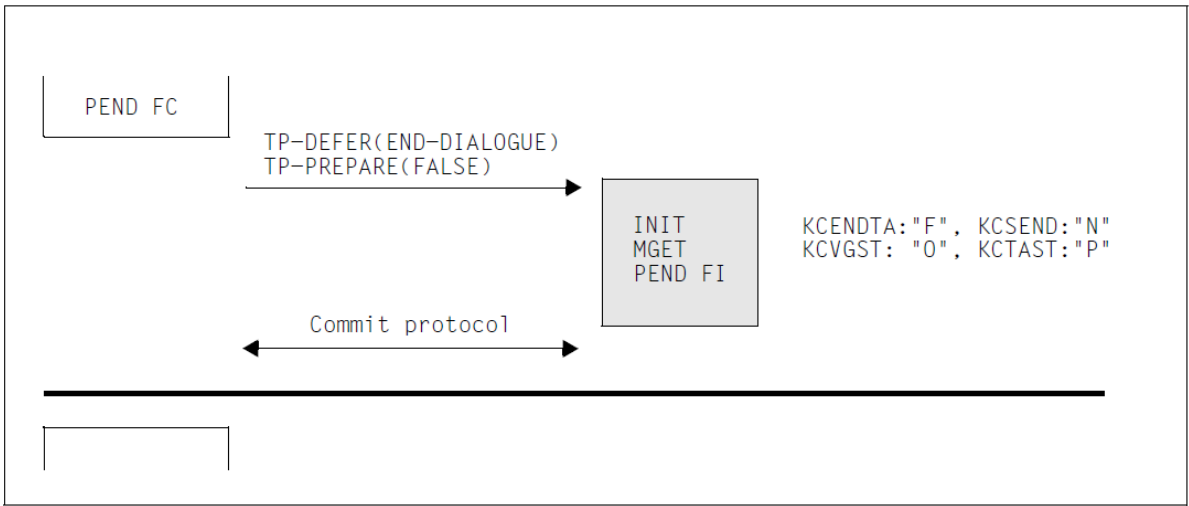
Example 8: No message to the job receiver and PEND SP/RE



In the first job submitter program unit run, instead of PEND SP, you can issue an MPUT to the client, and another PEND call to request end of service or end of transaction. This results in the following command sequence:

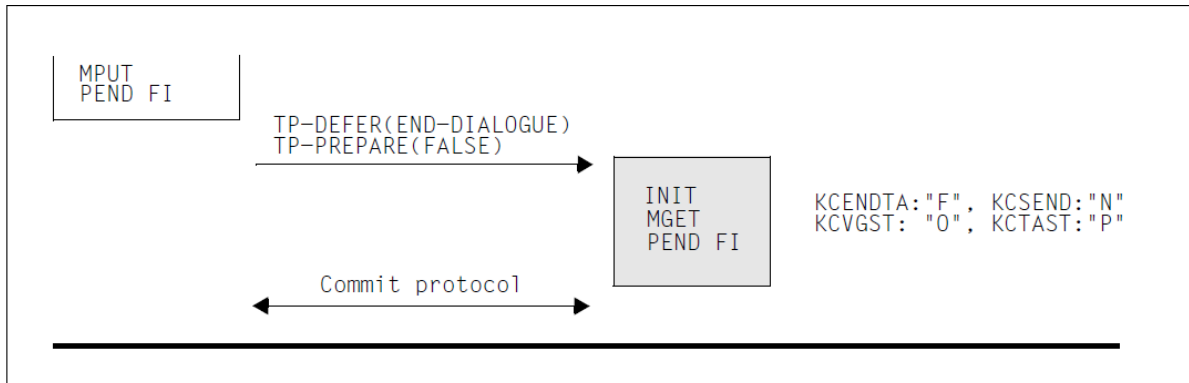


Example 9: No message to the job receiver and PEND FC/FI

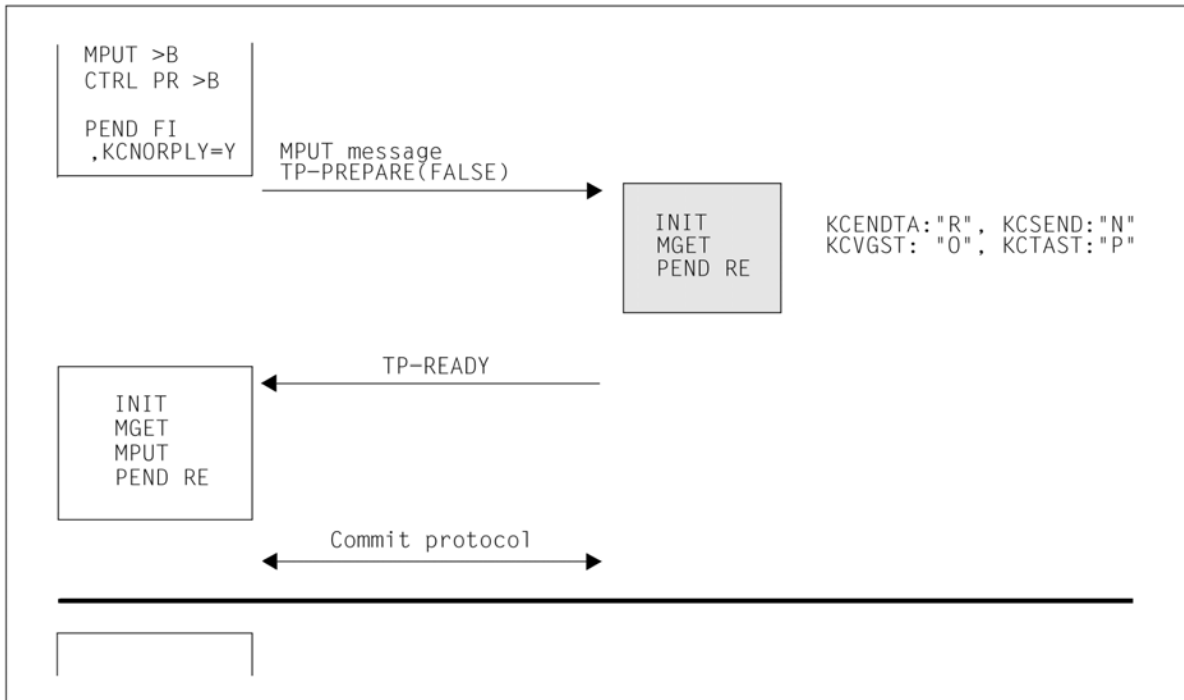


In the example above, the job-submitting service is not to be continued as in examples 6 and 7. Instead, it terminates at the same time as the job receiver. If PEND FC (service chaining) is used, the dialog step is continued in a follow-up service.

In the first job submitter program unit run, instead of PEND FC, you can issue an MPUT and a PEND FI. In this case no follow-up service is performed in the job submitter. The command sequence is then as follows:



Example 10: Message to job receiver and CTRL PR, KCNORPLY=Y



In this case, the job receiver receives an end-of-transaction request and a message from the job submitter without, however, the job submitter passing the send authorization to the job receiver (DATA-PERMITTED=FALSE). The job receiver cannot send any more messages. When the follow-up program unit starts, the job submitter waits after the PEND KP for the receipt of TP-READY.

5.4.9.2 Multiple job receivers

When communicating with more than one job receiver, the situation of the job submitter is essentially the same whatever the physical number of job receivers. It is therefore sufficient to consider a configuration involving one job submitter (A) and two job receivers (B and C).

From the job receiver's point of view, this case is identical to the situations illustrated in the previous section, since the only communication partner known to the job receivers is the job submitter.

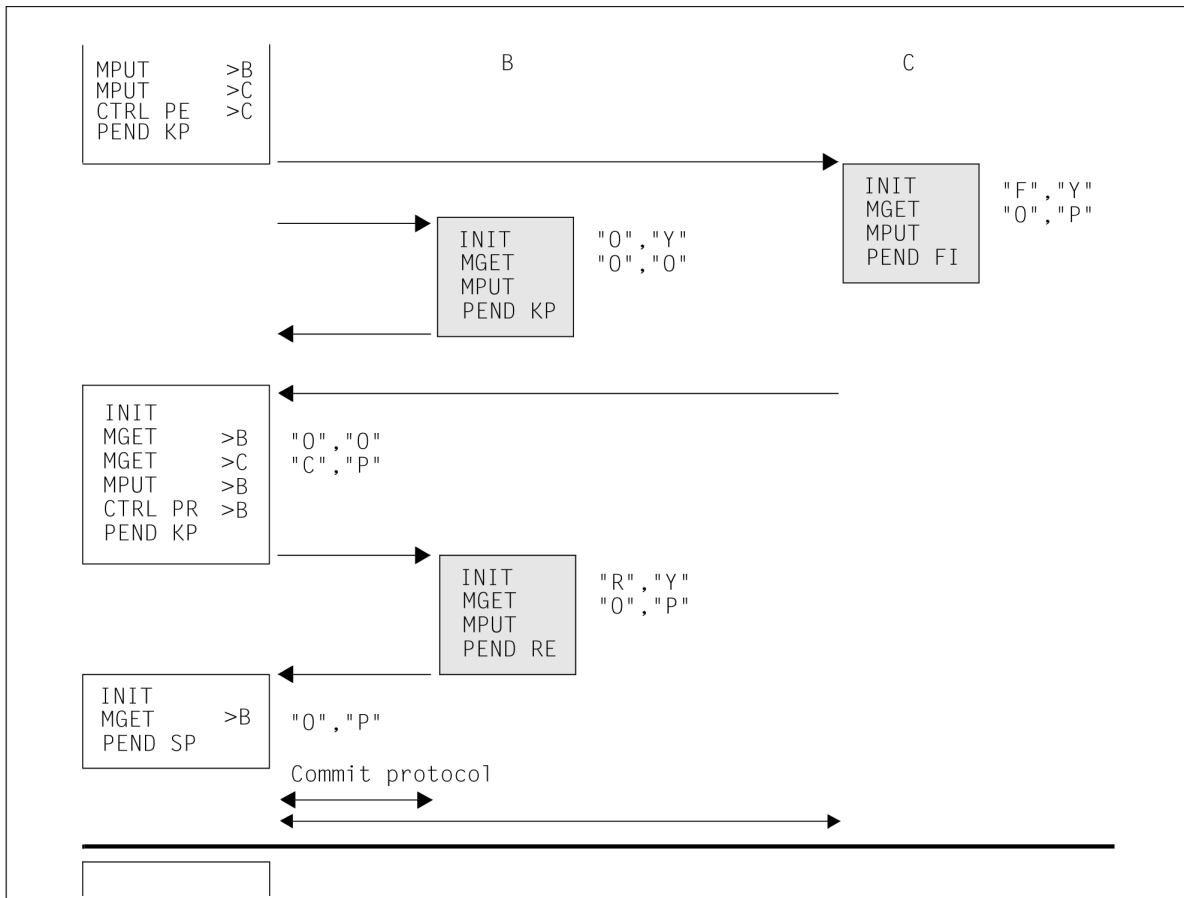
However, this scenario is also not very different for the job submitter. There is simply an increase in the number of possible combinations.

The job submitter can communicate with each individual job receiver as described in the previous section. Additionally, the job submitter can communicate either with one or with multiple job receivers in a single processing step. The follow-up program unit run in the job-submitting service is not started until responses have been received from all the job receivers to which messages were sent in the last processing step.

The job submitter can either use the CTRL call to request individual job receivers to request end of transaction or end of dialog or issue an appropriate PEND call to inform all job receivers of the situation simultaneously.

Since the situation has not changed greatly compared to communication with a single job receiver, a single example will suffice here. For reasons of space, the protocol flow is not illustrated.

Example 11: Multiple job receivers



In this example, job submitter A communicates with job receivers B and C. The dialog with C is to be terminated. However, C has to send a final message to A before terminating. To make this possible, A issues an MPUT and a CTRL PE to partner C. The dialog with partner B is not to be terminated yet. A therefore simply sends a message to B and keeps the transaction open by using PEND KP to terminate the program run.

The "F,Y" specifications inform C that it still has to send a message to A and that the transaction has to be terminated with PEND FI. For B, the transaction and dialog remain open. This is indicated by "O,Y".

In the second program unit run, A now uses CTRL PR to request B to end the transaction. However, A wants to receive the response from B in the current transaction and therefore uses PEND KP to terminate the program run. The stati "R,Y" signal the end of transaction request to B. B then sends a response to A and uses PEND RE to terminate the transaction.

Since both C and B have now requested end of transaction, A can finally terminate the distributed transaction. At the end of transaction the dialog with C is simultaneously terminated, whereas the dialog with B remains open.

5.4.9.3 More complex dialog trees

Finally we shall look at cases in which a service (B) communicates with a job submitter (A) and a job receiver (C) via the OSI TP protocol using Chained Transactions. Compared to the previous cases, only the intermediate node B is in a new situation since it possesses both a job submitter A and a job receiver C.

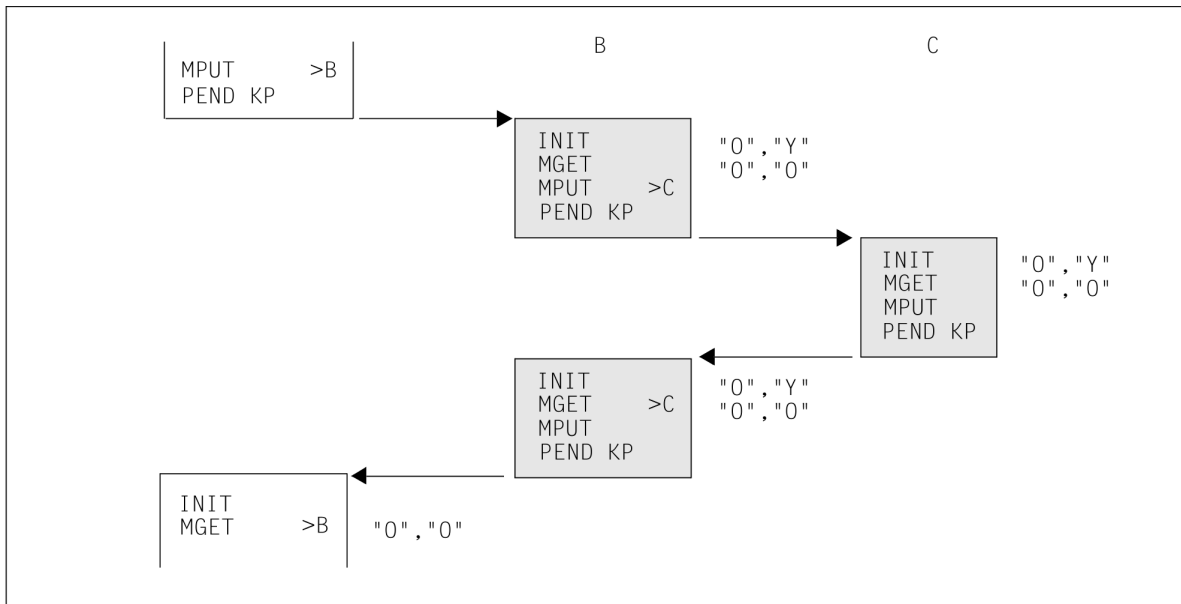
When the OSI TP protocol is used, an intermediate node is not free to decide when an end of transaction or end of dialog is to occur. This also applies to dialogs with its job receiver. The intermediate node B cannot request end of transaction or end of service from job receiver C until B itself has received an end-of-transaction request from its job submitter.

The following examples depict individual, characteristic situations. There are numerous other possibilities which can be constructed by combining the cases described in the sections above.

Data transfer phase

The data transfer phase is the period in which no CTRL calls are issued by any of the partners, and the program runs are terminated exclusively by PEND KP.

Example 12: Data transfer phase in multi-step transfer trees.



B need not always communicate with A and C in alternation, as is the case in this example. B can also conduct multiple dialog steps consecutively with C or communicate exclusively with A before reintegrating C into the communication.

However, it is important to note that B may not send messages to A and C simultaneously. An intermediate node may pass the send authorization either to the job submitter or to one or more job receivers, but not to the job submitter and a job receiver at the same time.

A service may transfer the end-of-transaction send authorization for a maximum of one dialog.

End of transaction

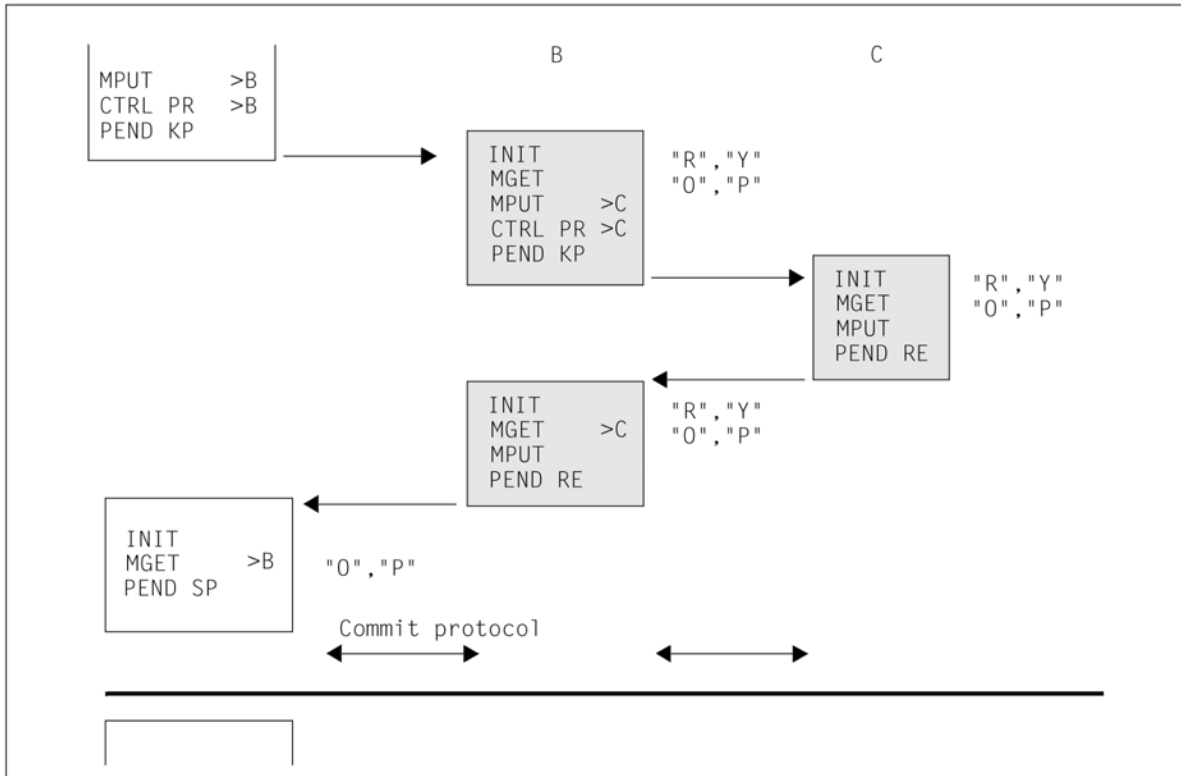
After B has received the end-of-transaction request from A, it has 3 options:

- B can send a message to C and simultaneously request C to terminate the transaction (see also examples 12, 14, 15)

- B can continue the data transfer phase with C and request C to terminate the transaction in a later processing step. (see also example 13)
- B can refrain from further communicating with C in the current transaction and itself request end of transaction. (see also example 16)

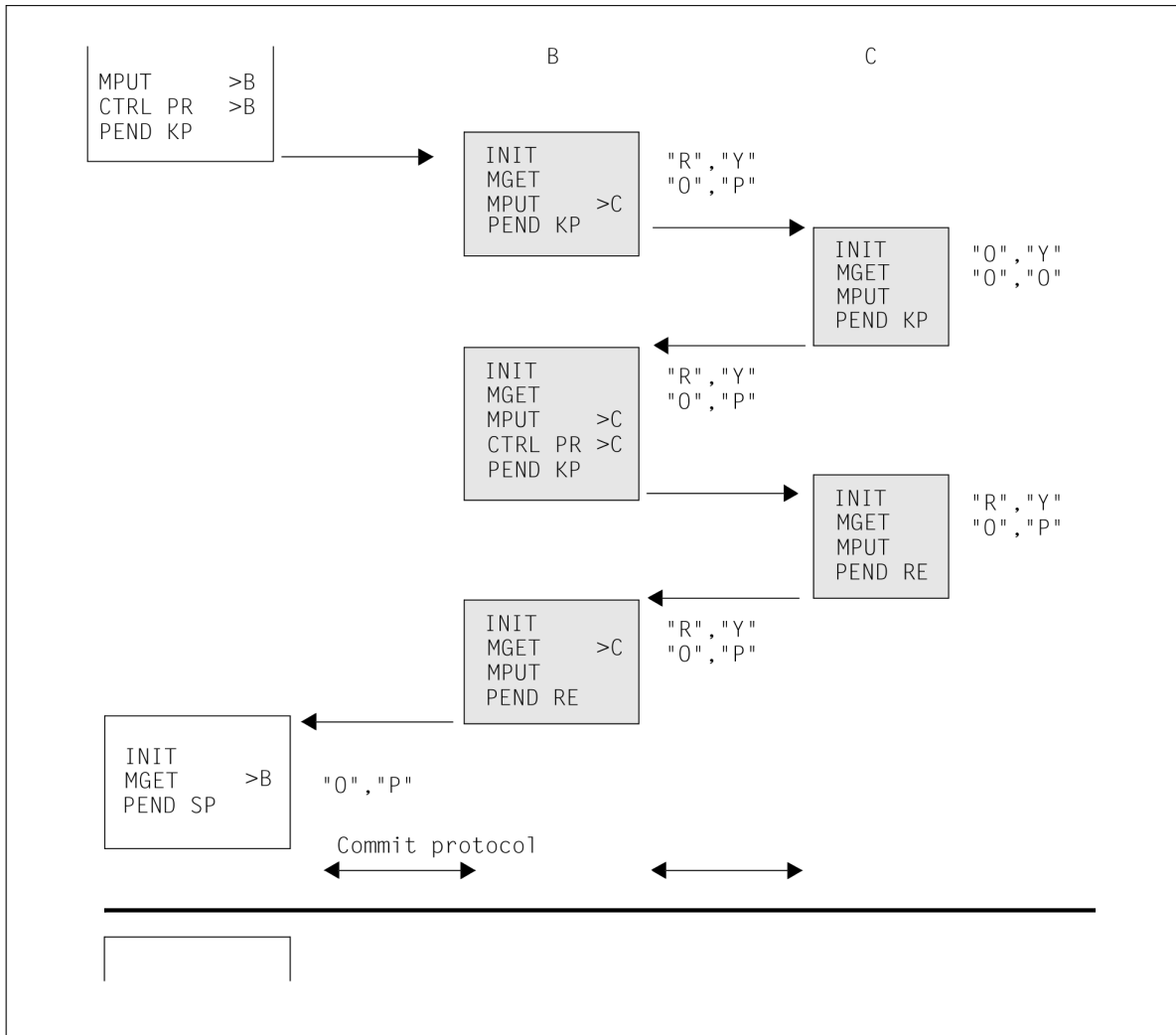
A, B or C may own the end-of-transaction send authorization.

Example 13: End-of-transaction send authorization is owned by A



In the example above, B cannot pass the end-of-transaction send authorization to C since A has not yet passed the end-of-transaction send authorization to B.

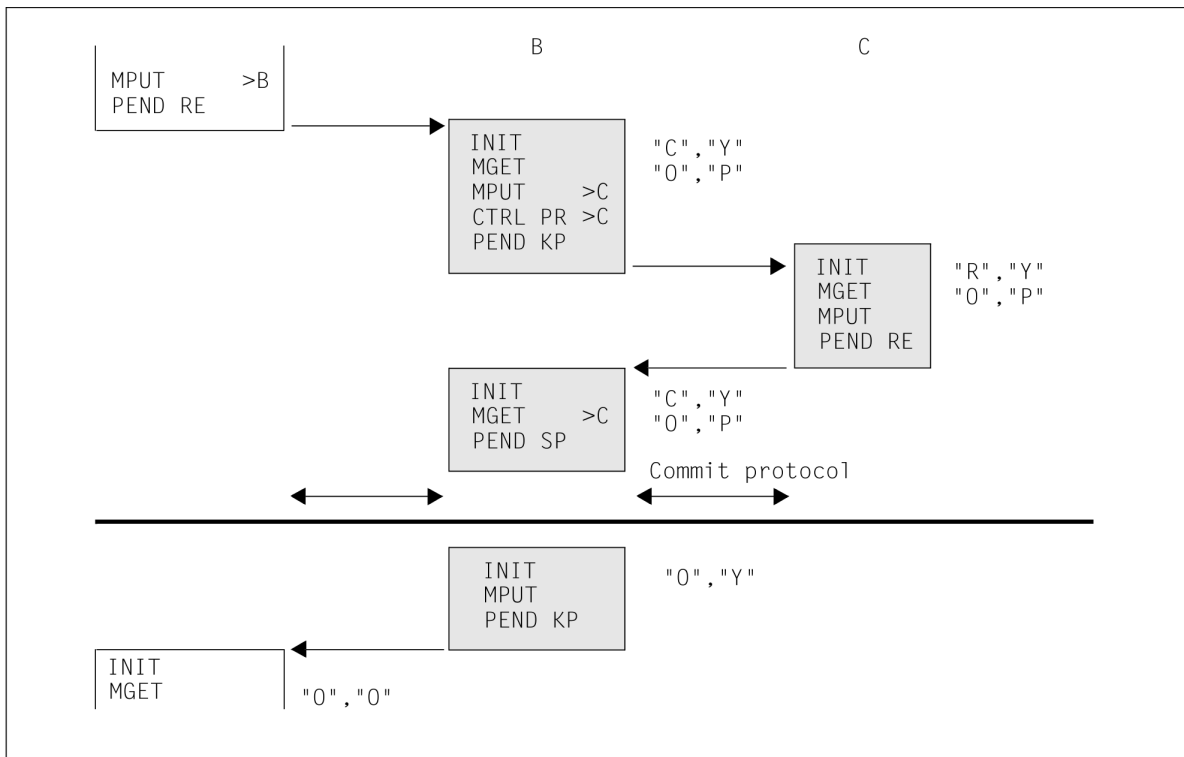
Example 14: B continues the dialog with C - end-of-transaction send authorization is owned by A



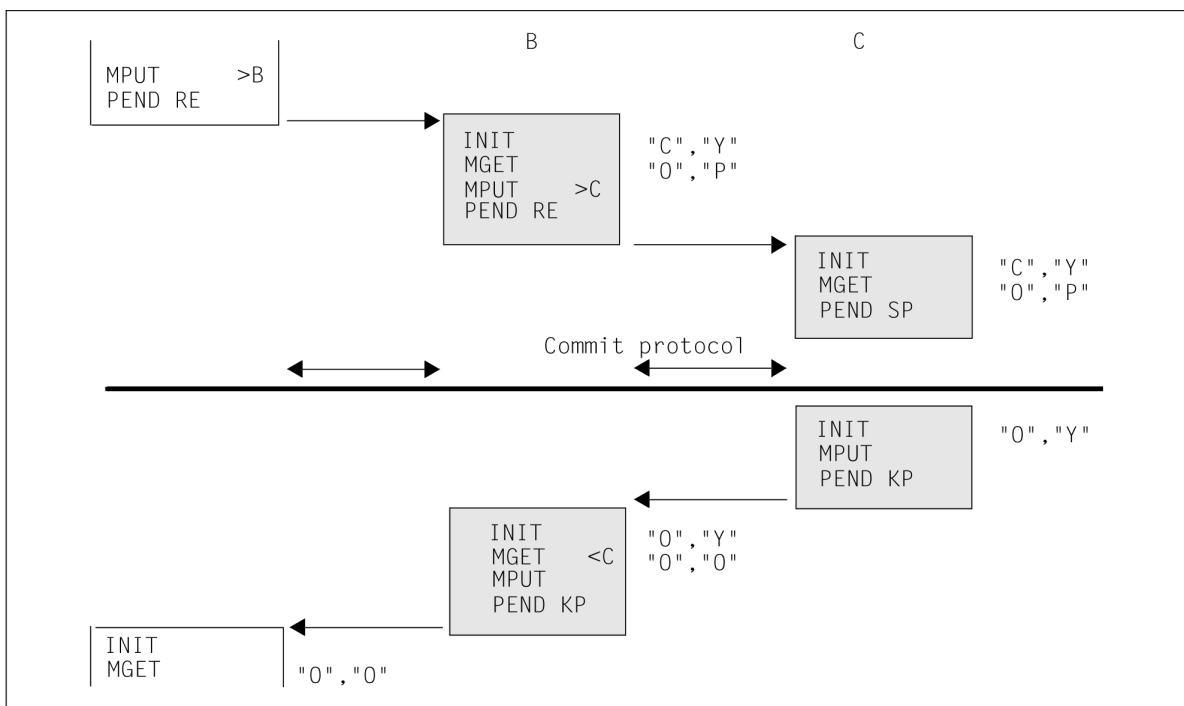
In this example, B does not initially request C to terminate the transaction and, instead, continues the data transfer phase with C. In this example only one more dialog message is exchanged. However, it would be possible to continue the data transfer phase beyond this. In this case, B and C can only use PEND KP to terminate the program runs. At some time B must request C to end the transaction.

In this example, again, B cannot pass the end-of-transaction send authorization to C since A has not yet transferred the end-of-transaction send authorization to B.

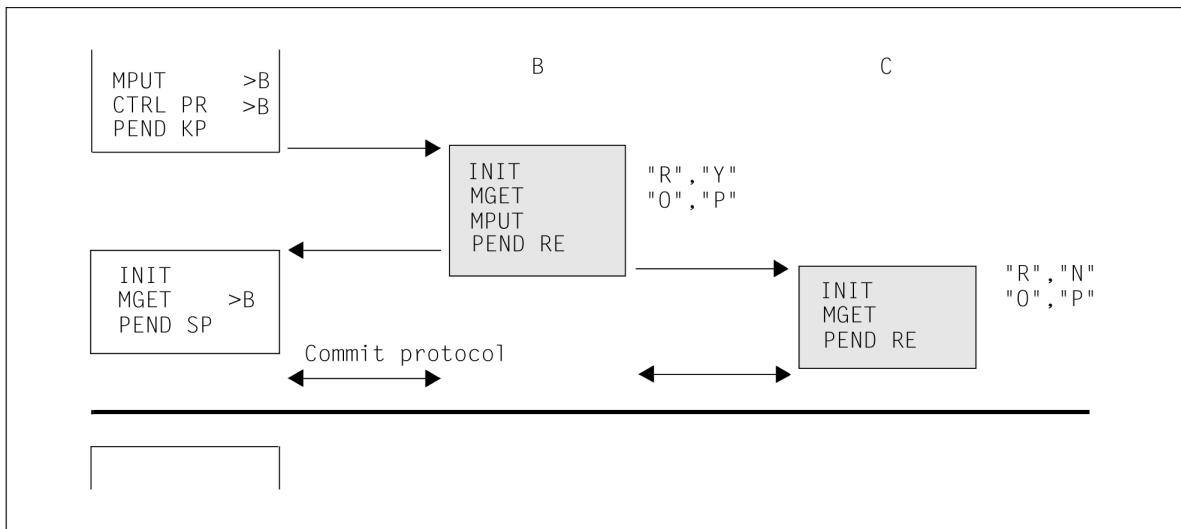
Example 15: End-of-transaction send authorization is owned by B



Example 16: End-of-transaction send authorization is owned by C



Example 17: No message to job receiver before end of transaction



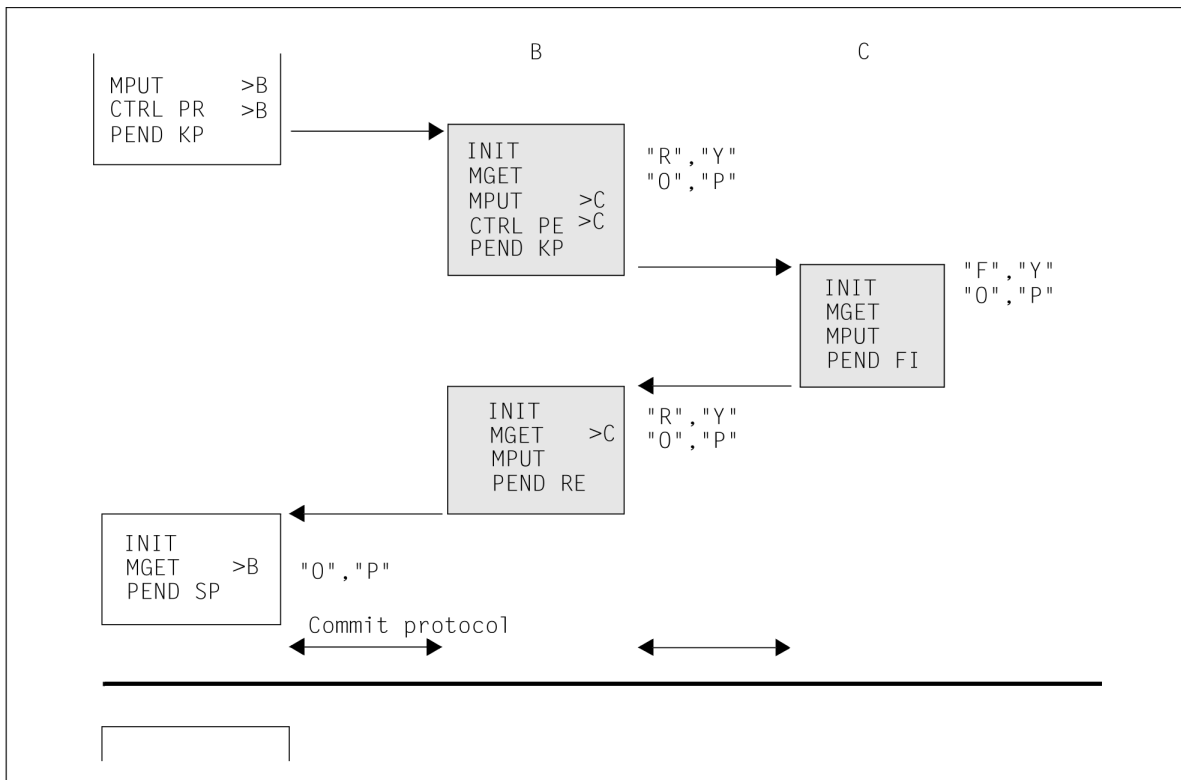
In this example, B refrains from sending another message to C in the current transaction, and requests end of transaction immediately.

After PEND RE from node B, an MPUT message is sent to A and a PREPARE protocol element is sent to C. This requests C to terminate the transaction. C does not then receive any further user messages. The MGET call at C simply reads the status of the dialog with B. This call can be omitted.

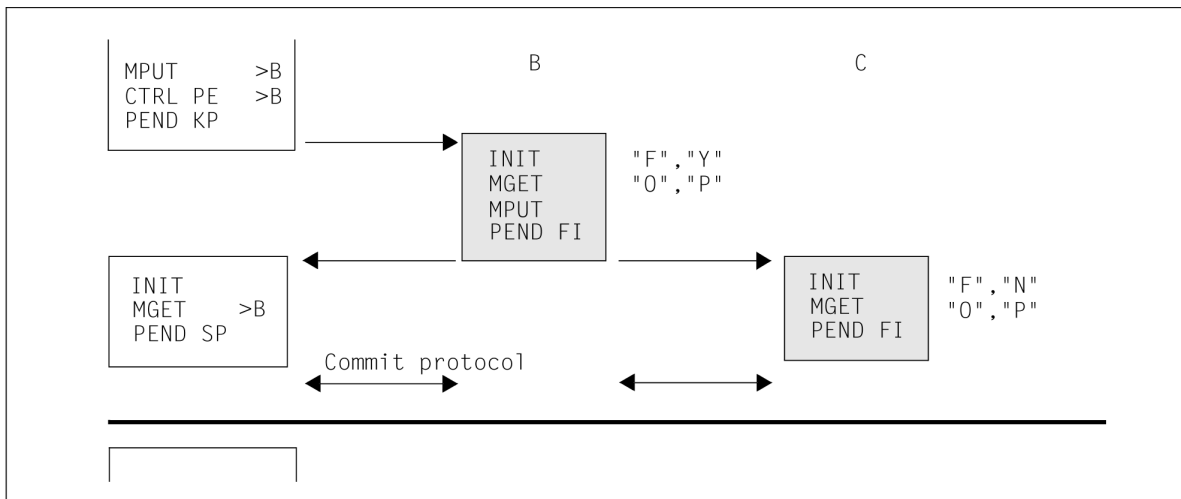
End of dialog

An intermediate node can bring about the job-submitter-based end of dialog in the same way as an end of transaction. These possibilities are depicted in the two examples below.

Example 18: B first terminates the dialog with the job receiver.



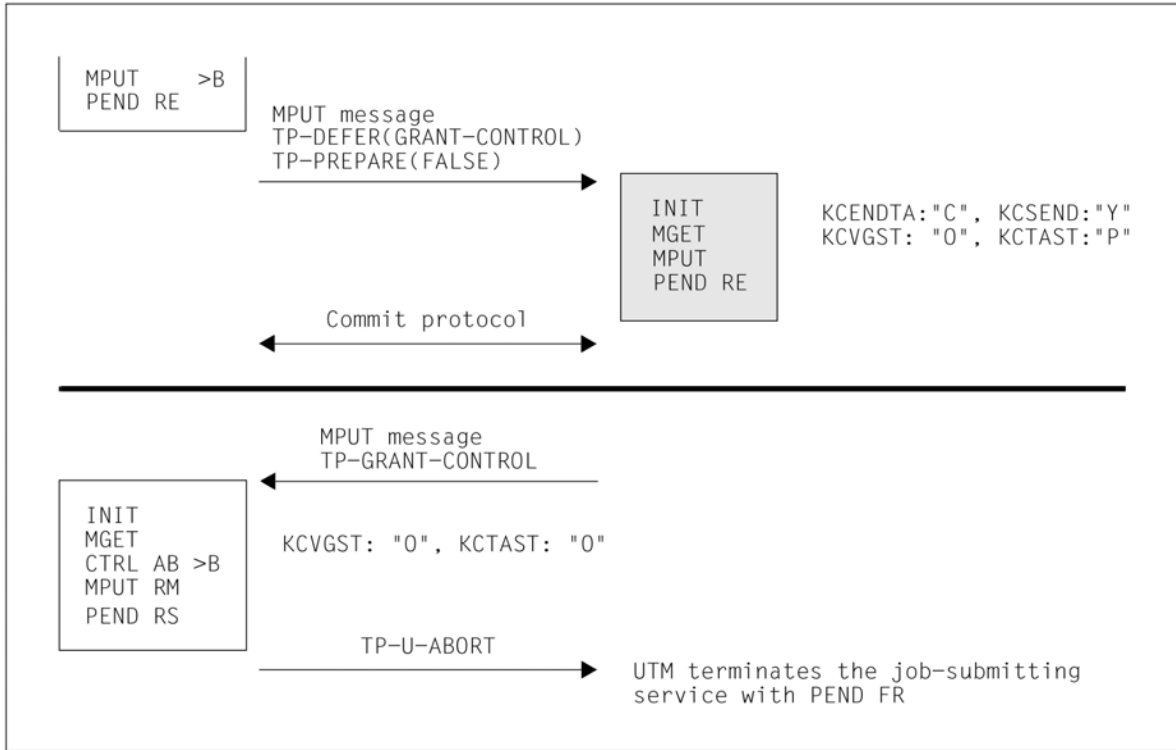
Example 19: Simultaneous end of dialog with job receiver and job submitter.



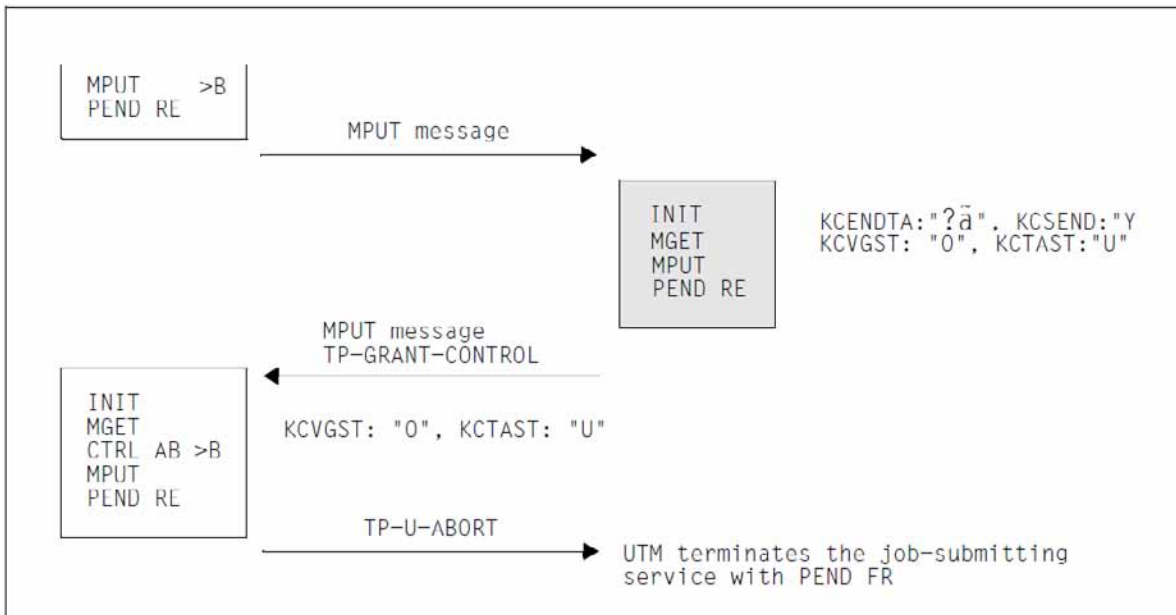
5.4.9.4 Using CTRL AB to terminate a job receiver

CTRL AB terminates a job-receiving service abnormally. The job submitter must roll back the distributed transaction after a CTRL AB for a job receiver for which the functional unit Commit is selected. No rollback is necessary for a job receiver dialog without Commit.

Example 20: Terminating a dialog for which the Commit FU is selected.



Example 21: Terminating a dialog for which Commit FU is not selected



5.5 UTM-controlled queues in distributed processing

A job-submitting service can use the FPUT or DPUT call to send an asynchronous job to a remote asynchronous service (Remote Queuing). The job-submitting service may either be a dialog or an asynchronous service.

openUTM uses two local queues for asynchronous jobs to a remote applications: one queue is located in the sending application, the other in the receiver. This deferred delivery principle makes sure that distributed message queuing under openUTM is entirely independent of whether or not a connection is currently established. If no connection can be established, the job remains in the local send queue until the connection is established. The following applies once the connection has been established.

- With LU6.1, the jobs are transmitted to the partner immediately.
- With OSI TP, it may be some time before the jobs are transmitted. This time is limited by the value generated in MAX CONRTIME. Note that the time is set to 10 minutes if CONRTIME=0.

If a serious error occurs while transmitting a job, i.e. while the connection is open, then the job is deleted from the local send queue but is not entered in the corresponding message queue of the partner application. In this case, a K239 message is output in the local application.

A serious error that results in the loss of the job may occur, for example, if the job is sent to a TAC which is locked in the partner application. The exact cause can be identified from the K086 (LU6.1) or K119 (OSI TP) message which is output in the partner application:

Loss of a job can be prevented by activating saving of messages in the local dead letter queue in the local application for the LPAP or OSI-LPAP partner, see section [“Dead Letter Queue”](#).

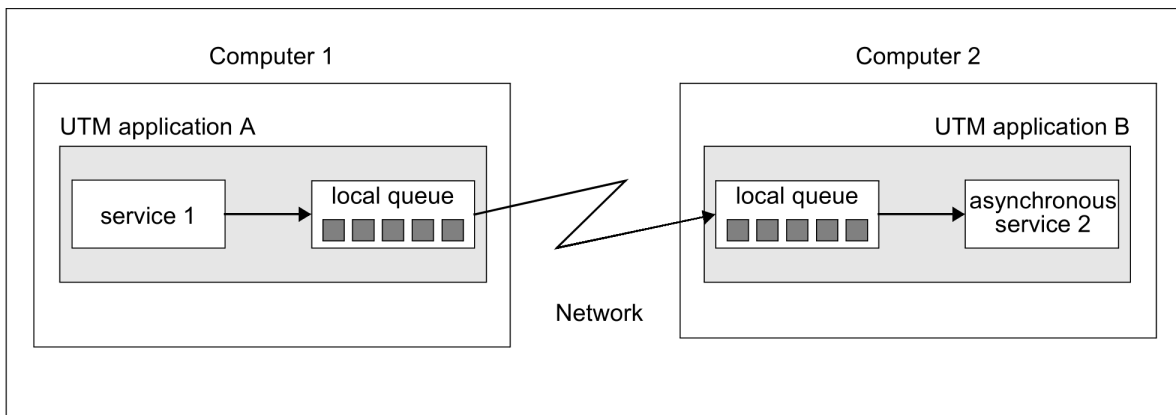


Figure: Remote queuing with openUTM

5.5.1 Job submitter side

You use an **APRO AM** call to address the job-receiving service. Enter the service ID in the KCPI field.

In the case of distributed processing via OSI TP you can use the APRO call to select whether or not to transfer an asynchronous job with global transaction management. If global transaction management is used, openUTM ensures that the job is transferred precisely once as long as it is not lost during transmission due to a serious error (see "[UTM-controlled queues in distributed processing](#)").

In the event of a connection failure, asynchronous jobs without global transaction management are may sometimes be transferred more than once.

After an APRO AM call, the job-submitting service can:

- enter a service identification as the destination in KCRN and use FPUT to send an asynchronous job or DPUT to send a time-driven asynchronous job to the corresponding remote service.
- use MCOM BC to define the start of a job complex and use DPUT to send an asynchronous job (basic job) to the partner application within the complex and to create the associated positive or negative confirmation jobs. The confirmation jobs are processed by the local application.
use MCOM BC to define the complex ID and enter the service Id in KCRN. For DPUT, you must then enter the complex ID in KCRN.

You **must** issue an FPUT or DPUT call with this service ID within the program unit which addresses the remote service with APRO AM, otherwise openUTM aborts the service with KCRCCC=86Z and releases the service ID when PEND is called.

The service ID is released in the job-submitting service in the following cases:

- after a successful FPUT NE or DPUT NE call
- on the next PEND call (also PEND KP and PEND PA/PR)
- after a RSET call
- after the return code 40Z following an FPUT or DPUT call
- in job complexes with this service ID: When calling MCOM EC or after a return code 40Z following MCOM BC or after calling DPUT

Once released, this service ID can be used for another job submitter/job receiver relationship in the job-submitting service.

The job entry in the job submitter is deleted from the message queue as soon as it has been successfully transferred and inserted into the corresponding message queue of the partner application. Depending on the processing result, the positive or negative confirmation job is then started when message complexes are used.

5.5.2 Job receiver side

Here an asynchronous job for a partner application is handled as if it had been created by a service in your own application. Asynchronous jobs from services in the local application and asynchronous jobs issued by remote services are located in a shared message queue assigned to the asynchronous TAC. An asynchronous service is started for each job in turn, as resources become available. The asynchronous service uses the entry in the KCTERMN field of the KB header to identify whether or not the job submitter is a remote service.

Asynchronous services for remote queuing are structured in exactly the same way as for local queuing (see "[Structure of an asynchronous service](#)"). However, in distributed processing via OSI TP another possibility exists: asynchronous jobs to dialog services.

Asynchronous jobs to remote dialog services (only via OSI TP)

When using the OSI TP protocol for an asynchronous job for which APRO was used to specify global transaction management, the job receiver may be a **dialog** service.

After receipt of an asynchronous job for a dialog service, the service is immediately started in the partner application rather than being inserted into a message queue like a job to an asynchronous service. In the application of the job submitter, the job is not deleted from the message queue until the dialog service is terminated. Depending on the processing result, the positive or negative confirmation job is then started when message complexes are used.

A dialog service which is started by an asynchronous job must use PEND FI to terminate the transaction and may not contain an MPUT to the job submitter (KCENDTA=F and KCSEND=N).

5.6 Service-controlled queues in distributed processing

Messages to can also be transferred to TAC queues of remote applications with fail safety by means of LU6.1 and OSI TP. Generation and programming are similar to when you send jobs to dialog or asynchronous TACs in remote applications (see "[Addressing remote services](#)").

Generation

In an LTAC statement, the name of a TAC queue in the remote application is assigned to a local LTAC name as the RTAC name.

```
LTAC REMOTEQ, RTAC=name-of-TAC-queue-in-remote-application
```

Programming

The message is addressed by means of an APRO AM call and sent by means of a subsequent FPUT call.

```
INIT
...
APRO AM, KCPI=>VGID, KCRN=REMOTEQ
FPUT NE, KCRN=>VGID
...
PEND FI
```

6 Program structure in communication with transport system applications

This chapter describes the points you have to take into account when programming communication with transport system applications (= TS applications).

Overview

A transport system application is connected as a client with partner type APPLI or SOCKET to a UTM application. For partner type SOCKET, the transport system end point has to be generated with T-PROT=(SOCKET [, *ANY|*USP[, SECURE]) and communication above TCP/IP must take place using the UTM socket protocol (USP). You can generate the transport system application as follows:

- Explicitly using a PTERM/LTERM statement:

```
PTERM . . . ,PTYPE=APPLI/SOCKET[ , BCAMAPPL= socket-application-name ]
LTERM . . .
```

- As LTERM pool using a TPOOL statement:

```
TPOOL . . . ,PTYPE=APPLI/SOCKET[ , BCAMAPPL= socket-application-name ]
```

For TS applications with SOCKET type, you have to generate an additional application name used as transport system end point:

```
BCAMAPPL socket-application-name ,T-PROT=(SOCKET[ , *ANY|*USP[ , SECURE])
```

From a TS application of the type APPLI it is possible in the UTM application to:

- start a service
- create a message for a TAC queue or temporary queue

You will find information on generating TS applications in the openUTM manual “Generating Applications”.

6.1 Communication with TS applications of the type APPLI

For an input message from the TS application of type APPLI applies:

- If a message sent to the UTM application is intended to start a service, the TAC must be at the beginning of the message.
- If the message is to be appended to the message queue for a TAC queue or a temporary queue, the name of the queue must be at the beginning of the message. If the message is going to a temporary queue, no TAC or LTERM may exist in the application under the name of the temporary queue.
- If the TAC is shorter than 8 characters, it must be separated from the rest of the message by at least one space.
- If the specified TAC or the name of the queue is invalid, the event service BADTACS is started, provided it has been generated. Otherwise, the message K009 is sent to the TS application, unless a separate message module is being used in which PARTNER has not been generated as the destination for the message K009.

If the TS application starts a service then this service can read the message with the KDCS call MGET or FGET. If the TS application sends a message to a service-controlled queue then any service can read the message with the KDCS call DGET. If, during a read call, the KCLA length is shorter than the length of the message segment, only the requested part is read; the rest of the message is lost. The return code 01Z indicates that the message has not been read in its entirety.

Please note that the TS application must provide the name of the TAC or the queue in the “correct” code for the UTM application, i.e. in EBCDIC for a UTM application on BS2000 systems and in ASCII for a UTM application on Unix, Linux or Windows systems.

Alternatively, in applications on Unix, Linux or Windows systems, code conversion can be generated for the connection to the TS application (operand MAP=SYS1/SYS2/SYS3/SYS4 in the PTERM or TPOOL statement).

6.2 Communication with socket USP applications

openUTM works on a message-oriented basis and does not start a program unit until a complete message has been received for the program unit. The socket interface is a byte-stream interface.

openUTM therefore requires a communication protocol above and in addition to TCP/IP in order to detect message limits. The `UTM socket protocol (USP)` provided by openUTM serves this purpose and enables the byte streams received via the socket interface to be converted to messages (see "[Structure of the socket protocol header](#)"). TCP/IP is required as the transport protocol.

Sample programs

The socket-client sample programs SOC BSP and USOCV6 and a program unit SOC MIRR for socket partners are supplied with openUTM. SOC MIRR ("socket mirror") returns the received messages to the socket client.

On BS2000 systems, you can find the sources and the object modules for the sample programs in the library SYSLIB.UTM.070.EXAMPLE.

On Unix and Linux systems, SOC BSP (source `socbsp.c`), USOCV6 (source `usocv6.c`) and SOC MIRR (source `socmirr.c`) form part of the sample application. You will find the sources under `utmsample/soc-c` or `utmsample/utm-c` (`utmsample` = directory containing the sample application).

On Windows systems, SOC BSP (source `socbsp.c`), USOCV6 (source `usocv6.c`) and SOC MIRR (source `socmirr.c`) are components of the Quick Start Kit . The sources are located in the directory `utmpath\utmsample\soc-c` or `utmpath\utmsample\utm-c`.

6.2.1 Input messages for openUTM

In the case of input messages of socket applications, a corresponding protocol header must be set up in the partner application, and this must precede each message segment or fragment. The protocol header is truncated and not transferred to the program unit.

The following applies to the data that comes after the protocol header:

- If a service is to be started with a message sent to openUTM, the TAC must be at the beginning of the message.
- If the message is to be inserted in the message queue of a TAC queue or of a temporary queue, the name of the queue must be at the beginning of the message. If the message goes to a temporary queue, there must be no TAC or LTERM in the application under the name of the temporary queue.
- If the TAC is shorter than eight characters, it must be separated from the rest of the message by at least one blank.
- If the specified TAC or the name of the queue is invalid, the BADTACS event service is started (provided it has been generated). If not, message K009 is sent to the socket application, unless a separate message module is used in which PARTNER has not been generated as the message destination for message K009.

If the TS application starts a service then this service can read the message (segments) or messages with the KDCS call MGET or FGET. If the TS application sends one or more messages to a service-controlled queue then any service can read the message (segments) or messages with the KDCS call DGET. The following then applies.

- If the KCLA length is shorter than the length of the message segment at the MGET call, only the requested part is read; the rest of the message is not lost, however. The return code 02Z indicates that the message segment has not been read in its entirety. The rest of the message segment can be read with the next read call, another message segment with the next read call but one, and so on.
- If the KCLA length is shorter than the length of the message segment at the DGET/FGET call, only the requested part is read; the rest of the message is lost. The return code 01Z indicates that the message segment has not been read in its entirety. A further message segment is read with the next read call.

If all the message segments are read, this is indicated by the return code 10Z.

If no code conversion has been generated for the connection to the socket partner (PTERM or TPOOL statement, operand MAP=USER), then the socket application must supply the name of the queue or queues in the "correct" code for the UTM application, i.e. in EBCDIC for a UTM(BS2000) application and in ASCII for a UTM application on Unix, Linux or Windows systems.

6.2.2 Output messages of openUTM

When messages are sent to socket partners, each message segment or fragment must be sent by means of a separate MPUT NT/NE call. At each MPUT call, a separate message segment is created, even if zero is specified as the length. A message with a length of zero is only sent, however, if a USP header is created automatically for the message to be sent and is placed in front of it (see the table below). The exception is that if the program unit contains only one MPUT call, no message is sent, regardless of the value of the USP-HDR parameter.

If the socket partner expects a USP header when it receives a message then you can define during generation that openUTM should automatically create a USP header for messages to the socket partner and precede them with this header.

This is specified at generation using the USP-HDR= operand in the PTERM or TPOOL statement:

- for all messages, i.e. K messages + MPUT/FPUT messages (USP-HDR=ALL)
- for K messages only (USP-HDR=MSG)
- no header (USP-HDR = NO)

If no code conversion has been generated for the socket partner (MAP=USER operand in the PTERM or TPOOL statement), you can also generate the USP header in the program unit itself and prefix it to the message.

For information on generating sockets applications, please refer to the openUTM manual "Generating Applications"

Exchanging long messages

Input messages and dialog output messages of any length can be exchanged with socket partners. If an entire message is longer than 32767 bytes (output) or 32000 bytes (input), the message must be **fragmented** (i.e. it must consist of several message segments). The maximum length of each message segment is 32767 bytes (including the USP header) at output and 32000 bytes at input.

Message segments can be identified by the fact that the relevant flag field and the corresponding message type in the USP header are set (see below). In the case of outputs, the program must set these values.

Fragmented input messages must be read using a corresponding number of MGET/FGET/DGET NT calls (see "[Communication via socket connections](#)"). Fragmented dialog output messages must be sent using a corresponding number of MPUT NT calls.

Asynchronous output messages (FPUT/DPUT) cannot be fragmented. Their length must not exceed 32700 bytes.

6.2.3 Structure of the USP header

The header contains the identifier, two version fields, a flag field, a type field and a length field. openUTM expects the protocol described on the input side. This has the following structure:

Identifier ASCII, 4 bytes	Major version 1 byte	Minor version 1 byte	Flags 1 byte	MsgType 1 byte	MsgSize 4 bytes	Data Max. 31988 bytes
 UTMS(55544D53)	 01	 01		 Message type	 0000xxxx	 Data

Explanation

Identifier

The identification field must always contain the ASCII string "UTMS" (=0x55544D53) for openUTM.

Major version

The major version field must always contain the value 0x01.

Minor version

The minor version field must always contain the value 0x01.

Flags

The flag field is an information field. Only bit 0x02 is evaluated: if it is set, the message is followed by another fragment. If it is not set, it is not followed by a fragment. All the other bits are reserved for future versions.

MsgType

The type field can contain the values 0x00, 0x01 or 0x07:

- Receive messages from the client:
In the case of unfragmented messages, the client sets the value 0x00 for `MsgType`. In the case of fragmented messages, the client sets the value 0x00 for `MsgType` when the first fragment is received (bit 0x02 is set in the flag field). For the fragments that follow, the value 0x07 is set for `MsgType` (bit 0x02 remains set). Bit 0x02 is not set for the last of these fragments.
- Send messages to the client:
In the case a USP header is created (e.g. with USP-HDR=ALL), openUTM sets the value 0x01 for `MsgType` when the first fragment is sent and the value 0x07 for fragments that follow.

MsgSize

The length field `MsgSize` contains the length of the message or message segment, including the header. This length must not exceed 32000 bytes on the input side and 32767 bytes on the output side. The message length is transferred in network byte order (big endian). The C functions `htonl` (host to network long) and `ntohl` (network to host long) can be used to carry out conversions between the local view and the network view.

Examples

1. The client sends messages to openUTM, see the sample source file SOCBSP.C shipped with the product:

- The client sends one message (without fragmentation)
- The client sends two message segments
- The client sends three message segments

Number of message segments	Identifier	Major version	Minor version	Flag	MsgType	Size
1 whole message	55544D53	01	01	00	00	0000nnnn
2 segments						
• segment 1	55544D53	01	01	02	00	0000nnnn
• segment 2	55544D53	01	01	00	07	0000mmmm
3 segments						
• segment 1	55544D53	01	01	02	00	0000kkkk
• segment 2	55544D53	01	01	02	07	0000nnnn
• segment 3	55544D53	01	01	00	07	0000mmmm

2. The server sends messages to the client (USP header is created):

- one whole message (without fragmentation)
- three message segments

Number of message segments	Identifier	Major version	Minor version	Flag	MsgType	Size
1 whole message	55544D53	01	01	00	01	0000nnnn
3 segments						
• segment 1	55544D53	01	01	02	01	0000kkkk
• segment 2	55544D53	01	01	02	07	0000nnnn
• segment 3	55544D53	01	01	00	07	0000mmmm

kkkk, *nnnn*, *mmmm* are the lengths of the different message segments.

7 KDCS calls

This chapter gives you all the information you need to use the KDCS program interface in your program. You call the openUTM linkage program with the KDCS call. On the basis of the entries in the KDCS parameter area, openUTM recognizes and performs the desired function.

7.1 Complete overview of KDCS calls

UTM calls implement the KDCS interface as standardized under DIN 66 265 ("Interfaces of a Kernel for Transaction-oriented Application Systems"). The UTM program interface is an upward-compatible extension to this DIN standard. The table below lists these extensions.

CALL	Included in DIN 66 265	Extensions to DIN 66 265
APRO	no	Distributed processing
CTRL	no	Distributed processing (only for OSI TP)
DADM	no	Administration of message queues (asynchronous jobs)
DGET	no	Read from service-controlled message queues
DPUT	yes	Confirmation jobs and user information
FGET	yes	Distributed processing
FPUT	yes	Distributed processing
GTDA	yes	none
INFO	no	Information services
INIT	yes	Distributed processing
LPUT	yes	none
MCOM	no	Definition of job complexes
MGET	yes	Distributed processing
MPUT	yes	Distributed processing
QCRE	no	Create temporary queue
QREL	no	Delete temporary queue
PADM	no	Administration of printers and printer output
PEND	yes	Distributed processing, PEND KP/PS/FC/SP/RS/FR not contained in DIN 66 265
PGWT	no	Program management
PTDA	yes	none
RSET	no	Rollback operation
SGET	yes	none
SIGN	no	Signing on and off, changing password, checking authorization data

CALL	Included in DIN 66 265	Extensions to DIN 66 265
SPUT	yes	none
SREL	yes	none
UNLK	no	Unlocking storage areas

The table below shows the KDCS calls and their functions.

CALL	Function	Function group
APRO	Address job-receiving service	Message communication (with distributed processing)
CTRL	Control OSI TP dialogs	Message communication (with distributed processing)
DADM	Administer asynchronous jobs	Management of message queues and printers
DGET	Read messages from a service-controlled message queue	Message communication - message queuing
DPUT	Generate time-driven asynchronous job and confirmation jobs	Message communication - message queuing
FGET	Receive asynchronous message	Message communication - message queuing
FPUT	Generate asynchronous job	Message communication - message queuing
GTDA	Read from TLS	Memory management
INFO	Request information	Information services
INIT	Signing on a program to openUTM	Program management
LPUT	Write to log file	Logging facility
MCOM	Define job complex	Message communication
MGET	Receive dialog message	Message communication - dialog
MPUT	Send dialog message	Message communication - dialog
QCRE	Create temporary message queues	Management of temporary message queues
QREL	Delete temporary message queues	Management of temporary message queues
PADM	Control printers and printer outputs	Management of message queues and printers
PEND	Terminate program	Program management

CALL	Function	Function group
PGWT	Set wait point in a program unit run	Program management
PTDA	Write to TLS	Memory management
RSET	Roll back requested changes and operations	Program management
SGET	Read from secondary storage area	Memory management
SIGN	Sign on and off, change password, check authorization data	Sign-on management
SPUT	Write to secondary storage area	Memory management
SREL	Release secondary storage area	Memory management
UNLK	Unlock TLS, ULS or GSSB	Memory management

The next table lists the function groups and the calls associated with them.

Function group	Associated UTM calls
Sign-on management	SIGN
Program management	INIT, RSET, PEND, PGWT
Message communication - dialog	MGET, MPUT
Message communication - message queuing	MCOM, DGET, DPUT, FGET, FPUT
Management of message - queues and printers	DADM, PADM
Management of temporary - message queues	QCRE, QREL
Memory management	GTDA, PTDA, SGET, SPUT, SREL, UNLK
Information services	INFO
Logging facility	LPUT
Distributed processing	APRO, CTRL, DPUT, FPUT, INIT, MCOM, MGET, MPUT, PEND, RSET, PGWT

After each call (except PEND) openUTM returns information in the KDCS communication area.

The fields of the KDCS parameter area set prior to a call or returned after its execution have particular names. These are meant to help you deal with the KDCS interface and its description. Their use also enhances the maintenance and transferability of programs. The appendix gives an overview of all operand fields and their use in the various calls.

7.2 Comments on the description of the KDCS calls

This section describes all the KDCS calls in alphabetical order. This makes it easier for you to look them up.

Every call description consists of 4 parts:

- First, the functions of the call are described.
- Then there is a schematic diagram of the call with all necessary entries. The fields to which you have to assign a value before the call are grayed:

gray	you must assign a value to this field before the call
------	---

The corresponding C/C++ macros are also listed for each call. For a detailed description of these macros refer to [section "C/C++ macro interface"](#).

- This diagram is followed by the description of the statements in the KDCS parameter area and in the 2nd parameter, as well as the return information from openUTM.
- Finally the particularities of the call are explained.

If "—" is entered in a table, then the entry is irrelevant for the function concerned.

i The field names of the KDCS interface for COBOL and C/C++ are mostly identical and differ only in the rules for lower case/upper case specification. In cases where further differences exist, the field name for C/C++ is printed after the COBOL field name (separated by a slash), e.g. "KCTAG/kcday".

i The return code 79Z is a general error code which indicates that the value in the field KCOP=operation code has an invalid value. It cannot therefore be assigned to any operation code.

7.3 APRO Address job-receiving service

The APRO call (address program) enables you to address a job-receiving service or a TAC queue in the job-submitting service. The APRO call is only applicable with distributed processing with UTM-D. Data is sent to the job-receiving service using either MPUT or FPUT/DPUT. In these calls the receiver is specified by means of the service identifier defined in the APRO call.

Setting the 1st parameter (KDCS parameter area)

The following table shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area						
	KCOP	KCOM	KCLM	KCRN	KCPA	KCPI	KCOF
Address a dialog service	"APRO"	"DM"	0/19/58	LTAC name	(OSI-)LPAP name / Master-LPAP name / blanks	service ID	Permitted OSI function
Address an asynchronous service or a TAC queue	"APRO"	"AM"	0/19/58	LTAC name	(OSI-)LPAP name / Master-LPAP name / blanks	service ID	Permitted OSI function

The entry in the KCPA field depends on the type of addressing involved:

- for single-step addressing the field must contain blanks
- for double-step addressing the field must contain the name of the partner application ((OSI-)LPAP name or Master-LPAP name).

Further information on single and double-step addressing of job-receiving service with distributed processing can be found in the openUTM manual "Concepts and Functions".

Setting the 2nd parameter (selecting special OSI TP function combinations)

The second parameter area is only used for communication via the OSI TP protocol. It allows you to specify function combinations other than those available via the standard selection using the KDCS KCOF parameters. It also allows you to select whether SIGNON data should be transferred to the job-receiving service. A language-specific data structure is available for the second parameter area: for COBOL in the KCAPROC COPY element, for C/C++ in the *kcapro.h* include file.

If the second parameter area is used, you must specify the values 19 or 58 in the field KCLM for the length of the data structure and the field KCDF must contain the value "O".

Setting the parameters in the KDCS parameter area	
Field name in the KDCS parameter area	Contents
KCOP	"APRO"
KCOM	"DM"/"AM"
KCLM	0/19/58
KCRN	LTAC name
KCPA	(OSI-)LPAP name / Master-LPAP name / blanks
KCPI	service ID
KCOF	OSI functions

Setting the parameters in the second parameter area (only for KCOF=0)	
Field name in the 2nd parameter area	Contents
KCVERS	Version number of data structure
KCFUPOL	Polarized FU (Y)
KCFUHSH	Handshake FU (Y/N)
KCFUCOM	Commit FU (Y/N)
KCFUCHN	Chained FU (Y/blanks)
KCFUFILL	empty - for future extensions
KCSECTYP	Security type (N/S/P)
KCUIDTYP	Data type of user ID (P/T/O)
KCUIDLTH	Length of user ID
KCUSERID	User ID
KCSECFIL	empty - for future extensions
KCPWDTYP	Data type of the password (P/T/O)
KCPWDLTH	Length of the password
KCPSWORD	Password

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Second parameter area

C/C++ macro calls	
Macro names	Parameters
KDCS_APRODM / KDCS_APROAM	(kcrn,kcpa,kcpi)
KDCS_APRODM_OSI / KDCS_APROAM_OSI	(kcrn,kcpa,kcpi,kcof)
KDCS_APRODM_OSI_O / KDCS_APROAM_OSI_O	(nb,kclm,kcrn,kcpa,kcpi)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

You can enter the following information for the APRO call in the KDCS parameter area:

KCOP

In the KCOP field, enter the APRO operation code.

KCOM

In the KCOM field, enter the operation modifier:

- DM (Dialog message) for addressing a dialog service
- AM (asynchronous message) for addressing an asynchronous service or a TAC queue.

KCLM

In the KCLM field, enter the length of the 2nd parameter area:

- length zero, if no second parameter area is used
- length 19, if a second parameter area is used and the "N" or "S" security type is selected
- length 58, if a second parameter area is used and "P" security type is selected.

KCRN

In the KCRN field, enter the logical transaction code (LTAC name) of the job-submitting service.

KCPA

In the KCPA field, you may have to identify a partner application depending on the type of addressing:

- enter the logical name of the partner application in the case of double-step addressing, i.e. the LPAP name, OSI-LPAP name or master LPAP name of an OSI-LPAP or LU6.1-LPAP bundle.
- enter blanks for single-step addressing (the name of the partner application is in this case taken from the generation statement LTAC).

The partner application entry in KCPA has priority over the partner application specified in the LTAC statement at generation.

KCPI

In the KCPI field, assign the service ID to be used by the job-submitting service in the MPUT, MCOM, FPUT, DPUT or MGET calls to address the job-receiving service. The service ID must begin with the character ">".

KCOF

The KCOF field contains the functions permitted for communication with an OSI TP partner (irrelevant for communication via LU6.1 protocol).

Possible values:

- **B** (basic functions)
Basic functions
- **H** (handshake functions)
Basic and handshake functions (only possible with APRO DM)
- **C** (chained transactions)
Basic and commit functions with chained transactions
- **O** (other combination)
The functions are selected via the second parameter area, i.e. if KCOF=O is specified, a second parameter area must be passed during the KDCS call.

i When addressing an OSI TP job receiver, you must specify binary zero for all unused fields of the KDCS parameter area.

You specify the following in the second parameter area:

KCVERS

In the KCVERS field, enter the version number of the data structure: this is 1 in this openUTM version.

KCFUPOL

In the KCFUPOL field, specify whether the "polarized control" functional unit should be selected. Since "shared control" is not supported in this version, the only permitted entry is "Y".

KCFUHSH

In the KCFUHSH field, specify whether the "Handshake" functional unit should be selected (Y/N).

If an asynchronous service is addressed (APRO AM), then "N" must be specified for KCFUHSH.

KCFUCOM

In the KCFUCOM field, specify whether the "Commit" functional unit should be selected (Y/N). The "Commit" functional unit can only be selected if the addressed OSI-LPAP partner contains the abstract syntax CCR in the application context (**C**ommitment, **C**oncurrency and **R**ecovery).

KCFUCHN

In the KCFUCHN field, specify whether the "Chained Transactions" functional unit should be selected. This field is only relevant if the "Commit" functional unit has also been selected, i.e. if KCFUCOM=Y is set.

Since "Unchained Transactions" are not supported in this version, the only permitted entry here is "Y" if the "Commit" functional unit was selected.

If the "Commit" functional unit was **not** selected, the KCFUCHN field is irrelevant. In this case, enter a blank.

KCSECTYP

In the KCSECTYP field, enter the security type.

The security type controls whether SIGNON data (user ID and password) is transferred to the job-receiving service:

- N (none)
No SIGNON data is transferred to the job-receiving service.
- S(same)
The user ID under which the local service runs, is transferred to the job-receiving service.
- P(program)
The values specified in the KCUSERID and KCPSWORD fields are transferred to the job-receiving service as the user ID and password.

You can only select the security types "S" or "P", if the addressed OSI-LPAP partner in the application context contains the abstract syntax UTMSEC.

KCUIDTYP

In the KCUIDTYP field, you enter the data type of the user ID specified in the KCUSERID field:

- P: The string entered in KCUSERID is a "printable string" type.
- T: The string entered in KCUSERID is a "T61 string" type.
- O: The string entered in KCUSERID is an "octet string" type.
An octet string is a hexadecimal string. No code conversion is performed

For the range of values for these data types refer to the openUTM manual "Generating Applications", KDCDEF statement LTAC.

KCUIDLTH

In the KCUIDLTH field, you enter the length of the user ID specified in the KCUSERID field (in bytes, 16 maximum).

KCUSERID

In the KCUSERID field, you specify the user ID which, if KCSECTYP=P is set, will be transferred to the job-receiving service.

KCPWDTYP

In the KCPWDTYP field, you enter the data type of the password specified in the KCPSWORD field:

- P: The string entered in KCPSWORD is a "printable string" type.
- T: The string entered in KCPSWORD is a "T61 string" type.

- O: The string entered in KCPSWORD is an "octet string" type (see also the field "[KCUIDTYP](#)")

For the range of values for these data types refer to the openUTM manual "Generating Applications", KDCDEF statement LTAC.

KCPWDLTH

In the KCPWDLTH field, you enter the length of the password specified in the KCPSWORD field (in bytes, 16 maximum). If no password is to be transferred, enter zero.

KCPSWORD

In the KCPSWORD field, you enter the password which, if KCSECTYP=P is set, will be transferred to the job-receiving service.

i Any field of the 2nd parameter area which is not used must be filled with blanks. Exception: Any length field which is not used must be filled with zeroes.

For the KDCS call you enter:

1st parameter

The address of the KDCS parameter area.

2nd parameter

(if required): the address of the second parameter area (selection of special OSI TP function combinations).

Macro names

The use of C/C++ calls is described in detail in [section "C/C++ macro interface"](#).

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code, see next page.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the APRO call

The following codes can be analyzed in the program:

000 Function carried out.

40Z UTM cannot perform the function. There is a generation error or a system error, or the APRO function was called although the application was generated without distributed processing, or no connection to the partner application possible at the moment (see value of KCRCDC).

41Z Impermissible APRO call. This can be, for example, for one of the following reasons:

- APRO call was issued in a sign-on service.
- In a service, communication with certain partners is to be performed via LU6.1 and with others via the OSI TP protocol using the "Commit" functional unit.
- In a distributed transaction using the OSI TP protocol, associations are to be established via more than one local ACCESS-POINT.
- An association with a "Commit" functional unit is to be established. However, the abstract syntax CCR (**C**ommitment, **C**oncurrency and **R**ecovery) is **not present** in the application context of the associated OSI-LPAP partner.
- An "S" or "P" security type association is to be established. However, the abstract syntax UTMSEC is **not present** in the application context of the associated OSI-LPAP partner.

42Z Entry in KCOM invalid

43Z Entry in KCLM invalid.

44Z Value in KCRN does not identify a valid LTAC of a job-receiving service.
Possible reasons:

- configuration does not recognize the associated LTAC
- LTAC is locked
- user ID has no keycode for the LTAC
- entry in KCOM does not match the specified LTAC (value DM in KCOM and LTAC of an asynchronous service or a TAC queue; or value AM in KCOM and LTAC of a dialog service).

46Z Entry in KCPA invalid, i.e. no partner application is generated under the specified name, or blanks were entered in KCPA and there is no application name defined in the LTAC generation statement.

47Z KCOF=O was specified. However the 2nd parameter area is missing or invalid.

48Z Invalid data structure version.

55Z Entry in KCPI invalid (does not begin with ">"), or service ID already assigned by job-submitting service.

58Z Value in KCOF invalid

Additional error codes can be found in the dump:

71Z INIT call missing or was given the form DM in the MSGTAC program.

89Z When addressing an OSI TP job receiver, unused fields of the KDCS parameter area were not specified binary zero.

Features of the APRO call

- A service which communicates with a partner application via OSI TP protocol using the "Commit" functional unit cannot communicate with another partner application via LU6.1.
- If the OSI TP protocol is used in a service which takes part in a distributed transaction part, all job receivers must be allocated to the same local ACCESS-POINT and, if necessary, this ACCESS-POINT must be identical to the ACCESS-POINT used for the communication with a job-submitting service.
- Security types P and S can be selected both with APRO DM and with APRO AM. In the case of dialog services, the job submitter is signed on by means of the transferred user ID when the service is started and signed off again when it terminates. In the case of asynchronous services, the transferred user ID remains active only until the job has been entered in the appropriate queue.

For dialog services, the job submitter is rejected when there is already an OSI TP dialog service running under this name, when a user is logged on through an LTERM partner and it is prohibited for users to sign on to the application more than once (SIGNON statement, MULTI-SIGNON=NO) or when the user ID has been configured with RESTART=YES and the functional unit commit has not been selected.

The job submitter can always sign on under the user ID passed in order to be able to place a job in a queue for asynchronous services.

If security type "S" is selected, openUTM transfers the user ID under which the local service is running, to the job-receiving service. It is assumed that T61 String is used.

If security type "P" is selected in the 2nd parameter area, you must specify user ID and password. Additionally, the data type of user ID and password must also be specified. Possible data types are Printable String, T61 String and Octet String. For the range of values for these data types, refer to the openUTM manual "Generating Applications", KDCDEF statement LTAC.

Note for BS2000 systems

If Octet String is specified, no code conversion is performed. The Octet String type is necessary when you transfer passwords which were generated in Hex-String (PASSWORD=X'aabccc..') format.

- A successful APRO DM call means that a virtual connection has been established with the partner application. A successful APRO call does not mean that it is possible to exchange messages with the job-receiving service. A session or association is not reserved until the end of the program unit run in which the first message was sent to the job-receiving service.
- If at the time of the APRO call no connection to the remote application has been established, UTM initiates the connection setup.
- If openUTM returns a KDCS error code != 000 as a result of an APRO DM call no message should be sent with MPUT to the job receiver, because the service would then be aborted with KCRCCC=74Z.
- A message has to be sent to a job-receiving service addressed by APRO DM in the same transaction, otherwise openUTM aborts the service with KCRCCC=87Z at PEND.
- An asynchronous job must be associated with an asynchronous service addressed by APRO AM before the next PEND call, otherwise openUTM aborts the service with 86Z at PEND.
- A RSET call only rolls back the address of a dialog service if the APRO DM occurred in the same processing step, i.e. no dialog message has as yet been sent to the job-receiving service (MPUT with following PEND /PGWT).
- If multiple job-submitting services exist simultaneously in one application, these may use identical service identifiers. These may also be used for addressing differing job-receiving services.

-
- If a job complex is to be sent to the remote application, the APRO AM call must precede the MCOM BC call and the service identifier for the MCOM BC call must be entered in the KCRN field.
 - Life of a service ID

A service ID created with APRO DM is relevant for transaction security, i.e. it forms part of transaction-logged security. It is present until the job-receiving service is terminated and is not released until the end of the transaction in which the job submitter has read the message from the job receiver.

A service identifier created by APRO AM is released

- after a successful FPUT/DPUT NE call,
- at the next RSET or PEND call,
- after 40Z has been returned by an FPUT/DPUT call, or
- with job complexes with that service identifier: following an MCOM EC call or after 40Z has been returned by an MCOM BC or DPUT call.

Once a service ID has been released, it can be used for the next job receiver/submitter relationship.

- Addressing a Master LPAP

If a master LPAP is addressed with the APRO call, a slave LPAP from the LPAP bundle is selected if this is the first APRO call of the current transaction for this master LPAP.

- With an APRO DM call, the first slave LPAP is selected to which a logical connection has been established. If no logical connection has been established to any slave LPAP, the return value is 40Z/KD10.
- With an APRO AM call, the first slave LPAP is selected to which a logical connection has been established. If no logical connection has been established to any slave LPAP, one of the slave LPAPs is selected.

For every slave LPAP checked during selection, and to which no association or session is established, establishment of an association or session is initiated.

If a slave LPAP has been selected, the same slave LPAP is used for every additional APRO call in this transaction addressed to the master LPAP.

A subsequent APRO DM call can return 40Z/KD10 if the first APRO call was APRO AM and no association or session had previously been established to any of the slave LPAPs or if the logical connection has been cleared again in the interim.

i For more detailed information on message distribution, see the openUTM manual “Generating Applications”.

7.4 CTRL Control OSI TP Dialog

The CTRL (control) function call is used for distributed processing via the OSI TP protocol. It allows you to explicitly control a dialog with an OSI TP partner.

The CTRL PR and CTRL PE calls may only be addressed to job-receiving services for which the "Commit" functional unit was selected.

There are a number of variants of the CTRL call:

- CTRL PR (Prepare to Commit)
CTRL PR requests the job-receiving service to initiate the end of transaction. If the local service also sends data to the partner with an MPUT call, then it can use the CTRL call to specify whether or not the remote service is still permitted to send data.
- CTRL PE (Prepare End Dialogue)
CTRL PE requests the job-receiving service to initiate the end of dialog. If the local service also sends data to the partner with an MPUT call, then it can use the CTRL call to specify whether or not the remote service is still permitted to send data.
- CTRL AB (Abort Dialogue)
CTRL AB initiates an abnormal termination of the current dialog with the job-receiving service. MPUT calls to this job receiver are deleted and not sent. If the Commit functionality is selected for the dialog, openUTM ensures that the distributed transaction is rolled back to the last consistency point before the dialog is terminated. A separate CTRL call must be issued for each dialog which is to be terminated abnormally.

Setting the 1st parameter

The table below shows the various options and associated specifications in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOM	KCLA	KCLM	KCRN	KCMF/kcfn	KCNORPLY
Prepare to Commit	"PR"	0	0	service ID	blanks	"Y"/0
Prepare End Dialogue	"PE"	0	0	service ID	blanks	"Y"/0
Abort Dialogue	"AB"	0	0	service ID	blanks	0

Setting the 2nd parameter

Here you have to specify the address of the message area. The message area is not used in this version of openUTM. It is intended for future extensions.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"CTRL"
KCOM	"PR"/"PE"/"AB"
KCLA	0
KCLM	0
KCRN	Service ID
KCMF/kcfn	Blanks
KCNORPLY	"Y"/0

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameter
KDCS_CTRLPR/KDCS_CTRLPE/KDCS_CTRLAB	(kcrn)

openUTM return information	
Field name in KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the CTRL call the following entries are required in the KDCS parameter area:

KCOP

In the KCOP field, you must enter the CTRL operation code.

KCOM

The **KCOM** field must contain one of the following operation modifiers:

- **PR** (PRepare to commit)

This variant requests the job-receiving service to initiate the end of transaction. The following also applies:

- If the local service also sends data to the job-receiving service with an MPUT call, then it can use the KCNORPLY field to specify whether or not the job-receiving service is still permitted to send data in the current transaction. The local service is then only continued after completion of the processing step if the remote service has initiated an end-of-transaction.
- If the local service does not send any data to the job-receiving service then the job-receiving service may also not send any more data in this transaction. The local service then does not wait for the job-receiving service to initiate an end-of-transaction following completion of the processing step.

- **PE** (PRepare End dialogue)

This variant requests the job-receiving service to initiate the end of dialog. The following also applies:

- If the local service also sends data to the job-receiving service with an MPUT call, then it can use the KCNORPLY field to specify whether or not the job-receiving service is still permitted to send data in the current dialog. The local service is then only continued after completion of the processing step if the remote service has initiated an end-of-dialog.
- If the local service does not send any data to the job-receiving service then the job-receiving service may also not send any more data in this dialog. The local service then does not wait for the job-receiving service to initiate an end-of-dialog following completion of the processing step.

- **AB** (ABort dialogue)

This variant initiates an abnormal termination for the current dialog with a job-receiving service. If the Commit functionality is selected for the dialog, openUTM ensures that the distributed transaction is rolled back to the last synchronization point using an appropriate PEND call before the dialog is terminated. A separate CTRL call must be issued for each dialog which is to be terminated abnormally. With CTRL AB, messages sent to the partner using MPUT are deleted.

KCLA

The KCLA field must be set to zero.

KCLM

The KCLM field must be set to zero.

KCRN

In the KCRN field, specify the service ID (VGID) of the partner service to which the CTRL call refers.

KCMF / kcfm

In the KCMF/kcfm field, enter blanks.

KCNORPLY

If KCOM=PR/PE, the value Y can be entered in the KCNORPLY field. This value informs the job-receiving service that it cannot send any more data in this transaction or this dialog, even if the local service continues to send data to the job-receiving service with MPUT.

You must specify binary zero for all unused fields.

For the KDCS call you enter:

1st parameter

The address of the KDCS parameter area.

2nd parameter

As 2nd parameter: the address of the message area. This address must be specified for all CTRL calls even though CTRL calls do not currently use the message area.

Macro names

The use of C/C++ calls is described in detail in section “[C/C++ macro interface](#)”.

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual “Messages, Debugging and Diagnostics”).

KDCS return codes in the KCRCCC field for the CTRL call

The following codes can be analyzed in the program:

- 000 Function carried out successfully.
- 40Z The application was generated without distributed processing.
- 41Z CTRL call is impermissible at this point.
Possible reasons are:
 - The call was issued for an asynchronous service, i.e. the specified service ID was defined using an APRO AM call.
 - The call is addressed to a partner to which an MPUT HM has already been sent.
 - A CTRL PE or PR is addressed to a partner for which FU commit has not been selected.
 - A CTRL PE or PR is addressed to a partner to which no MPUT has as yet been sent following an APRO.
- 42Z The function variant in KCOM is invalid.
- 43Z The value specified in KCLA or KCLM is invalid.
- 44Z The service ID specified in KCRN is invalid or no service ID has been specified.
- 45Z The KCMF/kcfn field is not filled with blanks.
- 49Z The content of unused fields in the KDCS parameter area is not equal to binary zero.
- 54Z The KCNORPLY field in CTRL PR or PE has a value other than Y or binary 0.

Additional error codes can be found in the dump:

71Z No INIT call has been issued in the program unit run.

77Z Invalid area address.

Features of the CTRL calls

- No end of transaction may be requested at the end of a processing step in which a CTRL PR or PE call and an MPUT call have been addressed to the same partner.
- You may address the CTRL PR / PE / AB call only to those job-receiving services which are currently involved in a distributed dialog, i.e. which were addressed with an APRO DM.
- You may address CTRL PR and CTRL PE calls only to those job-receiving services for which the Commit functional unit has been selected and for which an MPUT has already been issued after APRO.
- You can issue CTRL calls for multiple partners in a single processing step or program unit run.
- Only those PEND calls with the operation modifiers RS, FR and ER are allowed after a CTRL AB call for a dialog with an AN service in which the commit functionality has been selected.

7.5 DADM Administer message queues

The DADM (delayed free message administration) call provides the following functions for administering message queues that enable you:

- to read summary information about messages in a message queue into the message area (user identification, job identification (job ID), creation time, starting time and existing confirmation jobs, original destination ...)
- to read user information into the message area that has been generated with DPUT NI/QI/+I/-I. The user information can only be read if the confirmation job becomes the main job.
- to change the processing order of messages in a message queue
- to delete individual messages or all the messages from the message queue
- to assign either selected messages or all messages in the dead letter queue each to their original destination or to a new destination

Unix, Linux and Windows systems

In a UTM cluster application you can only administer message queues of the local node application.

The format of the DADM call is discussed in detail below. For further information on the administration of the message queue refer to the openUTM manual “Administering Applications”.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area							
	KCOP	KCOM	KCLA	KCRN	KCLT	KCQTYP	KCMOD	Time ¹
Read overview information	"DADM"	"RQ"	54	Job ID / blank	LTERM/ (OSI-)LPAP /TAC	Binary zero	Binary zero	Binary zero
					Queue			
Read user information	"DADM"	"UI"	Length	Job ID	Binary zero	Binary zero	Binary zero	Time point (absolute)
Change order	"DADM"	"CS"	0	Job ID	Binary zero	Binary zero	Binary zero	Time point (absolute)
Delete individual message from a queue	"DADM"	"DL"	0	Job ID	LTERM/ (OSI-)LPAP /TAC	Binary zero	"C"/"N"	Time point (absolute)
					Queue			
Delete all messages from a queue	"DADM"	"DA"	0	Blank	LTERM/ (OSI-)LPAP /TAC	Binary zero	Binary zero	Binary zero
					Queue			
Move single message	"DADM"	"MV"	0	Job ID	TAC/LPAP /OSI-LPAP /Blank	Binary zero	Binary zero	Time point (absolute)
Move all messages	"DADM"	"MA"	0	Blank	TAC/LPAP /OSI-LPAP /Blank	Binary zero	Binary zero	Binary zero

¹ The time point is specified in the fields KCTAG/kcday, KCSTD/kchour and KCMIN.

All fields of the parameter areas not in use must be assigned the value binary zero.

Setting the 2nd parameter

Here you have to supply the address of the message area into which openUTM is to read the message. A language-specific data structure enables you to structure the message area when calling DADM RQ, in COBOL this is the KCDADC COPY element and in C/C++ the *kcdad.h* include file.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"DADM"
KCOM	"RQ"/"UI"/"CS"/"DL"/"DA"/"MV"/"MA"
KCLA	Length in bytes/0
KCRN	Job ID/blanks
KCLT	LTERM name / TAC / (OSI-)LPAP name / queue /binary zero / blanks
KCTYP	Destination type:"Q"/"U"/binary zero
KCMOD	"C"/"N"/binary zero
KCTAG / ...	Time specification (absolute)
<ul style="list-style-type: none"> • KCTAG/kcday 	<ul style="list-style-type: none"> • Day (absolute)/binary zero
<ul style="list-style-type: none"> • KCSTD/kchour 	<ul style="list-style-type: none"> • Hour (absolute)/binary zero
<ul style="list-style-type: none"> • KCMIN 	<ul style="list-style-type: none"> • Minute (absolute)/binary zero
<ul style="list-style-type: none"> • KCSEK/kcsec 	<ul style="list-style-type: none"> • Second (absolute)/binary zero

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_DADMRQ	(nb,kcla,kcrn,kclt)
KDCS_QADMRQ	(nb,kcla,kcrn,kclt,kcqtyp)
KDCS_DADMUI	(nb,kcla,kcrn,kcday,kchour,kcmin,kcsec)
KDCS_DADMCS	(nb,kcrn,kcday,kchour,kcmin,kcsec)
KDCS_DADMDL	(nb,kcrn,kclt,kcmod,kcday,kchour,kcmin,kcsec)
KDCS_QADMDL	(nb,kcrn,kclt,kcmod,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DADMDA	(nb,kclt)
KDCS_QADMDA	(nb,kclt,kcqtyp)
KDCS_DADMMV	(nb,kcrn,kclt,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DADMMA	(nb,kclt,kcqtyp)

openUTM return information	
Message area	Contents
	Data
Field name in the KB return area	
KCRLM	Actual length
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF / kcrfn	Job ID/blanks

For the DADM call you make the following entries in the appropriate fields of the KDCS parameter area:

KCOP

In the KCOP field, enter the DADM operation code.

KCOM

In the KCOM field, select the operation modifier:

- RQ to read the overview information on a message queue
- UI to read the user information of a main job created by means of DPUT NI/QI
- CS to give preference to a specific message

-
- DL to delete a single message
 - DA to delete all messages in the message queue
 - MV to move a single message from the dead letter queue into either the original message queue, any asynchronous TAC, any TAC queue, an LPAP partner or an OSI-LPAP partner.
 - MA to move each message from the dead letter queue. In this case, you have two possibilities:
 - Moving into their original message queues
 - Move all messages with the original destination TAC, LPAP or OSI-LPAP to any other destination of the same type (asynchronous TAC/TAC queue, LPAP partner or OSI-LPAP partner).
Messages whose original type is not the same as the new destination remain in the dead letter queue.
To move all messages, up to three calls with new destinations of the type TAC, LPAP and OSI-LPAP are therefore required.

KCLA

In the KCLA field, enter the length of the data to be transferred to the message area. For KCOM = RQ enter 54, for KCOM = CS/DL/DA/MV/MA enter 0.

KCRN

In the KCRN field, specify the message in the queue to be administered. The following specifications are required:

- blanks
if KCOM = DA/MA or if KCOM = RQ and the call refers to the first message in the queue
- the job ID
if KCOM = UI/CS/DL/MV or if KCOM = RQ and the call refers to the subsequent messages in the queue.
The job ID is always returned to the KCRMF/kcrfn field in the preceding DADM RQ.

KCLT

In the KCLT field, identify the queue. That means:

- If KCOM = RQ/DL/DA, specify:
 - the LTERM name if the message was for an LTERM partner
 - the (MASTER-)(OSI-)LPAP name if the messages was for an (OSI-)LPAP partner
 - the TAC if the message was for an asynchronous program
 - the name of the queue if you want to administer messages of a USER queue, a TAC queue or a temporary queue
- If KCOM = UI/CS, specify binary zero.

- If KCOM = MV/MA, specify the following:
 - the TAC, if the single message or all messages with original target TAC or TAC queue are to be directed to an asynchronous program,
 - the name of a TAC queue, if the single message or all messages with original target TAC or TAC queue are to be directed to a service-controlled queue,
 - the name of an LPAP partner (but not a MASTER-LU61-LPAP), if the individual message or all messages with the original destination LPAP are to be sent to an LPAP partner,
 - the name of an OSI-LPAP partner (but not a MASTER-OSI-LPAP), if the individual message or all messages with the original destination OSI-LPAP are to be sent to an OSI-LPAP partner,
 - blank, if the single message or all messages are each to be assigned back to their original destination.

i All messages whose original target does not match the new target are remaining in the dead letter queue

KCQTYP

In the KCQTYP field, specify the type of the queue:

- If KCOM = RQ/DL/DA, specify:
 - binary zero, if the queue belongs to an LTERM, an (OSI-)LPAP or a TAC, or if it is a TAC queue,
 - Q in the case of a temporary queue created with QCRE,
 - U in the case of a USER queue.
- If KCOM=UI/CS/MV/MA enter binary zero.

KCMOD

In the KCMOD field, specify whether openUTM should activate the negative confirmation job when a job complex is deleted. The following values are possible:

- binary zero, if KCOM = RQ/UI/CS/DA/MV/MA,
- C to delete the complete job if KCOM = DL; in the case of job complexes all the confirmation jobs are deleted also,
- N to activate the negative confirmation job if KCOM = DL; the message itself is deleted.

KCTAG / ...

If KCOM = UI/CS/DL/MV, enter the time the message was generated as follows: in the **KCTAG/kcday** field, the day in the year (working day, value 001 to 366), in **KCSTD/kchour** the hour, in the **KCMIN** field the minute and in **KCSEK/kcsec** the second. This time can be ascertained before with DADM RQ.

If KCOM = RQ/DA/MA enter binary zero.

For the KDCS call you enter:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area into which openUTM is to read the message. You have to enter the address even if you have entered 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in section "[C/C++ macro interface](#)".

openUTM returns:

If KCOM = RQ/UI: the message in its actual or at most in its desired length in the specified message area.

KCRLM

In the KCRLM field: the actual length of the message, possibly deviating from the length requested in KCLA of the parameter area.

KCRCCC

In the KCRCCC field: the KDCS return code.

KCRCDC

In the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KCRMF / kcrfn

In the KCRMF/kcrfn field: if KCOM = RQ the job ID of the next message in the queue (see KCLT) or blanks for the last message in the queue.

KDCS return codes in the KCRCCC field for the DADM call

The following codes can be analyzed in the program:

- 000 Operation executed (if KCOM = RQ/UI) or the administration job accepted (if KCOM = CS/DL/DA/MV/MA). The real execution is not determined until the end of the transaction. A decision about actual execution is not made until the end of the transaction (see "[Features of the DADM call](#)").
- 01Z Length conflict: KCLA < KCRLM, the message is truncated.
- 07Z Not all messages from the dead letter queue could be moved because the task-specific buffer area generated for the restart information is too small, see openUTM manual "Generating Applications" "Restart area".
Action: Generation with KDCDEF, defining a larger buffer area with MAX RECBUF=(...,length), or repeating the DADM call.
- 40Z The system cannot perform the operation (generation error or system error, original destination no longer exists, no administration privileges, locked by another service), see KCRCDC.

42Z Entry in KCOM invalid.

43Z Length specified in KCLA is negative or invalid.

44Z Job ID specified in KCRN is invalid.

46Z Entry in KCLT is invalid. Possible causes:

- The specified LTERM or (MASTER-)(OSI-)LPAP name does not exist.
- The TAC is invalid or locked.
- The TAC is not a process TAC or a dialog TAC.
- There is no USER queue or temporary queue with the specified name, or the type specified in KCTYP does not fit the queue name.
- with KCOM=MV/MA: an LTERM name, master LU61-LPAP name or master OSI-LPAP LPAP name was specified, the specified TAC has been deleted or KDCMSGTC or KDCDLETQ was specified.
- with KCOM=MV: blanks were specified but the original destination of the message has been deleted.
- with KCOM=MV: The types of the original target and the new target do not match,i.e.:
 - original target: TAC or TAC- queue, new target LPAP or OSI-LPAP
 - original target: LPAP, new target TAC or TAC queue or OSI-LPAP
 - original target: OSI-LPAP, new target TAC or TAC queue or LPAP

47Z Message area missing or cannot be written in the specified length.

49Z Contents of unused fields of KDCS parameter area not equal to binary zero.

56Z Value in KCMOD or time entry in KCTAG/kcday, KCSTD/kchour, KCMIN or KCSEK/ksec is invalid.

An additional return code can be found in the dump:

71Z INIT missing in this program.

Return information in the message area for DADM RQ

There is a data structure available for the return information for the DADM RQ call, for COBOL the KCDADC COPY element and for C/C++ the *kcdad.h* include file. This data structure can be used to define the message area and has the following structure:

Byte	Field name COBOL/C/C++	Meaning	
1 - 8	KCDAGUS	UTM user ID of the job submitter	
9 - 16	KCDADPID	Job ID (assigned by UTM)	
17 - 25	KCDAGTIM ¹	Time of the FPUT/DPUT call in the form <i>dddhhmss</i> :	
17 - 19	KCDAGDOY	<i>ddd</i>	Day in the year (value range 000 - 366)
20 - 21	KCDAGHR	<i>hh</i>	Hour (value range 00 - 23)
22 - 23	KCDAGMIN	<i>mm</i>	Minute (value range 00 - 59)
24 - 25	KCDAGSEC	<i>ss</i>	Second (value range 00 - 59)
26 - 34	KCDASTIM ¹	For time-delayed jobs enter the desired starting time in the form <i>dddhhmss</i> .	
26 - 28	KCDASDOY	<i>ddd</i>	Day in the year (value range 000 - 366)
29 - 30	KCDASHR	<i>hh</i>	Hour (value range 00 - 23)
31 - 32	KCDASMIN	<i>mm</i>	Minute (value range 00 - 59)
33 - 34	KCDASSEC	<i>ss</i>	Second (value range 00 - 59)
		For a job without time delay blanks are returned.	
35	KCDAPMSG	Y	positive confirmation job exists
		N	no positive confirmation job exists
36	KCDANMSG	Y	negative confirmation job exists
		N	no negative confirmation job exists
37 - 44	KCDADEST	Destination of the message or the original destination for dead letter queue	

Byte	Field name COBOL/C /C++	Meaning	
45	KCDATYPE	Type of the message destination or type of original destination for dead letter queue	
		Q	for temporary queue
		U	for USER queue
		T	for TAC queue
		A	for asynchronous TAC
		L	for LTERM
		P	for LPAP
		O	for OSI-LPAP
46 - 53	KCDAFCTM	Generation time or time DPUT converted to FPUT in the message. In the case of service-driven queues, the messages displayed with DADM RQ can be unambiguously assigned to the messages read with DGET BF. KCDADPID or KCDAFCTM must correspond to the return values KCRDPID or KCRGTM of the corresponding DGET BF call.	
54	KCDAGUST	Type of the submitter	
		U	for user
		S	for LU6.1 session
		O	for OSI association

¹ For C/C++, the KCDAGTIM and KCDASTIM summary fields are not defined. However the specific fields for day /hour/minute/second are defined.

Features of the DADM call

- Ascertaining the job ID

The job ID is assigned internally by UTM. It can be ascertained in the program unit as follows with a DADM RQ call: for the first DADM RQ call (with KCRN = blanks) openUTM supplies information on the first message in the queue. On this occasion openUTM writes the job ID amongst other things to the message area. If there are more messages for the queue in the message queue, openUTM in each case returns the job ID of the next message to KCRMF/kcrfn. When the last message in the queue is reached, openUTM enters blanks in the KCRMF/kcrfn field.

- DADM CS/DL/DA/MV/MA calls (change order, delete or move) are transaction-logged and are not executed until the end of the transaction. After such a call, therefore, KCRCCC = 000 does not necessarily guarantee that the call can be executed successfully, because the message in the queue could be deleted in the meantime by another DADM call. You can check whether a DADM CS/DL/DA/MV/MA call has been successful by issuing a DADM RQ call in a subsequent transaction.

-
- The DADM CS call puts the relevant message in first position in the queue. In the case of time-driven messages whose starting point has not yet been reached, the call is rejected with 40Z.
 - After a delete job with DADM DL/DA no more delete jobs can be submitted within the same transaction and no DADM CS call; openUTM rejects this with 40Z.
 - Jobs that are currently being processed cannot be administered. This applies, for example, if messages in a USER queue or a temporary queue are currently being read. If these jobs are destined for printers, printing can be stopped by means of a PADM call.
 - A program unit which issues a DADM call must be running under a user ID with administration privileges, otherwise openUTM acknowledges the DADM call with 40Z. There is the following exception:
If a service is started from a printer control LTERM and if only such jobs are administered which are directed to printers of the printer control LTERM, then neither the program unit nor the user need the administration privileges.
 - The dead letter queue consists of messages that could not be processed. To be able to process these messages, possibly after eliminating the error, they must either be assigned to their original destination or to a new destination with the same type. You can use DADM MV to move a single message or DADM MA to move all messages from the dead letter queue into a specific queue or the original queue. In this case, there are two possibilities:
 - Move to the relevant initial message queue(s).
 - Move the message or all messages with the original destination TAC (asynchronous TAC or TAC queue), LPAP or OSI-LPAP to any other destination of the same type.

A previously defined QLEV and the STATUS of the recipient queue is thereby ignored.

With DADM MA, messages are remaining in the dead letter queue in the following cases without this is indicated by a return code:

- KCLT = blank: All messages whose original destination no longer exists.
- KCLT != blank: All messages whose original destination does not match the new destination. Messages whose original destination no longer exists only match the new destination asynchronous TAC or TAC queue.

7.6 DGET Read a message from a service-controlled queue

The call DGET (data GET) is used to read a message or message segment into the message area from a service-controlled queue. The following are service-controlled queues: TAC queues, USER queues and temporary queues

DGET provides several ways of reading the messages of a queue:

- sequential processing (DGET FT/NT)
- browsing (DGET BF/BN)
- selective processing (DGET PF/PN)

With sequential or selective processing the message is read and then deleted from the queue, whereas with browsing the message remains in the queue. For the dead letter queue only browsing (read without delete) is allowed.

Each variant also allows several message segments to be read. The first segment is read using DGET FT/BF/PF (first). Subsequent segments are read within the same program unit run using DGET NT/BN/PN (next) without an intervening PGWT call.

In this way, as many message segments as have been sent with DPUT QT can be read. Each message segment sent with DPUT QT must be read using a separate DGET.

Message segments that have not been read are lost

- when a new message is read with DGET FT,
- when PGWT is called,
- when the program unit run is terminated.

If the transaction is rolled back, processed messages are placed back in the queue (redelivery) and can then be read and processed again using DGET. The maximum number of redeliveries can be set in the generation (MAX REDELIVERY=). Once this limit has been reached, then, depending on the TAC statement's DEAD-LETTER-Q parameter for the generation, the processed message is either deleted at the end of the transaction or is saved in the dead letter queue unless (in the case of message complexes) no negative acknowledgment job has been defined.

Messages from USER or temporary queues cannot be saved in the dead letter queue. They are therefore lost after the maximum number of redeliveries.

The format of the DGET call is described in detail in the following. You will find more information on the subject of message queues in section "[Message Queuing \(asynchronous processing\)](#)".

Setting the KDCS parameter area (1st parameter)

The following tables show the different options and the entries that have to be made in the KDCS parameter area.

Sequential processing									
Function of the call	Entries in the KDCS parameter area								
	KCOP	KCOM	KCLA	KCMF/ kcfn	KCRN	KCQTYP	KCWTIME	KCQRC	KCDPID
Read new message or first message segment from queue	"DGET"	"FT"	Length	Blank	Queue name	Type of the queue	Wait time in seconds	0	Binary zero
Read next message segment from queue	"DGET"	"NT"	Length	Blank	Queue name	Type of the queue	0	0	Binary zero
Browsing									
Function of the call	Entries in the KDCS parameter area								
	KCOP	KCOM	KCLA	KCGTM	KCRN	KCQTYP	KCWTIME	KCQRC	KCDPID
Read first message segment of the first or next message	"DGET"	"BF"	Length	Blank / creation time*	Queue name	Type of the queue	Wait time in seconds	-1 / redelivery counter	Blank / DPUT ID
Read next message segment	"DGET"	"BN"	Length	Creation time*	Queue name	Type of the queue	0	0	DPUT ID

Selective processing									
Function of the call	Entries in the KDCS parameter area								
	KCOP	KCOM	KCLA	KCGTM	KCRN	KCQTYP	KCWTIME	KCQRC	KCDPID
Process first message segment of a specific message	"DGET"	"PF"	Length	Creation time*	Queue name	Type of the queue	0	0	DPUT-ID
Process next message segment	"DGET"	"PN"	Length	Creation time*	Queue name	Type of the queue	0	0	DPUT-ID

* Value in the KB return area KCRGTM of the preceding DGET BF

Setting the 2nd parameter

Here you have to make available the address of the message area to which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"DGET"
KCOM	"FT"/"NT"/"BF"/"BN"/"PF"/"PN"
KCLA	Length in bytes
KCMF/kcfn KCGTM	Blanks Blanks / creation time
KCRN	Name of the queue
KCQTYP	"T"/"U"/"Q"
KCWTIME	Wait time in seconds/0
KCQRC	0 / -1 / redelivery counter
KCDPID	Binary zero / blank / DPUT ID

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro call	
Macro names	Parameter
KDCS_DGETFT/KDCS_DGETNT	(nb,kcla,kcfn,kcrn,kcqtyp,kcwtime,kcfkt1,kcfkt2)
KDCS_DGETBF/KDCS_DGETBN/KDCS_DGETPF/KDCS_DGETPN	(nb,kcla,kcrn,kcqtyp,kcwtime,kcqrc,kcgtm,kcdpid)

Returns from openUTM	
Message area	Contents
	Data
Field name in KB return area	
KCRLM	Actual length
KCRMF/kcfn (DGET FT/NT only)	In the case of OSI TP partner: name of the abstract syntax
KCRWVG (DGET FT only)	Number of services that are waiting
KCRUS (DGET FT only)	UTM user ID of the message creator
KCRQRC (DGET BF only)	Queue-specific redelivery counter
KCRGTM (DGET BF only)	Creation time of the message read
KCRDPID (DGET BF only)	DPUT ID of the message read
KCRRRC (DGET FT/BF/BN/PF only)	Redelivery counter of the message read
KCRCCC	Return code
KCRCDC	Internal return code

In the KDCS parameter area you make the following entries for the DGET call:

KCOP

In the KCOP field, enter the DGET operation code.

KCOM

In the KCOM field, enter:

- FT to process the first message segment of the first/new message
- NT to process a further message segment of the first/new message
- BF to read the first message segment of a message (browse without deleting)
- BN to read a further message segment of the message (browse without deleting)

-
- PF to process the first message segment of a specific message
 - PN to process a further message segment of a specific message

KCLA

In the KCLA field, specify the length of the message area to which the message is to be read. openUTM enters the length of the message segment that has actually been read in the KCRLM return field.

If the message and all its message segments is not to be read, you can specify the value 0 here for DGET FT. A subsequent DGET NT is then rejected with the return code 10Z.

KCMF/kcfn

KCGTM

The KCGTM or KCMF/kcfn field must be supplied as follows:

- with blank for KCOM = FT/NT.
- with blank for KCOM = BF if the first segment of the first message of the queue is to be read.
- with the creation time of the message for KCOM = BN/PF/PN or if, for KCOM = BF, the next message is to be read. The creation time is returned in the KCRGTM field for the last DGET BF call.

KCRN

In the KCRN field, specify the name of the queue from which the message is to be read.

KCQTYP

In the KCQTYP field, specify the type of the queue:

- T for a TAQ queue
- U for a USER queue
- Q for a temporary queue

KCWTIME

In the KCWTIME field, specify for DGET FT/BF the maximum number of seconds to be waited for the arrival of a message. If you specify 0, there will be no wait. If a wait time is specified, the subsequent program unit when PEND is specified must be assigned to a TAC class.

In the case of DGET NT/BN/PF/PN you must specify 0.

KCQRC

In the KCQRC field, specify for DGET BF the behavior after a transaction has been processed and rolled back. You can specify:

- either the value returned in the KCRQRC field for the previous DGET BF call. This ensures that all messages of the queue are always read. A message that has already been processed may be read again after the transaction has been rolled back.
- or the value -1 or the constant KDCS_NO_QRC. This may mean that not all messages of the queue are read.

You must specify 0 for DGET FT/NT/BN/PF/PN.

KCDPID

In the KCDPID field, specify:

- binary zero for KCOM = FT/NT
- blank if, for KCOM = BF, the first segment of the first message is to be read.
- the DPUT ID for KCOM = PF/PN or if, for KCOM = BF/BN, the next message/message segment is to be read. The DPUT ID is returned in the KCRDPID field in the previous DGET BF call.

In the KDCS call you specify:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area to which openUTM is to read the message. You also specify the address of the message area when you enter a length of 0 in KCLA.

Macro names

The section "[C/C++ macro interface](#)" describes in detail how to use macro calls for C/C++.

openUTM returns:

Message area

In the specified message area the message segment in its actual length or, at most, the length of the message area.

KCRLM

In the KCRLM field the actual length of the message segment read providing a value > 0 was specified in KCLA.

For KCOM = FT/NT:

KCRMF/kcrfn

In the KCRMF field the name of the abstract syntax of the message segment read, provided the message originates from an OSI TP partner. Otherwise, it returns blanks.

KCRWVG

In the KCRWVG field the number of services that are already waiting for messages from the specified queue (the current service is not counted). KCRWVG is only supplied in the case of DGET FT.

KCRUS

In the KCRUS field the UTM user ID under which the DGET message was created. KCRUS is only supplied in the case of DGET FT.

For KCOM = BF:

KCRQRC

In the KCRQRC field, the queue-specific redelivery counter. This value is needed to supply the KCQRC field in the next DGET BF call.

KCRGTM

In the KCRGTM field, the creation time (binary) of the message read. This value is needed to supply the KCGTM field in the next DGET BF/BN/PF/PN call.

KCRDPID

In the KCRDPID field, the DPUT ID of the message read. This value is needed to supply the KCDPID field in the next DGET BF/BN/PF/PN call.

For KCOM = BF/BN/PF:

KCRRRC

In the KCRRRC field, the redelivery counter of the message read. This indicates how often the message was redelivered after the transaction was processed and rolled back. KCRRRC can accept a maximum value of 254. If this value has been reached and if the number of redeliveries was not limited at generation, the value 254 is always returned after each additional DGET BF/BN/PF call.

For all variants:

KCRCCC

In the KCRCCC field the KDCS return code (see next page).

KCRCDC

In the KRCDC field, the internal return code of openUTM (see openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the DGET call

The following codes can be analyzed in the program:

- 000 The operation was executed.
- 01Z Length conflict: $KCLA < KCRLM$; the message was truncated because the message segment is longer than the message area.
- 04Z Not all of the message segments were read at the previous DGET call; as a result of the current DGET FT /BF/PF call, the message segments that have not yet been read are lost.
- 08Z In the case of reading with waiting ($KCWTIME > 0$): there is currently no message.

In this case, no more DGET calls are permitted and the program unit must be terminated with PEND PA/PR or a wait point must be set with PGWT PR. As soon as a message arrives, the maximum wait time elapses or the queue is deleted, openUTM continues the service with the next program unit or openUTM continues the service after the PGWT PR. A follow-up program unit must be assigned to a TAC class.

-
- 10Z In the case of DGET NT/BN/PN: all the message segments of the message have been read.
- 11Z In the case of reading without waiting (KCWTIME=0): there is no message.
- 40Z In the case of DGET NT/BN/PN: the name or type of the specified queue does not match the previous DGET call of the current program unit run. Message segments may have been lost. No message has been read.
- In the case of DGET FT/PF: there is a generation error (the value MAX ...,RECBUF=... is too low).
- 41Z The DGET call is made in the first part of the sign-on, which is impermissible, or the previous DGET call produced the return code 08Z. This means it is necessary to wait, and no further DGET calls are permitted in this program unit.
- 42Z Possible causes:
- The value in KCOM is invalid or does not match the previous DGET call (e.g. DGET PN after DGET BF)
 - or the first message segment was not read in this program unit run,
 - or a PGWT call was issued in the meantime.
- 43Z The value in KCLA or KCWTIME is negative or invalid, or KCWTIME was not supplied with 0 for DGET NT/BN/PF/PN.
- 44Z The value in KCRN is invalid. This means one of the following things:
- There is no queue with the specified name and type.
 - The queue was deleted.
 - The USER that started the service or the user's LTERM has no authorization (KSET) to read the queue.
 - The specified TAC is not generated with TYPE=Q.
 - The dead letter queue has been read in another way than with Browse (read without delete, i.e. DGET BF/BN).
- 45Z The value in KCMF/KCGTM is invalid:
- For DGET FT/NT: KCMF was not supplied with blanks.
 - For DGET BN/PF: there is no message with the specified DPUT ID and creation time, or the message was deleted in the meantime.
- 47Z The message area is missing, or the specified area address is invalid.
- 49Z Unused fields have a value that is not equal to binary zero.
- 53Z For DGET BF/PF: the value in KCDPID is not a valid DPUT ID or does not match the entries in KCRN and KCQTYP.
- For DGET BN/PN: the value in KCDPID or KCGTM does not match the corresponding value of the last DGET BF/PF call.

An additional return code can be found in the dump:

71Z An INIT has not yet been called in the program unit run.

Features of the DGET call

- Message length

The actual message length is returned in the KCRLM field. The following applies:

- When $KCRLM \leq KCLA$, only KCRLM characters (bytes) are transferred to the message area. The contents of the rest of the message area are undefined.
- When $KCRLM > KCLA$, only KCLA characters are transferred to the message area. The rest ($KCRLM - KCLA$) are lost and can no longer be read by means of a subsequent DGET.

In the description of the MGET call you will find an example that indicates what openUTM does when there are length conflicts.

- Browsing and processing

- During browsing (DGET BF/BN) messages can be read in parallel by several services.
- During message processing (DGET FT/NT/PF/PN) each message segment can be read once only. All message segments are deleted as soon as the transaction is terminated.
- If a message is to be read (DGET BF/BN) and then processed with DGET PF, the DPUT ID and creation time returned for DGET BF must be specified in the DGET PF call.

- Waiting for messages

In a dialog or asynchronous service DGET calls may be issued for different queues until it is necessary to wait for a message. In other words, if there is no message for a DGET call with waiting, this is indicated in the program by $KCRCCC = 08Z$ ($KCWTIME > 0$).

The following KDCS calls should be programmed, depending on whether a wait is required for a message.

- If a wait is required, the program unit must be terminated with PEND PA/PR so that it is possible to wait for the arrival of the message outside the program context, or a wait point must be set in the program unit using PGWT PR.
- If no wait is required, the transaction must be rolled back (RSET, PEND RS or PGWT RB) or the service must be terminated with PEND ER/FR.

Otherwise, the error code 72Z is returned for the PEND call.

- Continuing the program

If there is a wait for a DGET message, openUTM starts the next program unit or continues the program after the PGWT PR:

1. as soon as a message arrives
2. when the maximum wait time elapses or
3. when the queue is deleted
4. as soon as the processed message is redelivered (redelivery after transaction rollback), providing DGET FT is used for waiting or KCQRC was supplied with the value of the KB return field KCRQRC by the previous browse call.

In a) to c) above all services waiting for messages in the queue are continued (not just the first waiting service).

In the case of redelivery (d)) only the services that are able to read redelivered messages are continued. This ensures that arriving or redelivered messages can be read in parallel by the services.

If the program is continued in a PEND PA/PR follow-up program unit, it must be assigned to a TAC class. In other words, TAC classes must have been generated if this functionality is to be available. If they have not been, the PEND call is rejected with KCRCCC=74Z.

- Redelivery

If a transaction is rolled back, any processed message is placed back in the queue and can be read again. The application must have been generated accordingly and the generated maximum number of redeliveries must not have been reached. For more information refer to the openUTM manual "Generating Applications", REDELIVERY operand in the MAX statement.

- In the KDCMSGTC service and in the KDCSGNTC sign-on service, the DGET call can only be used without specifying a wait time.
- If the main message of a job complex is read, and a positive or negative confirmation job is defined for it (only possible in the case of TAC queues),
 - the positive confirmation job is started once the transaction containing the DGET call has been successfully terminated,
 - the negative confirmation job is started once the transaction containing the DGET call has been rolled back without delivery of the main message again, i.e. there is no redelivery.
- If DGET is used to read from a queue for which there is data access control, the user ID under which the service is running and the LTERM partner must have access authorization (KSET) for the corresponding queue. Users are however always allowed to access their own USER queue. In the case of applications without explicitly generated user IDs, no data access control can be assigned for the queues assigned to the USERS.
- Saving faulty messages into the dead letter queue

If an error occurs, messages from TAC queues can be saved into the global dead letter queue as a last fallback stage. The queue must be generated with DEAD-LETTER-Q=YES for this. A processed message is then placed into the dead letter queue when the transaction is rolled back, if it cannot be redelivered (see redelivery) and if no negative acknowledgement job was defined.

When a message is saved into the dead letter queue, the number of redeliveries for this message is rolled back to zero if necessary.

7.7 DPUT Generate time-driven asynchronous messages

The DPUT (delayed free message PUT) call enables you:

- to send messages to USER queues, TAC queues or temporary queues. The messages to TAC queues can also be time-driven.
- to enter time-driven asynchronous jobs with their messages or message segments in a message queue (output jobs to LTERM partner, background jobs to local asynchronous services, background jobs to remote asynchronous services which were previously addressed using an APRO AM call)
- to log user information concerning these jobs
- to create confirmation jobs within a job complex plus the associated user information
- to pass print options (= RSO parameter list) for RSO printers (only on BS2000 systems)

You enter the desired point in time in the KDCS parameter area (see table on "[DPUT call without job complex](#)"). At the given time, the job is entered in the queue of jobs to be executed. In other words, the time-driven job is not executed exactly at the specified time, but at this time at the earliest.

The message segments generated using DPUT are collected by openUTM and are terminated at the next PEND call. Following the end of a transaction, the message segments are sent as a **single** message to the appropriate queue. Exception: If formatted message segments are sent to terminals, each of these segments forms a separate message.

Because of the various functions, the DPUT call has two formats:

- DPUT call without job complex, and
- DPUT call within a job complex.

The format of the DPUT call is described in detail below. For further information on message queuing refer to section "[Message Queuing \(asynchronous processing\)](#)".

7.7.1 DPUT call without job complex

Setting the KDCS parameter area (1st parameter)

The following two tables show the various options and entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCLM	KCRN	KCMF/ kcfn	KCDF
Output job in format mode	"DPUT"	"NT"/ NE"	Length	LTERM name	Format identifier	Screen function
Unix, Linux and Windows systems: Output job in line mode	"DPUT"	"NT"/ NE"	Length	LTERM name	Blanks	—
BS2000 systems: Output job in line mode	"DPUT"	"NT"/ NE"	Length	LTERM name	Blanks / edit profile	Screen function / binary zero
Background job for asynchronous program in the same application	"DPUT"	"NT"/ NE"	Length	TAC	—	—
Message for service-controlled queue	"DPUT"	"QT"/ QE"	Length	Name of the queue	—	—
Job for transport system application	"DPUT"	"NT"/ NE"	Length	LTERM name of application	Blanks	Binary zero
Background job for job-receiving service via LU6.1	"DPUT"	"NT"/ NE"	Length	service -ID	—	—
Background job for job-receiving service via OSI TP	"DPUT"	"NT"/ NE"	Length	service-ID	Blanks / name of abstract syntax	—
Log user information	"DPUT"	"NI"/ QI"	Length	as for related DPUT NT/NE or DPUT QT/QE	Blanks	Binary zero
BS2000 systems: Pass parameter list for RSO printers	"DPUT"	"RP"	Length	LTERM name	Blank	Binary zero

NT, QT: Message segment for job

NE, QE: Last message segment or entire message for job

NI, QI: User information for a subsequent message

RP: RSO parameters (BS2000 systems)

Entry in KCOM field	Additional entries in the KDCS parameter area (KCPUT/kc_dput)						
	KCMOD	KCTAG/ kcday	KCSTD/ kchour	KCMIN	KCSEK/ kcsec	KCQTYP	Other fields
"NT"/"NE"	"A"	001 - 365 /366	00 - 23	00 - 59	00 - 59	—	—
	"R"	000 - 364 /365				—	
	Blanks	—	—		—		
"QT"/"QE"	"A"	001 - 365 /366	00 - 23	00 - 59	00 - 59	Binary zero	Binary zero
	"R"	000 - 364 /365					
	Blanks	Binary zero	Binary zero		"U" / "Q" / Binary zero		
"NI"	"A"	001 - 365 /366	00 - 23	00 - 59	00 - 59	Binary zero	Binary zero
	"R"	000 - 364 /365					
	Blanks	Binary zero	Binary zero		"U" / "Q" / Binary zero		
"QI"	"A"	001 - 365 /366	00 - 23	00 - 59	00 - 59	Binary zero	Binary zero
	"R"	000 - 364 /365					
	Blanks	Binary zero	Binary zero		"U" / "Q" / Binary zero		
"RP" (BS2000 systems)	"A"	001 - 365 /366	00 - 23	00 - 59	00 - 59	Binary zero	Binary zero
	"R"	000 - 364 /365					
	Blank	Binary zero					

A: absolute time

R: relative time (= time interval)

In the case of DPUT NT/NE or DPUT QT/QE you have to specify the same times as for the associated DPUT NI or DPUT QI.

Setting the 2nd parameter

Here you have to supply the address of the message area from which openUTM is to read the message or user information or the RSO parameter list.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"DPUT"
KCOM	"NT"/"NE"/"QT"/"QE"/"NI"/"QI"/"RP"
KCLM	Length in bytes
KCRN	LTERM name / TAC / service ID / queue name
KCMF/kcfn	Format ID / blanks / Name of abstract syntax / Name of edit profile (only BS2000 systems)
KCDF	Screen function / binary zero
KCMOD	"R"/"A"/"BLANK"
KCTAG/...	Time specification (rel./abs.)
<ul style="list-style-type: none"> • KCTAG/kcday 	<ul style="list-style-type: none"> • Day (rel./abs.) / binary zero
<ul style="list-style-type: none"> • KCSTD/kchour 	<ul style="list-style-type: none"> • Hour (rel./abs.) / binary zero
<ul style="list-style-type: none"> • KCMIN 	<ul style="list-style-type: none"> • Minute (rel./abs.) / binary zero
<ul style="list-style-type: none"> • KCSEK/kcsec 	<ul style="list-style-type: none"> • Second (rel./abs.) / binary zero
KCQTYP	"U" / "Q" / binary zero
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_DPUTNT/KDCS_DPUTNE	(nb,kclm,kcrn,kcfn,kcdf,kcmod,kcday,kchour,kcmin,kcsec)
KDCS_DPUTQT/KDCS_DPUTQE	(nb,kclm,kcrn,kcfn,kcdf,kcmod,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DPUTNI	(nb,kclm,kcrn,kcmod,kcday,kchour,kcmin,kcsec)
KDCS_DPUTQI	(nb,kclm,kcrn,kcmod,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DPUTRP	(nb,kclm,kcrn,kcmod,kcday,kchour,kcmin,kcsec)

openUTM return information	
Field name in KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the DPUT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the DPUT operation code.

KCOM

In the KCOM field, enter the required operation modifier:

- NT for the message segment of the job
- NE for the total message or last message segment of the job
- NI for the user information associated with the job.
- QT for the message segment for a service-controlled queue
- QE for the entire message or last message segment for a service-controlled queue
- QI for the user information associated with the message for a service-controlled queue
- RP for the parameter list of an RSO printer (only on BS2000 systems).

KCLM

In the KCLM field, specify the length of the message to be sent (length zero is permissible).

For KCOM = RP, this is the length of the RSO parameter list (only on BS2000 systems).

KCRN

In the KCRN field, enter the destination of the message:

- the name of the LTERM partner if this DPUT call generates an output job or passes an RSO parameter list

-
- the name of the USER queue, TAC queue or temporary queue, if this DPUT call creates a message to a service-controlled queue (KCOM=QT/QE/QI).
 - the transaction code of an asynchronous program if this DPUT call generates a background job (without distributed processing)
 - the service ID of a job-receiving service if this background job is directed to a job-receiving service.

KCMF / kcfn

In the KCMF/kcfn field:

- Blanks in line mode or for a job sent to another application without distributed processing.
- In the case of messages to OSI TP partners:
The name of the abstract syntax of the message. Space characters stand for the abstract syntax of UDT; in this case, BER is used as the transfer syntax and the message is encoded by openUTM. If you enter a value other than blanks, the message must be transferred to openUTM in encoded format, i.e. in the transfer syntax corresponding to this abstract syntax.

Only on BS2000 systems:

- A format identifier in format mode

In the case of messages to RSO printers:

If a format has been specifically created for RSO printers then the FHS formatting system does not need to know the printer type because FHS generates a logical message which is then converted into the physical message by RSO.

If not, FHS must support the printer type as generated in RSO as otherwise formatting errors will occur.

- Blanks when passing an RSO parameter list.
- Edit profile(for line mode or an RSO printer)

If the message is to be sent to an RSO printer, then only the CCSNAME parameter of an edit profile is evaluated. The name of the character set is passed to RSO. All other parameters of the edit profile are ignored because these options are VTSU-B edit options, and the message is being prepared by RSO.

In the case of messages to an asynchronous service of the same application, to USER, TAC or temporary queues or to an LU6.1 partner, this field is irrelevant.

KCDF

In the KCDF field, enter the screen function for output jobs to terminals. Enter binary zero for user information (KCOM = NI/QI), RSO parameter lists or jobs for transport system applications.

In the case of background jobs, messages to LU6.1 partners and messages to USER, TAC and temporary queues, this field is irrelevant.

On BS2000 systems, you also have to specify binary zero if an edit profile or a #format is entered in KCMF /kcfn.

KCMOD

In the KCMOD field, select the type of time entry:

- A for absolute
- R for relative

-
- blanks, if the job is to be executed without a wait time.
messages to USER and temporary queues cannot be sent on a time-driven basis, which is why blanks must be specified in KCMOD

KCTAG / ...

Here you enter the necessary time specifications for the call, absolute or relative depending on the entry in KCMOD:

- for absolute time entry: desired time with day of the year in **KCTAG/kcday** (working day), hour in **KCSTD/kchour**, minute in **KCMIN** and second in **KCSEK/kcsec**.
- for relative time entry: interval to desired execution time with number of days in **KCTAG/kcday**, number of hours in **KCSTD/kchour**, number of minutes in **KCMIN** and the number of seconds in **KCSEK/kcsec**.
- for KCMOD = blanks:
binary zero if user information is to be logged with KCOM = NI/QI or when a message is to be sent to a USER or temporary queue (KCOM= QE/QT) (otherwise irrelevant)

KCQTYP

In the KCQTYP field, specify in the case of messages to a queue the type of the queue(only in conjunction with KCOM=QT/QE/QI):

- Q for a temporary queue created with QCRE
- U for a queue assigned to a user ID (USER queue)
- binary zero in all other cases

Message area

You enter in the message area the message or user information you want to output or the RSO parameter list you want to pass.

You enter the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area from which UTM is to read the message or user information or RSO parameter list. You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

In the KCRCCC field, the KDCS return code.

KCRCDC

In the KRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the DPUT call without job complex

The following codes can be analyzed in the program:

000 Function carried out

06Z Time entry changed without preceding DPUT NE, i.e. at least one of the fields KCMOD, KCTAG/kcday, KCSTD/kchour, KCMIN or KCSEK/kcsec has a value differing from that in the first message segment (for KCMOD=A/R).

openUTM takes the time entry from the first DPUT call and continues the message.

40Z openUTM cannot perform the function, see entry in KCRCDC. Possible causes:

- KCDF does not contain binary zero although this is required in this particular situation
- in the case of jobs without distributed processing, the name changes in KCRN and the type changes in KCQTYP, without the preceding DPUT job being terminated.
- in the case of distributed processing: there is no logical connection to the partner application and KCMOD = "BLANK".

41Z The call is not allowed at this location:

- the call was initiated in the first part of the sign-on service or
- the call was initiated in the sign-on service after a SIGNON call and before the PEND PS call.

42Z The entry in KCOM is invalid.

43Z The length entry in KCLM is negative or invalid.

44Z The value in KCRN or KCQTYP is invalid. Possible causes:

- the value is not the transaction code of an asynchronous program nor a TAC queue and there is no name of a LTERM partner or the LTERM name of an UPIC or HTTP client, and it is also not a valid service ID. See KCRCDC.
- although the value is the transaction code of an asynchronous programs, the transaction code is locked or access protected.
- KCQTYP=U: the value in KCRN does not specify a user or a user with access authorization.
- KCQTYP=Q: the value in KCRN does not specify a temporary queue.
- No queued messages can be generated for the dead letter queue (KDCDLETQ).
- for KCOM = RP (only on BS2000 systems): the value is not an RSO printer or the current RSO version does not support this function.

45Z The entry in KCMF/kcfn is invalid. Possible causes:

- the format identifier in KCMF/kcfn is not valid
- if the message destination is a partner to which communication is established using the OSI TP protocol, this return code indicates that the abstract syntax in the KCMF/kcfn field has not been generated for the partner application.

Only on BS2000 systems:

- for KCOM = RP: no blank entered
- the edit profile has not been generated
- the edit profile changes in message segments

47Z The address of the message area is invalid.

49Z The contents of unused fields of the KDCS parameter area are not equal to binary zero.

51Z After a DPUT NI/QI there is no DPUT NT/NE/QT/QE to the same destination.

52Z An attempt was made to send a time-driven message to a USER queue or temporary queue.

56Z The entry in KCMOD is invalid or the time entry in KCTAG/kcday, KCSTD/kchour, KCMIN or KCSEK/kcsec is invalid or is outside the generated time span.

An additional return code can be found in the dump:

71Z INIT was not issued in this program.

Features of the DPUT call

- The message area is not changed when the call is executed by UTM.
- More than one job can be generated in one program unit; the corresponding messages can each comprise more than one segment.
- You can also use screen output functions when you output +formats, *formats or messages in line mode, see chapter "[Screen output functions in format mode \(BS2000 systems\)](#)".
If you use #formats, you have to specify binary zero for KCDF, otherwise openUTM returns 40Z.
Only on BS2000 systems: If you use edit profiles (), openUTM also returns 40Z if you have not specified binary zero for KCDF.
- Jobs generated with DPUT are discarded as a result of PEND ER/FR, PEND RS or RSET.
- The TAC must be located at the beginning of the message area for DPUT calls to another UTM application that is generated as a transport system application.
- The message is also formatted before it is output.
- Messages are kept until:

-
- the referenced program unit or the printout is terminated, or
 - the transfer has succeeded for jobs to remote asynchronous services, or
 - the message is read at the terminal using KDCOUT and a new input has been made (except for the KDCLAST command).
 - the message to a queue is read by means of a DGET call, and the corresponding transaction is successfully completed.

- Jobs with messages of length 0

If you generate a message with a length of 0 (so-called "dummy message"), the following applies:

- a background job is executed, i.e. the asynchronous service is started without receiving a message
 - an empty format is output if the job is an output job in format mode
 - an output job for a transport system application is accepted, but will later be discarded by openUTM.
- Output jobs that are for one specific terminal are placed in the terminal message queue and can be read by the user with the KDCOUT command. Exactly one message is read per KDCOUT command. Each message can only be read once. If the KDCOUT command is entered more than once, then the next message is read from the terminal queue.

The user is informed at the end of a transaction that there are asynchronous messages available for a terminal through a message in the system status line.

This announcement can be suppressed on BS2000 systems if ANNOAMSG=N was specified in the configuration for the affected LTERM partner (default value: ANNOAMSG=Y). Asynchronous messages are then displayed immediately on the screen. This can disturb the dialog flow. The terminal user can, however, re-display the last screen using the KDCDISP command.

- There is no interaction between FPUT and DPUT calls, i.e. you can send DPUT calls with KCMOD = "BLANK" and FPUT calls to the same destination independently of each other.
- Print options for RSO printers (BS2000 systems)
If you use print options for jobs to RSO printers, you should first pass the list with the print options using DPUT RP, see RSO manual. Then submit the actual print job using DPUT NT/NE. The time specifications in DPUT RP and DPUT NT/NE must match.
- Handling message segments

- message segments in line mode are combined and output as **one** message to the LTERM partner. The message segments generated with DPUT are gathered by openUTM and terminated by the next PEND call, provided they have not yet been terminated by the program unit run with DPUT NE. When the transaction ends, the message segments are sent as a single message to the LTERM partner or to the other application.
- with formatted message segments to terminals, each segment generates a new format. The format name in KCMF may change. At a terminal, each format (each message segment) must be fetched with a KDCOUT command. Each DPUT NT call generates its own message. It is therefore not possible to structure the screen with different partial formats using DPUT NT calls. The formats arrive in the order in which they were sent.
- with message segments to printer, it is possible to switch between formatted message segments and unformatted message segments (in line mode). With message segments to terminals, this switch causes the old message to terminate and a new one to start.
- with DPUT NT calls to a local or asynchronous service each message segment must be read with a separate FGET.
- with DPUT QT calls to a service-controlled queue, each message segment must be read by means of a separate DGET.
- with PEND, the message segment most recently generated with DPUT is always assumed to be the final message segment, even if it was output with NT.
- In a sequence of message segments, a change of the destination specified in KCRN with no preceding DPUT NE/QE is only permissible in certain cases (see next point).
- Only on BS2000 systems: If the edit profile changes within a sequence of message segments addressed to a terminal, openUTM reacts with 45Z.
- The maximum possible number of DPUT NT/QE calls in a transaction depends on the RECBUF generation parameter in the KDCDEF statement MAX. 30 bytes per DPUT NE are occupied in this buffer. If the buffer is full, DPUT NE is rejected with KCRCDC=K704.

- Parallel messages

Parallel messages (i.e. change of destination before DPUT NE/NQ) are permissible if the destinations belong to different categories. There are three categories:

- LTERM partners, local asynchronous programs and service-controlled queues (KCRN=LTERM/TAC/queue name)
- job complexes (KCRN = complex ID)
- remote asynchronous services (KCRN = service ID) or remote TAC queues

Within these categories, parallel asynchronous jobs are only permitted if they are jobs for remote asynchronous services.

Apart from that, parallel job complexes are not supported, and the change of the LTERM/TAC/queue name requires the message to be concluded by means of DPUT NE/QE.

- Influence of generation parameters on the DPUT call

The following notes concern the generation of the UTM application. Further information on the individual generation parameters can be found in the openUTM manual "Generating Applications".

Limits for the time entry in the DPUT call are defined with the operands DPUTLIMIT1 and DPUTLIMIT2 in the MAX statement. The interval between the desired execution time and the DPUT call must not be greater than the time entry in DPUTLIMIT2 if **before** the time of the DPUT call, nor greater than the time entry in DPUTLIMIT1 if **after** the time of the DPUT call:

Current time - DPUTLIMIT2 < execution time < current time + DPUTLIMIT1

The time of the DPUT call is taken as the current time.

In the case of DPUT calls with KCMOD = A or R to LTERM partners generated with LTERM ..., QAMSG=N, openUTM does not check at the time of the DPUT call to see whether a client or printer is connected to the LTERM partner. It only does this once the time specified in the DPUT call has arrived. If there is then no connection, openUTM will store the message until a connection is set up.

In the case of DPUT calls with KCMOD = "BLANK" to LTERM partners generated with LTERM ..., QAMSG=N, openUTM checks at the time of the DPUT call whether a client/printer is connected to this LTERM partner. If not, UTM rejects the call with KCRCCC = 44Z, KCRCDC= K705.

For all messages to terminals and transport system applications generated with DPUT, the entire message must not exceed the maximum length of 32700 bytes.

When the KDCFILE is regenerated with the UTM tool KDCUPD, you can specify in the TRANSFER statement precisely which messages you wish to transfer to the new KDCFILE (see also openUTM manual "Generating Applications").

- The UTM administrator can use the administration call KDCINF STAT to query the number of waiting time-driven jobs (see the openUTM manual "Administering Applications", Administration commands, KDCINF).
- DPUT calls with distributed processing
 - Prior to the DPUT call, the KDCS parameter area in the job-submitting service must be given the same values as for sending messages to a TAC queue or for generating background jobs to an asynchronous program in its own application. The only thing that has to be specified as name in the KCRN field is the service ID which was assigned to the job-receiving service in the APRO call.
 - Once the DPUT NE/QE call has terminated (final message segment or complete message) or after the KDCS return code 40Z, the service ID in the job-submitting service is released. This ID can now be used to address another job-receiving service.
 - Only after the specified time has elapsed will the job generated with DPUT be sent to the partner application (if a free session or association is available).
 - Parallel asynchronous jobs to different job-receiving services are permissible.
- User information (DPUT NI/QI)

User information is always associated with a job generated by a DPUT call. The user information must be generated before the job itself. The addressee (entry in KCRN) and the time entry in the user information and in the job must agree. If this is not sequence is not adhered to, error 51Z occurs. If the associated job for an item of user information does not exist (i.e. if there is user information but no job), openUTM aborts the service at the PEND call with KCRCCC = 86Z.

User information can only be read with a DADM call; it is a type of "log information" and is not transferred to the addressee. The user information of a confirmation job can not be read until the confirmation job has been activated.

-
- Background jobs for an asynchronous program in the same application

Each background job starts an asynchronous service at the time specified.

Asynchronous programs which run in time-driven mode should check whether their work is still relevant, or whether they should terminate immediately. The program can ascertain the current time and date, as well as the time and date of application start-up, via the INFO call.

If the program needs the time of the DPUT call, it must be contained in the message.

DPUT calls can also be used to implement periodically recurring asynchronous jobs. This is done with an asynchronous program containing the periodically recurring action as well as a DPUT call to the program itself. The time can be specified as relative or absolute.

7.7.2 DPUT call in a job complex

A DPUT call within a job complex enables you to

- send time-driven messages (so-called basic jobs) and the associated messages/message segments (output jobs for LTERM partners or for asynchronous services, messages to TAC queues or background jobs to asynchronous services or TAC queues previously addressed with an APRO AM call)
- have user information associated with these jobs logged
- generate confirmation jobs and associated user information.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and corresponding entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCLM	KCRN	KCMF	KCDF
Basic job for LTERM partner or for local asynchronous service or local TAC queue	"DPUT"	"NT"/"NE"	Length	Complex ID	Format ID / blanks/ name of abstract syntax / edit profile (only BS2000 systems)	Screen function / binary zero
Basic job for TAC queue	"DPUT"	"QT"/"QE"	Length	Complex ID	—	
Basic job for remote asynchronous service or remote TAC queue	"DPUT"	"NT"/"NE"	Length	Complex ID	—	
User information for a job	"DPUT"	"NI"/"QI"	Length	Complex ID	Blanks	binary zero
Create confirmation job	"DPUT"	"+T"/"-T"	Length	Complex ID	Blanks	binary zero
User information for confirmation job	"DPUT"	"+I"/"-I"	Length	Complex ID	Blanks	binary zero

The operation modifiers in the KCOP field have the following significance:

NT/QT: message segment of a basic job

NE/QE: last message segment or total message of a basic job

NI/QI: user information associated with basic job

+T/-T: positive or negative confirmation job

+I/-I: user information associated with positive or negative confirmation job

The QE/QT/QI operation modifiers refer to a basic job with a TAC queue as the destination. It is not possible to specify a USER or temporary queue as the destination in the DPUT call in the job complex, because KCQTYP is not evaluated here and the destination is specified for the associated MCOM call.

The time entries for DPUT NT/NE/NI or DPUT QT/QE/QI are made as for the DPUT call without job complex. For DPUT NI/QI/+T/-T/+I/-I you have to set binary zero in all the unused fields of the KDCS parameter area.

Setting the 2nd parameter

Here you have to supply the address of the message area from which openUTM is to read the message or user information.

Setting the parameters	
Field name in KDCS parameter area	Contents
KCOP	"DPUT"
KCOM	"NT"/"NE"/"NI"/"QT"/"QE"/"QI"/"+T"/"-T"/ "+I"/"-I"
KCLM	Length in bytes
KCRN	Complex identifier
KCMF/kcfn	Format ID / blanks / name of abstract syntax / name of edit profile (only BS2000 systems)
KCDF	Screen function / binary zero
KCMOD	""R"/"A"/"?" / binary zero
KCTAG / ...	
• KCTAG/kcday	Day (rel./abs.)/"?" / binary zero
• KCSTD/kchour	Hour (r./a.)/"?" / binary zero
• KCMIN	Minute (r./a.)/"?" / binary zero
• KCSEK/kcsec	Second (r./a.)/"?" / binary zero
KCQTYP	irrelevant (not evaluated)
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_DPUTNT/KDCS_DPUTNE	(nb,kclm,kcrn,kcfn,kcdf,kcmod,kcday,kchour,kcmin,kcsec)
KDCS_DPUTQT/KDCS_DPUTQE	(nb,kclm,kcrn,kcfn,kcdf,kcmod,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DPUTNI	(nb,kclm,kcrn,kcmod,kcday,kchour,kcmin,kcsec)
KDCS_DPUTQI	(nb,kclm,kcrn,kcmod,kcday,kchour,kcmin,kcsec,kcqtyp)
KDCS_DPUTPT / KDCS_DPUTMT / KDCS_DPUTPI / KDCS_DPUTMI	(nb,kclm,kcrn)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the DPUT call within a job complex you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the DPUT operation code.

KCOM

In the KCOM field, enter the required operation modifier:

- NT/QT for message segment of the basic job
- NE/QE for total message or last message segment of the basic job
- NI/QI for user information associated with the basic job
- +T for a positive confirmation job
- -T for a negative confirmation job
- +I for user information relating to the positive confirmation job
- -I for user information relating to the negative confirmation job

The QE/QT/QI operation modifiers refer to a basic job with a TAC queue as the destination.

KCLM

In the KCLM field, specify the length of the message to be sent (length zero is permissible).

KCRN

In the KCRN field, enter the complex identifier (complex ID) assigned to the job complex (assigned in the MCOM call).

KCMF/kcfn

In the KCMF/kcfn (irrelevant for messages sent to an asynchronous service of the same application or to an LU6.1 partner):

- Blanks in line mode or for a job sent to another application without distributed processing.

In messages to OSI TP partners:

- The name of the abstract syntax of the message. Space characters stand for the abstract syntax of UDT; in this case, BER is used as the transfer syntax and the message is encoded by openUTM. If you enter a value other than blanks, the message must be transferred to openUTM in encoded format, i.e. in the transfer syntax corresponding to this abstract syntax.

Only on BS2000 systems:

- A format identifier in format mode

In the case of messages to RSO printers:

If a format has been specifically created for RSO printers then the FHS formatting system does not need to know the printer type because FHS generates a logical message which is then converted into the physical message by RSO.

If not, FHS must support the printer type as generated in RSO as otherwise formatting errors will occur.

- Edit profile (for line mode or an RSO printer)
If the message is to be sent to an RSO printer, then only the CCSNAME parameter of an edit profile is evaluated. The name of the character set is passed to RSO. All other parameters of the edit profile are ignored because these options are VTSU-B edit options, and the message is being prepared by RSO.

KCDF

In the KCDF field, enter the screen function for output jobs to terminals. Enter binary zero for user information (KCOM = NI/QI) or jobs for transport system applications.

This field is irrelevant for background jobs and messages to TAC queues.

On BS2000 systems, you must also specify binary zero if an edit profile or a #format is entered in KCMF/kcfn.

KCMOD

In the v field, you select the type of time entry for messages to the basic job (KCOM=NT/NE/NI or QT/QE/QI):

- A for absolute
- R for relative
- blanks, if the job is to be executed without wait time

Binary zero must be entered for messages to confirmation jobs (KCOM = +T/-T/+I/-I).

KCTAG / ...

For KCOM = NT/NE/NI or QT/QE/QI enter the necessary time specifications as for the DPUT call without job complex in these fields. For KCOM = +T/-T/+I/-I enter binary zero.

KCQTYP

The KCQTYP field is not evaluated.

Message area

Make the following entry in the message area:
the message or user information you want to output.

You enter the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area from which openUTM is to read the message (or user information). You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

In the KCRCCC field, the KDCS return code.

KCRCDC

In the KRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the DPUT call in a job complex

The following codes can be analyzed in the program:

- 000 Function carried out.
- 06Z Time entry changed without preceding DPUT NE, i.e. at least one of the fields KCMOD, KCTAG/kcday, KCSTD/kchour, KCMIN or KCSEK/kcsec has a value differing from that in the first message segment (for KCMOD=A/R).
openUTM takes the time entry from the first DPUT call and continues the message
- 40Z openUTM cannot perform the function, see entry in KRCDC. For distributed processing: there is no logical connection to the partner application and KCMOD = "BLANK".

41Z The call is not allowed at this location:

- an additional basic job is to be issued or user information is to be logged after a basic job (DPUT NE /QE) has been completed or
- the format identifier changes due to several DPUT NTs or
- the call was initiated in the first part of the sign-on service or
- the call was initiated in the sign-on service after a SIGNON call and before the PEND PS call.

42Z The entry in KCOM is invalid or KCOM = +T/-T was specified without defining a job complex or destination for the confirmation job

43Z The length entry in KCLM is negative or invalid.

44Z The complex identifier given in KCRN is invalid.

45Z The entry in KCMF/kcfn is invalid. Possible causes:

- the format identifier in KCMF/kcfn is invalid
- if the message destination is a partner with which communication is performed using the OSI TP protocol, this return code indicates that the abstract syntax specified in the KCMF/kcfn field has not been generated for the partner application.

Only on BS2000 systems:

- the edit profile has not been generated
- the edit profile changes in message segments

47Z The address of the message area is invalid.

49Z The contents of unused fields of the KDCS parameter area are not equal to binary zero.

51Z Incorrect DPUT call sequence (see below).

56Z The entry in KCMOD is invalid or the time entry in KCTAG/kcday, KCSTD/kchour, KCMIN or KCSEK/kcsec is invalid or is outside the generated timespan.

An additional return code can be found in the dump:

71Z INIT call missing in this program.

Features of the DPUT call within a job complex

- The following rules hold for the order of the DPUT calls:
 - the user information has to be written before the associated (confirmation) job: DPUT NI before DPUT NT/NE or DPUT QI before DPUT QT/QE, DPUT +I before DPUT +T and DPUT -I before DPUT -T. Only one DPUT +I/-I per DPUT +T/-T is permitted. The user information of a confirmation job cannot be read until the confirmation job has been activated.
 - the basic job must be started before the first confirmation job: DPUT NT/NE or DPUT QT/QE before the first DPUT +T/-T. Two or more DPUT +T or DPUT -T are permissible; these are considered in each case as **one** positive confirmation job (with +T) and **one** negative confirmation job (with -T).

- Changing the format identifier if there are more than one message segments (DPUT NT) is not permissible.
- If a DPUT call has return code 40Z all the messages and information associated with the job complex are lost; the complex ID is released.

For DPUT messages via distributed processing the service ID is also released with 40Z.

For all other return codes smaller than 70Z all the data of the complex is kept including the complex ID.

- Parallel asynchronous jobs (i.e. change of destination before DPUT NE/QE) are permitted if the destinations belong to different categories, i.e. it is possible to have a DPUT with KCRN = LTERM/TAC/Queue or KCRN = VGID before the DPUT NE.

Example for parallel asynchronous jobs

KDCS call	Destination and identifier	Remarks
MCOM BC	KCRN = PRINTER1 KCCCOMID = *COMPLEX KCPOS = ATAC5	Define start of a job complex and destinations of the job
DPUT NT	KCRN = *COMPLEX	1st message segment of basic job
DPUT NE	KCRN = ATAC1	Background job for a program
APRO AM	KCRN = LTAC KCPA = APPL1 KCPI = > VGID	Address job-receiving service
DPUT NE	KCRN = > VGID	Background job for job-receiving service
DPUT NE	KCRN = *COMPLEX	2nd message segment of basic job
DPUT +T	KCRN = *COMPLEX	Positive confirmation job
MCOM EC	KCRN = binary zero KCCCOMID = *COMPLEX	End of job complex

7.8 FGET Receive asynchronous message

The FGET (free message GET) call enables you to read an asynchronous message or message segment into the message area from the message queue allocated to the service.

The FGET call is only permitted in the first program unit run and processing step of an asynchronous service. Each message can only be read once. Each message segment must be read with its own FGET. The message (message segment) can be read again following an RSET call.

The format of the FGET call is described in detail below. For further information on message queuing refer to section ["Message Queuing \(asynchronous processing\)"](#).

Setting the KDCS parameter area (1st parameter)

The table below shows the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area		
	KCOP	KCLA	KCMF/kcfn
Read asynchronous message	"FGET"	Length	Format identifier / blanks / name of abstract syntax / edit profile (only on BS2000 systems)

Setting the 2nd parameter

Here you have to supply the address of the message area into which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"FGET"
KCLA	Length in bytes
KCMF/kcfn	Format identifier / blanks / name of abstract syntax / name of edit profile (only on BS2000 systems)

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_FGET	(nb,kcla,kcfn)

openUTM return information	
Message area	Contents
	Data
Field name in the KB return area	
KCRLM	Actual length
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcrfn	Format identifier/blanks
KCRRC	Redelivery counter

For the FGET call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the FGET operation code.

KCLA

In the KCLA field, specify the length in which the message is to be read. This length must not exceed the message area into which the message is to be read. Length zero means no receiving of messages. Any existing messages are lost.

KCMF/kcrfn

In the KCMF/kcrfn field, enter the format of the message to be read:

- in line mode: blanks
or on BS2000 systems: name of the **edit profile** (returned in the KCRMF/kcrfn field in the case of INIT). This name starts with a blank.
- in format mode on BS2000 systems: format identifier of the expected (partial) format. This is returned in the KCRMF/kcrfn field in the case of INIT or a preceding FGET call.
- for a message from a program unit of the same application or from an LU6.1 partner: irrelevant.

in messages to an OSI TP partner:

- name of the abstract syntax of the message.
This name was returned in the KCRMF/kcrfn field in the preceding INIT call. Here, blanks represent the abstract UDT syntax encoded in accordance with BER (Basic Encoding Rules); only in this case does openUTM transfer the message to the program unit decoded.
If you enter a value other than blanks, openUTM transfers the message to the program unit in encoded format (i.e. in the transfer syntax corresponding to this abstract syntax) and the program unit itself must convert the message into the local representation. This is possible, for example, using an ASN.1 compiler.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area into which openUTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section [“C/C++ macro interface”](#).

openUTM returns:

Message area

in the specified message area, the message (segment) in its actual or at most in its desired length.

KCRLM

in the KCRLM field, the actual length of the message (segment), possibly deviating from the length requested in the KCLA of the parameter area.

KCRCCC

in the KCRCCC field the KDCS return code (see next page).

KCRCDC

In the KRCDC field, the internal return code of openUTM (see the openUTM manual “Messages, Debugging and Diagnostics”).

KCRMF/kcrfn

In the KCRMF/kcrfn field:

- After reading in line mode: blanks
or on BS2000 systems: name of the edit profile of the last output message.
- After reading a partner service:
name of the format identifier or abstract syntax of the next message (segment).

Only on BS2000 systems:

- After reading an entire format: ID of most recently read format (always identical to ID of last output format).
- After reading a partial format: Identifier of the next format with input data.
- After reading final partial format: ID of most recently read partial format. In this case KCRMF = KCMF (or: kcrfn=kcrfn).

KCRRC

in the KCRRC field, the redelivery counter of the message read. This contains the number of redeliveries of the FGET message after abnormal termination of the asynchronous services in the first transaction.

Sender information, etc. is located in the KB header (entered by openUTM during INIT).

KDCS return codes in the KCRCCC field for the FGET call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 01Z Length conflict: $KCLA < KCRLM$; message was truncated.
- 03Z With partial formats:
KCMF/kcfn does not contain the name of the next returned partial format; the message area is unchanged and $KCRLM = 0$.

Entry message from a OSI TP partner:
KCMF/kcfn does not contain the abstract syntax of the next message to be read. No message is transferred to the message area.
- 05Z With individual formats: format in screen display different from format entered in KCMF/kcfn.

Only on BS2000 systems:
In line mode: edit profile in screen display different from edit profile entered in KCMF/kcfn.
- 10Z Message or all message segments already completely read.

Additional error codes to be found in the dump:

- 71Z Function called in a follow-up program unit or following a PGWT call of an asynchronous service or in a dialog service or still no INIT issued in program unit run.
- 73Z Length entry in KCLA negative or invalid.
- 77Z The message area is missing or cannot be accessed in the specified length.

Features of the FGET call

- The actual message length is returned in the KCRLM field. The following holds:
 - When $KCRLM \leq KCLA$, only KCRLM characters (bytes) are transferred into the message area. The contents of the remainder of the message area are undefined.
 - When $KCRLM > KCLA$, only KCLA characters are transferred into the message area. The remaining bytes ($KCRLM - KCLA$) are lost. They can no longer be read with a subsequent FGET.
- The description of the MGET call presents an example explaining how openUTM reacts in case of length conflicts
- A program unit can also receive asynchronous messages of length 0 when, for example,
 - a function key was pressed, but no message was allocated
 - a transaction code was sent without further data
 - if a program in the same application sent a background job with a message of length 0.

-
- TAC input from the terminal or a transport system application:
 - When an asynchronous TAC is entered in line mode and a format ID is entered in KCMF/kcfn, return code KCRCCC=05Z is not set (as with MGET), but rather KCRCCC=000, assuming the call is otherwise error-free.
 - When partial formats are input, each partial format must be read using a separate FGET.
 - If a message is input together with an asynchronous TAC, the TAC is separated from the message: the TAC is not read into the message area, but is available in the KB header after INIT.
 - openUTM does not convert from lowercase to uppercase letters.

Only on BS2000 systems: However, conversion is possible using edit profiles.

- The number of redeliveries is returned in the KCRRRC field. A message is always redelivered if an asynchronous service was terminated abnormally in the first transaction. The application must have been generated accordingly and the generated maximum number of redeliveries must not have been reached. For more information refer to the openUTM manual “Generating Applications”, REDELIVERY operand in the MAX statement.
- Saving faulty messages into the dead letter queue:

If an error occurs, asynchronous messages to transaction codes can be saved into the global dead letter queue as a last fallback stage. The TAC must be generated with DEAD-LETTER-Q=YES for this. If the asynchronous process terminates abnormally without successful termination of a transaction, the FGET message is placed in the dead letter queue if it cannot be redelivered (see redelivery) and no negative acknowledgement job was defined. As soon as an asynchronous process has reached a save point, neither redelivery nor saving the FGET message into the dead letter queue is possible since the message is taken to have been successfully processed. When a message is saved into the dead letter queue, the number of redeliveries for this message is rolled back to zero if necessary.

i Each message segment sent with FPUT NT must be read using a separate FGET.

7.9 FPUT Generating asynchronous messages

The FPUT (free message PUT) call enables you to create messages or message segments for message queues, which openUTM enters in receiver-specific queue:

- output jobs for LTERM partners
- background jobs for local asynchronous services
- background jobs for remote asynchronous services previously addressed with APRO AM calls
- asynchronous messages for local or remote TAC queues
- Only on BS2000 systems: pass print options (= RSO parameter list) for RSO printers

The message segments generated with FPUT are gathered by openUTM and terminated with the next PEND call. When the transaction ends the message segments are input as a single message into the appropriate message queue. Exception: If you send formatted message segments to terminals, each of these segments forms a separate message.

In the case of TAC queues, the recipient must read the message from the queue in a separate transaction.

Messages remain in a message queue until they are:

- successfully sent (LTERM partner)
- successfully processed (asynchronous service) or
- successfully read (TAC queue).

The format of the FPUT call is described in detail below. For further information on message queuing refer to section [“Message Queuing \(asynchronous processing\)”](#).

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCLM	KCRN	KCMF/kcfn	KCDF
Output job in format mode	"FPUT"	"NT"/ NE"	Length	LTERM name	Format identifier	Screen function
Unix, Linux, Windows systems: Output job in line mode	"FPUT"	"NT"/ NE"	Length	LTERM name	Blanks	—
BS2000 systems: Output job in line mode	"FPUT"	"NT"/ NE"	Length	LTERM name	Blanks / edit profile	Screen function / binary zero
Message for asynchronous program or TAC queue of the same application	"FPUT"	"NT"/ NE"	Length	TAC / Name of a TAC queue	—	—
Output job for transport system application	"FPUT"	"NT"/ NE"	Length	LTERM name of application	Blanks	Binary zero
Background job via LU6.1	"FPUT"	"NT"/ NE"	Length	service ID	—	—
Background job via OSITP	"FPUT"	"NT"/ NE"	Length	service ID	Name of abstract syntax / blanks	—
BS2000 systems: Pass parameter list for RSO printers	"FPUT"	"RP"	Length	LTERM name	Blank	Binary zero

NT: message segment of the job

NE: last message segment or entire message of the job

RP: RSO parameter list (BS2000 systems)

Setting the 2nd parameter

Here you have to supply the address of the message area from which openUTM is to read the message or the RSO parameter list.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"FPUT"
KCOM	"NT"/"NE"/"RP"
KCLM	Length in bytes
KCRN	LTERM name / TAC queue / service ID
KCMF/kcfn	Format identifier / blanks / edit profile (only on BS2000 systems)
KCDF	Screen function/binary zero
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro call	
Macro names	Parameters
KDCS_FPUTNT / KDCS_FPUTNE	(nb,kclm,kcrn,kcfn,kcdf)
KDCS_FPUTRP	(nb,kclm,kcrn)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the FPUT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the FPUT operation code.

KCOM

In the KCOM field, enter either NT or NE for total message or last message segment or RP for an RSO parameter list.

KCLM

In the KCLM field, specify the length of the message to be sent in the message area (length zero is permissible).

For KCOM = RP on BS2000 systems, this is the length of the data structure for the RSO parameter list.

KCRN

In the KCRN field, enter the destination of the message:

- the name of the LTERM partner if this FPUT call generates an output job or passes an RSO parameter list
- the transaction code of an asynchronous program if this FPUT generates a background job (without distributed processing)
- the service ID of a job-receiving service if this background job is directed to a job-receiving service
- the name of the TAC queue if the message is to be sent to a TAC queue
- the service ID of the remote TAC queue if this message is to be sent to a remote TAC queue

KCMF / kcfn

In the KCMF/kcfn field (If messages are sent to an asynchronous service or a TAC queue of the same application or to an LU6.1 partner then this field is irrelevant), specify:

- Blanks in line mode or for a job sent to another application without distributed processing or when passing an RSO parameter list.

In messages to an OSI TP partner:

- The name of the abstract syntax of the message. Here, blanks represent the abstract syntax of UTD. In this case the BER transfer syntax is used and the message is encoded openUTM.
If you enter a value other than blanks, the message must be transferred to openUTM in encoded form, i.e. in the transfer syntax corresponding to this abstract syntax.

Only on BS2000 systems:

- A format identifier (in format mode)

In the case of messages to RSO printers:

If a format has been specifically created for RSO printers then the FHS formatting system does not need to know the printer type because FHS generates a logical message which is then converted into the physical message by RSO.

If not, FHS must support the printer type as generated in RSO as otherwise formatting errors will occur.

-
- Edit profile (for line mode or an RSO printer)
If the message is to be sent to an RSO printer, then only the CCSNAME parameter of an edit profile is evaluated. The name of the character set is passed to RSO. All other parameters of the edit profile are ignored because these options are VTSU-B edit options, and the message is being prepared by RSO.

KCDF

In the KCDF field (irrelevant for background jobs and TAC queues):
the screen function if the FPUT call is intended for an LTERM partner. Enter binary zero for jobs to other applications without distributed processing or when passing RSO parameter lists.

On BS2000 systems, you must also specify binary zero if an edit profile or a #format is specified in KCMF/kcfn.

Message area

In the message area, you specify the message you want to output or the RSO parameter list you want to pass.

You enter the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area from which openUTM is to read the message or RSO parameter list. You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

In the KCRCCC field, the KDCS return code (see next page).

KCRCDC

In the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the FPUT call

The following codes can be analyzed in the program:

- 000 Function carried out
- 04Z The name in KCRN changes, and FPUT NE was not specified before.
- 40Z openUTM cannot perform the function (system or generation error, deadlock, long-term locks), see KCRCDC.
- 41Z KCRN addressed the LTERM partner that started the current service or FPUT was issued in the first part of the sign-on service or an FPUT call was issued in the sign-on service after the SIGN ON and before the PEND PS.

42Z Entry in KCOM invalid.

43Z Length entry in KCLM negative or invalid.

44Z Value in KCRN is not a TAC of an asynchronous program or a TAC queue, or the TAC is locked or prohibited and there is no name of an LTERM partner or the LTERM name of a UPIC or HTTP client, or there is no valid service ID (with distributed processing). See KCRCDC.
No asynchronous messages are allowed for the dead letter queue (KDCDLETQ).

Only on BS2000 systems:

For KCOM = RP the value in KCRN is not an RSO printer or the current version does not support this function.

45Z The entry in KCMF/kcfn is invalid. Possible causes:

- the format identifier in KCMF/kcfn is invalid
- if the message destination is a partner with which communication is performed using the OSI TP protocol, this return code indicates that the abstract syntax in the KCMF/kcfn field has not been generated for the partner application.

Only on BS2000 systems:

- for KCOM = RP: no blank entered
- the edit profile has not been generated
- the edit profile changes in message segments to terminals

47Z The message area is missing or not accessible in the specified length.

An additional error code can be found in the dump:

71Z INIT call missing in this program.

Features of the FPUT/DPUT call

- FPUT and DPUT calls which direct program units to an alias LTERM are processed as follows:
 - In an LTERM group without an LTERM bundle, openUTM sends FPUT/DPUT calls via the PTERM which is assigned to the primary LTERM.
 - In the case of an LTERM group whose primary LTERM is the master LTERM of an LTERM bundle, openUTM assigns all the queued messages sent to the group's alias LTERMs during this transaction to one of the slave LTERMs on transaction end. This procedure guarantees that the receiver possesses the same message sequence as was generated for an LTERM group during a transaction.
- FPUT and DPUT calls which direct program units to the master LTERM are assigned to one of the slave LTERMs at transaction end.
- FPUT and DPUT calls can also direct program units directly to the primary LTERM.
- The message area is not changed when openUTM executes the call
- Several jobs can be created in a program unit; the corresponding messages can consist of several segments.

-
- For outputs in +formats, *formats or messages in line mode you can also use the screen output functions, see the chapter "[Screen output functions in format mode \(BS2000 systems\)](#)".

Only on BS2000 systems:

- If you use #formats, then the KCDF must be set to binary zero, otherwise openUTM reacts with 40Z.
- Similarly, when working with edit profiles openUTM responds with 40Z if KCDF has not been set to binary zero.
- The jobs created with FPUT are discarded as a result of PEND ER/FR, PEND RS or RSET.
- No output job to the client with which the program is currently working (KCRN != KCLOGTER) may be generated in a dialog program.
- With FPUT calls to another UTM application which was generated as a transport system application, the TAC must be located at the start of the message area.
- If necessary, the message is formatted before being output.
- Asynchronous jobs are kept until:
 - the referenced program unit or printout is terminated, or, with jobs to remote asynchronous services, the transfer has been terminated successfully
 - the message is read at the terminal with KDCOUT and a new input has been made (except for the KDCLAST command) or
 - the message is read from a TAC queue by means of a DGET call and the transaction containing the DGET is completed successfully.
- Jobs with messages of length 0
 - If a message with a length of 0 is created (known as a "dummy message"), the following applies:
 - a background job is executed, i.e. the asynchronous service is started without receiving a message
 - an empty format is output if the job is an output job for a format terminal
 - in the case of a message for a TAC queue, an empty message is created that can be read by means of a DGET call
 - if the job is an output job for a transport system, it is accepted but will later be discarded by openUTM.
- Background jobs for an asynchronous program in the same application: Each background job starts a separate asynchronous service. If several complete messages are sent to the same TAC in a program unit run, a separate asynchronous service is started for each message.
- If several complete messages are sent to the same TAC queue in a program unit run, each message must be read by means of a separate DGET FT call.
- There is no interaction between FPUT and DPUT calls, i.e. DPUT calls with KCMOD = "BLANK" and FPUT calls can be sent at a certain location independent of one another.
- Output jobs intended for a terminal are inserted into the message queue and can be retrieved by the user with the KDCOUT command. Each KDCOUT command retrieves exactly one message. Each message can only be retrieved once. If the KDCOUT command is repeated the next message is retrieved from the queue.

At the end of transaction, a message in the system line informs the terminal user whether asynchronous messages are present for the terminal.

You can suppress this message on BS2000 systems by setting ANNOAMSG=N for the associated LTERM partner in the configuration (default value: ANNOAMSG=Y). Asynchronous messages are then displayed immediately on the screen. This may interrupt the dialog. However, the terminal user can use the KDCDISP command to display the last screen again.

-
- Print options for RSO printers (BS2000 systems)

If you use print options for jobs to RSO printers, you should first pass the list with the print options using FPUT RP, see RSO manual. Then submit the actual print job using FPUT NT/NE.

- Handling message segments

- Message segments in line mode are combined into **one** message and sent to the LTERM partner. The message segments generated with FPUT are gathered by openUTM and terminated with the next PEND call, provided they have not yet been terminated in the program unit run with FPUT NE. When the transaction ends, the message segments are sent as a single message to the LTERM partner or to another application.
- With formatted message segments to terminals, each segment forms a separate message. The format name in KCMF/kcfn needs not always stay the same. At a terminal, each format (message segment) must be fetched with a KDCOUT command. Each FPUT NT call generates a separate message. It is therefore not possible to structure a screen with different partial formats using FPUT NT calls. The formats arrive in the order in which they were sent.
- With message segments to printer, it is possible to switch between formatted message segments and unformatted message segments (in line mode). With message segments to terminals, this switch causes the old message to terminate and a new one to start.
- With FPUT NT calls to local or remote asynchronous services or local or remote TAC queues, each message segment must be read with a separate FGET NT.
- With PEND, the message segment most recently generated with FPUT is always assumed to be the final message segment, even if it was output with NT.
- The maximum number of FPUT NE calls which are possible in a transaction depends on the RECBUF generation parameter in the KDCDEF statement MAX. Each FPUT NE occupies 30 bytes in this buffer. If the buffer is full, FPUT NE is rejected with KCR CDC=K704.
- If, in a sequence of message segments, the name in KCRN (i.e. the message receiver) changes but no FPUT with "NE" was entered previously, a warning is issued (04Z) and a new message is started. The previous message (sequence of message segments) is terminated. This means that if the name in KCRN is changed back to the first recipient with a subsequent FPUT, the first message is **not** continued, but a new message is begun. The message is forwarded to the receiver when the next synchronization point is reached. Parallel messages, as used in DPUT, are therefore not possible.
- Only on BS2000 systems: If the edit profile changes within a sequence of message segments addressed to a terminal, openUTM reacts with 45Z.

- Influence of generation parameters on the FPUT call

The following notes concern the generation of the UTM application. Further information on the individual generation parameters can be found in the openUTM manual "Generating Applications".

- For messages for terminals and transport system applications, the total message may not exceed the value generated for the NB operand of the control statement MAX. In the case of messages to other partners the length of a message segment is limited to 32,767 bytes and the length of the total message is unlimited.
 - When the KDCFILE is regenerated with the UTM tool KDCUPD, you can specify in the TRANSFER statement precisely which messages you want to include in the new KDCFILE (see also the openUTM manual "Generating Applications").
 - Only on BS2000 systems: The ANNOAMSG operand in the KDCDEF control statement LTERM defines for each LTERM partner whether asynchronous messages are to be output immediately to this terminal or announced with a message. This message appears in the system status line.
- FPUT calls with distributed processing

-
- In the job-submitting service, the KDCS parameter area must be given the same values as for background jobs for an asynchronous program in its own application. The only thing that has to be specified as name in the KCRN field is the service ID which was assigned to the job-receiving service in the APRO AM call.
 - Once the FPUT NE call has terminated (final message segment or complete message) or after return of the KDCS error code 40Z, the service ID is released. This ID can now be used for a new job submitter/receiver relationship in this service.
 - If the wait time for using a session or association was set to 0 at generation time, and if no connection exists with the partner application at the time the FPUT call is issued, openUTM sets the error codes 40Z in KCRCCC and KD13 in KCRCDC after the FPUT call.

7.10 GTDA Read from TLS

The GTDA (get data) call enables you to read a TLS block (terminal specific long-term storage) into the specified message area. The block name is assigned during generation (TLS statement for KDCDEF).

A program unit of a dialog service can only read blocks from its "own" TLS, i.e. only the TLS of the LTERM/LPAP /OSI LPAP partner, via which the service was started.

A program unit run of an asynchronous service can read blocks from all the LTERM/LPAP/OSI-LPAP/Master-LPAP partners of a UTM application.

Setting the KDCS parameter area (1st parameter)

The table below shows the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area			
	KCOP	KCLA	KCRN	KCLT
Read from TLS (in dialog program)	"GTDA"	Length	Block name	—
Read from TLS (in asynchronous program)	"GTDA"	Length	Block name	LTERM / LPAP / OSI-LPAP / Master-LPAP name

Setting the 2nd parameter

Here you have to supply the address of the message area into which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"GTDA"
KCLA	Length in bytes
KCRN	Block name
KCLT	LTERM / LPAP / OSI-LPAP / Master-LPAP / -

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro call	
Macro names	Parameters
KDCS_GTDA	(nb,kcla,kcrn,kclt)

openUTM return information	
Message area	Contents
	Data
Field name in the KB return area	
KCRLM	Actual block length
KCRCCC	Return code
KCRCDC	Internal return code

For the GTDA call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the GTDA operation code.

KCLA

In the KCLA field, the length of the data to be transferred from the TLS.

KCRN

In the KCRN field, the name of the TLS block from which openUTM is to transfer data.

KCLT

For asynchronous programs only:

in the KCLT field, the name of LTERM/LPAP/OSI-LPAP/Master-LPAP partner whose TLS is to be read from (this field is not evaluated by dialog programs).

You enter the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area to which openUTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

Message area

The desired data in the specified message area.

KCRLM

In the KCRLM field, the actual length of the data in the TLS so that the program can detect deviations from the KCLA entry (important if KCLA entry is smaller). Exception: for KCLA = 0 you always have 0 returned in KCRLM.

KCRCCC

In the KCRCCC field, the KDCS return code, see next page.

KCRCDC

In the KRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the GTDA call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 40Z System cannot perform operation (generation error or system error, deadlock, time-out); see KRCDC.
- 41Z Call was issued in the first part of the sign-on service although this is not permitted by the generation.
- 43Z Length entry in KCLA invalid (e.g. negative).
- 44Z Block name in KCRN unknown or invalid.
- 46Z The LTERM/LPAP/OSI-LPAP/Master-LPAPname in KCLT invalid (with asynchronous programs only).
- 47Z Message area missing or cannot be accessed in the specified length.

An additional error code can be found in the dump:

- 71Z INIT missing in this program.

Features of the GTDA call

- A GTDA call locks the referenced TLS block against access for all the competing program units. All other TLS block of the referenced LTERM, LPAP or OSI LPAP partner are free
The TLS block can be explicitly unlocked with the UNLK call.
The TLS block is also unlocked by the PEND RE/FI/SP/FC/RS/ER/FR and RSET calls. With PEND PA/PR/KP and PGWT KP/PR the lock remains in effect.
In the section "[Action with locked storage areas \(TLS, ULS and GSSB\)](#)", there is a description of how openUTM reacts when the desired TLS block is locked.
- The TLS block is transferred in its actual length, but no longer than the length specified in KCLA. If the contents of KCLA > 0 for the GTDA call, the actual length of the data in the TLS is returned in the KCRLM field.

7.11 INFO Request information

The different variants of the INFO (information) call enable you to obtain the following information:

- **INFO CD (Card)**, only on BS2000 systems
the information stored on the user's ID card (only if terminal users have to prove their authorization via card reader during sign on) or Kerberos information.
- **INFO DT (Date/Time)**
date and time of the start of the application and program unit
- **INFO SI (System Information)**
system information (e.g. the name of the application and the host)
- **INFO PC (Predecessor Conversation)**
information on a stacked service
- **INFO LO (LOcale Information)**
information on the language environment of the LTERM partner
- **INFO CK (CheckK)**
the KCRCCC return code, normally returned by an MPUT, FPUT or PEND call.

These variants of the INFO call differ in the meaning of the 2nd parameters (message area) to be specified in the INFO call.

openUTM provides language specific data structures to structure the message area: for COBOL in the COPY element KCINFC, for C/C++ in the *kcinf.h*. include file.

Setting the KDCS parameter area (1st parameter) and the 2nd parameter

The table below shows the five types of INFO call and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCSparameter area				Meaning of the 2nd parameter
	KCOP	KCOM	KCLA	KCLT	
BS2000 systems: Read ID card or Kerberos information	"INFO"	"CD"	Length	—	Area for ID card or Kerberos information
Obtain date and time of application and program starts	"INFO"	"DT"	30	—	Area for date and time, see data structure for INFO DT.
Information about language environment of LTERM partner	"INFO"	"LO"	68	LTERM name	Area for requested name, see data structure for INFO LO.
Information on a stacked service	"INFO"	"PC"	39	—	Area for requested names, see data structure for INFO PC.
Obtain system information	"INFO"	"SI"	180	—	Area for requested names, see data structure for INFO SI
Check UTM call	"INFO"	"CK"	—	—	Parameter area, to be checked

Due to the different meanings of the 2nd parameter, the INFO call is presented here in two formats:

Format 1: INFO CD/DT/LO/PC/SI (see next page).

Format 2: INFO CK (see "INFO CK call").

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"INFO"
KCOM	"CD"/"DT"/"LO"/"PC"/"SI"
KCLA	Length of message area in bytes
KCLT	Name of LTERM partner / —

KDCS call	
1st parameter	2nd parameter:
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_INFOCD/KDCS_INFODT/KDCS_INFOSI/KDCS_INFOPC	(nb,kcla)
KDCS_INFOLO	(nb,kcla,kclt)

openUTM return information	
Message area	Contents
	Data
Field name in the KB return area	
KCRLM	Actual block length
KCRCCC	Return code
KCRCDC	Internal return code

For the INFO call you make the following entries in the KDCS parameter area to read the ID card information, obtain date and time, obtain system information and obtain information on the predecessor or on the language environment of the LTERM partner:

KCOP

In the KCOP field, enter the INFO operation code

KCOM

In the KCOM field, enter the desired function of the call:

- CD to read ID card or Kerberos information (CARD), only on BS2000 systems
- DT to obtain time and date of the start of the application and program unit (DATE/TIME)
- LO to obtain information on the language environment of the LTERM partner
- PC to obtain information on the predecessor in the stack
- SI to obtain system information

KCLA

In the KCLA field, the length of the message area used in which openUTM is to store the information. You have to specify the length in bytes. openUTM transfers the information up to a maximum length of KCLA.

Only with INFO LO:

KCLT

in the KCLT field, enter the name of the LTERM partner whose language environment is to be obtained.

If KCLT is set to binary zero before the call, openUTM transfers the data of the LTERM partner via which the service is to be started.

Only on BS2000 systems:

If the LTERM partner belonging to the program unit run is specified in KCLT, openUTM transfers additional information about the associated physical terminal (PTERM).

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter:

The address of the message area into which openUTM is to write the information. openUTM transfers the requested information in a fixed structure. For this, language specific data structures are available: for COBOL in the KCINFC COPY element, for C/C++ in *kcinf.h*. include file.

Macro names

The use of C/C++ calls is described in detail in the [section "C/C++ macro interface"](#).

openUTM returns:

Message area

The desired data in the specified message area.

KCRLM

In the KCRLM field, the actual length of the data transferred.

With KCRCCC \geq 40Z the length is 0.

Only on BS2000 systems:

With INFO CD, **KCRLM** specifies the length of the Kerberos information transferred to the receiving area.

KCRCCC

In the KCRCCC field, the KDCS return code. 0

KCRCDC

In the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the INFO CD/DT/LO/PC/SI calls

The following codes can be analyzed in the program:

- 000 The requested information was transferred to the message area in its full length.
- 01Z Information was transferred. However, the message area is too short and the information was truncated.
- 09Z *only on BS2000 systems:*
for INFO CD: the Kerberos dialog returned an error or the Kerberos information was returned in truncated form because it was longer than the value generated with MAX PRINCIPAL-LTH.
KCRLM shows the length in which the Kerberos information was transferred to the receiving area.
- 40Z Generation error or system error. See KCRCDC.
- 41Z INFO call with KCOM = CD/PC not permitted in asynchronous program.
- 42Z KCOM invalid.
- 43Z KCLA invalid.
- 46Z Only with INFO LO:
the LTERM name specified in the KCLT field is invalid.
- 47Z Message area missing or cannot be accessed in the specified length
- 49Z Only with INFO LO:
unused parameters were not set to binary zero for the call.

An additional error code can be found in the dump:

- 71Z INIT not yet issued in this program unit

Features of the INFO CD call (BS2000 systems)

With this function the INFO call reads the ID card information stored during sign-on to the specified message area if the user used a magnetic strip card for authentication during sign on. For more information see also [section "Support for ID card readers on BS2000 systems"](#).

The stored Kerberos information (= Kerberos Principal name) can be read if either the user was signed on by means of Kerberos, or a Kerberos dialog has been executed for the client and afterwards no further user signed on using a magnetic strip card.

The INFO CD call for reading ID card information or Kerberos information is permitted in dialog programs only.

In order to be able to call the ID card information in the program, you have to set the following operands during generation:

- the CARD= operand must be specified for the current user ID in the KDCDEF control statement USER, and
- the CARDLTH= operand in the KDCDEF control statement MAX.

i openUTM sets the identifier "A" in the KCAUSWEIS/kccard field of the KB header if the card was inserted during the preceding input.

Features of the INFO DT call

With this function the INFO call writes the start times of the application and program unit to the specified area, using a length of 30 bytes. The information is structured as follows:

Field name COBOL	Field name C/C++	Byte	Meaning of the information
KCDATAS	—	1 - 6	Date of application startup in the form <i>ddmmyy</i> , where:
KCTAGAS	as_day	1 - 2	<i>dd</i> - day (value range 01 - 31)
KCMONAS	as_mon	3 - 4	<i>mm</i> - month (value range 01 - 12)
KCJHRAS	as_year	5 - 6	<i>yy</i> - year (value range 00 - 99)
KCTJHAS	as_doy	7 - 9	Day of application startup (working day, value range 001 - 366)
KCUHRAS	—	10 - 15	Time of application startup in the form <i>hhmmss</i> , where:
KCSTDAS	as_hour	10 - 11	<i>hh</i> - hour (value range 00 - 23)
KCMINAS	as_min	12 - 13	<i>mm</i> - minute (value range 00 - 59)
KCSEKAS	as_sec	14 - 15	<i>ss</i> - second (value range 00 - 59)
KCDATAK	—	16 - 21	Date of program unit startup in the form <i>ddmmyy</i> , where:
KCTAGAK	ps_day	16 - 17	<i>dd</i> - day (value range 01 - 31)
KCMONAK	ps_mon	18 - 19	<i>mm</i> - month (value range 01 - 12)
KCJHRAK	ps_year	20 - 21	<i>yy</i> - year (value range 00 - 99)
KCTJHAK	ps_doy	22 - 24	Day of application startup (working day, value range 001 - 366)
KCUHRAK	—	25 - 30	Time of program unit start in the form <i>hhmmss</i> , where:
KCSTDAK	ps_hour	25 - 26	<i>hh</i> - hour (value range 00 - 23)
KCMINAK	ps_min	27 - 28	<i>mm</i> - minute (value range 00 - 59)
KCSEKAK	ps_sec	29 - 30	<i>ss</i> - second (value range 00 - 59)

Features of the INFO LO call (BS2000 systems)

Using the INFO LO variant of the INFO call the program unit run can request information about the location of LTERM partners and application. The location of an LTERM partner determines the language environment of the client. The location of the application determines the default setting for the language environment.

The call returns the following data:

- the location of the LTERM partner whose name is specified in the KCLT field

- the location of the application

If KCLT is set to binary zero before the call, openUTM transfers the data of the LTERM partner via which the service was started.

If the call is executed in a dialog service and the name of the LTERM partner is set in the KCLT field associated with the program unit run, openUTM also provides the following data about the associated physical terminal (PTERM):

- number of extended ISO character sets supported by the terminal or printer
- ISO variant numbers of all supported character sets
- default user character set, allocated to the BS2000 user ID under which the UTM application is running.

With the INFO LO call openUTM displays the data in the message area structured as follows:

Field name	Byte	Meaning of contents
KCLTLANG	1 - 2	Language identifier of LTERM partner
KCLTTERR	3 - 4	Territory identifier of LTERM-partner
KCLTCCSN	5 - 12	CCS-name of LTERM-partner
	13 - 20	Blanks
KCAPLANG	21 - 22	Language identifier of application
KCAPTERR	23 - 24	Territory identifier of application
KCAPCCSN	25 - 32	CCS-name of application
	33 - 40	Blanks
KCDEFCCS	41 - 48	User default character set of BS2000 user ID under which the UTM application runs
Information about the connected terminal (only out put in dialog services if KCLT contains the name of the LTERM partner associated with the service. If the partner is not a terminal the values is X"00").		
KCCCSNO	49	Number of the extended ISO-character sets supported by the terminal
KCHSET1	50	Variant number of the first supported ISO character set
KCHSET2, KCHSET3 ... to KCHSET16	51 - 65	Variant numbers of other ISO character sets supported by the physical terminal. Length of each field is 1 byte.
	65 - 68	Blanks

Features of the INFO LO call (Unix, Linux and Windows systems)

With the INFO LO variant of the INFO call, the program unit run can request information about the language currently set for the LTERM partner.

This function enables you to run program units in multiple languages. In the program unit run, the language set for an LTERM partner can be queried with INFO LO and messages sent in the same language.

INFO LO returns the following information:

- Language and territory identifiers as well as the \$LANG variable of the LTERM partner specified in KCLT. The cell outputs the currently set \$LANG variable of the user ID under which the associated dialog terminal process was started.
- Language and territory identifiers as well as the \$LANG variable of the UTM application. The cell outputs the currently set \$LANG variable of the user ID under which the associated application was started.

Language and territory identifiers are retrieved from the \$LANG variable at program runtime. Example: From \$LANG=En_US.ASCII, openUTM creates the language identifier En and the territory identifier US.

The INFO LO call provides data structured as follows:

Field name	Byte	Meaning of the contents
KCLTLANG	1 - 2	Language identifier of the LTERM partner
KCLTTERR	3 - 4	Territory identifier of the LTERM partner
KCLTNLSL	5 - 20	\$LANG variable of the specified LTERM partner
KCAPLANG	21 - 22	Language identifier of the application
KCAPTERR	23 - 24	Territory identifier of the application
KCAPNLSL	25 - 40	\$LANG variable of the application
	41 - 68	Blanks

Features of the INFO PC call

With this call you can query information about a stacked service.

If the current service was started by service stacking, the INFO PC call provides, for example, the following information about the preceding service (that is the service that is immediately before the current service in the stack):

- date and time of last processing
- format identifier of last screen output
- the next TAC
- the service TAC

openUTM writes this information to the specified area, using a total length of 39 bytes.

Field name	Byte	Meaning of the information
KCPFN	1 - 8	Format identifier of the last screen output
KCPNXTAC	9 - 16	Name of the next TAC
KPCCVTAC	17 - 24	Name of the service TAC
KCPLDATE ¹	25 - 33	Date of last processing in the form ddmmyy, where:
KCPLDAY	25 - 26	dd - day (value range 01 - 31)
KCPLMON	27 - 28	mm - month (value range 01 - 12)
KCPLYEAR	29 - 30	yy - year (value range 00 - 99)
KCPLDOY	31 - 33	Working day of last processing, value range 001 - 366
KCPLTIME1	34 - 39	Time of last processing in the form hhmmss, where:
KCPLHOUR	34 - 35	hh - hour (value range 00 - 23)
KCPLMIN	36 - 37	mm - minute (value range 00 - 59)
KCPLSEC	38 - 39	ss - second (value range 00 - 59)

¹For C/C++ the summary fields KCPLDATE and KCPLTIME are not defined. However, the specific fields for day/month/year/working day/hour/minute/second are defined.

If there is no stacking, openUTM returns blanks.

Features of INFO SI call

With this call, you can query information on the application and system, e.g. the name of the application and the host on which the application is running.

In dialog services INFO SI also provides the PTERM name, host name and application name of the communication partner.

openUTM writes this information to the specified area as follows - byte 17 - 40 are set to binary zero in asynchronous services.

Field name	Byte	Meaning of the information
KCAPPLNM /applnam	1 - 8	Name of the UTM application
KCHOSTNM /hostname	9 - 16	<i>BS2000 systems:</i>
		<ul style="list-style-type: none"> Name of the host where the application is running.
KCPTRMNM	17 - 24	<i>Unix, Linux and Windows systems:</i>
		<ul style="list-style-type: none"> Standalone applications: Name of the host generated with MAX HOSTNAME. UTM cluster applications: Name of the host generated with CLUSTER-NODE VIRTUAL-HOST
KCPTRMNM	17 - 24	In a dialog service
		<ul style="list-style-type: none"> For distributed processing via LU6.1: CON name of the communication partner For distributed processing via OSI TP: OSI-CON name of the communication partner Otherwise the PTERM name of the communication partner
KCPTRMNM	17 - 24	In an asynchronous service: Blanks
KCPRONM	25 - 32	In a dialog service
		<ul style="list-style-type: none"> OSI TP job-receiving service: Blanks otherwise: Host name of the communication partner
KCPRONM	25 - 32	In an asynchronous service: Blanks
KCBCAPNM	33 - 40	In a dialog service
		<ul style="list-style-type: none"> OSI TP job-receiving service: ACCESS-POINT name via which the association with the partner is established otherwise: BCAMAPPL name via which the connection to the partner is established
KCBCAPNM	33 - 40	In an asynchronous service: Blanks
KCVERS	41 - 46	openUTM version <i>Vnn.nx</i> (e.g. V07.0A)

Field name	Byte	Meaning of the information
KCIVER	47 - 48	Version number of the KDCS interface ¹
KCIVAR	49	"B" for BS2000 systems, "X" for Unix and Linux system or "N" for Windows system
KCFILL1	50	Not currently used
KCLANG	51 - 52	<p><i>Only on Unix, Linux and Windows systems:</i></p> <ul style="list-style-type: none"> Language identifier, e.g: "EN" for English (The value of this language identifiers corresponds to the value of the first two bytes of the \$LANG variable)
KCHSTNML	53 - 116	<p><i>BS2000 systems:</i></p> <ul style="list-style-type: none"> Long name of the host where the application is running.
		<p><i>Unix, Linux and Windows systems:</i></p> <ul style="list-style-type: none"> Standalone applications: Long name of the host generated with MAX HOSTNAME. UTM cluster applications: Long name of the host generated with CLUSTER-NODE VIRTUAL-HOST
KCPRONML	117 - 180	<p>In a dialog service</p> <ul style="list-style-type: none"> OSI TP job-receiving service: Blanks otherwise: Long host name of the communication partner <p>In an asynchronous service: Blanks</p>

¹ The version number indicates the version of function extensions available, irrespective of the product variant. In this way, UTM application programs can be created to run in different product variants and openUTM versions. As the functionality of the KDCS interface is extended, the version number is increased. For openUTM V7.0 it is 9. The version number of the KDCS interface is not incremented if the extended functionality of the KDCS interface affects data structures of KDCS calls that have a separate version number.

7.11.1 INFO CK call

With this function the INFO call checks whether the specifications for an MPUT, FPUT or PEND call in KCRN are permitted. openUTM transfers the KDCS return code expected for the checked call to KCRINFCC. INFO CK checks the following calls:

- MPUT NT/NE
- FPUT NT/NE
- PEND PA/PR/KP/SP/RE/FC.

This function enables you, for example, to check prior to a PEND RE call whether the intended follow-up TAC is permitted for this call. This may, for example, prevent the service from aborting.

Setting the parameters	
Field name in KDCS parameter area	Contents
KCOP	"INFO"
KCOM	"CK"
Message area	
	KDCS parameter area of the call to be checked

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameter
KDCS_INFOCK	(nb)

openUTM return information	
Field name in the KB return area	Contents
KCRINFCC	KCRCCC return code of the checked call
KCRCCC	Return code
KCRCDC	Internal return code

For the INFO call you make the following entries in the KDCS parameter area to check the KDCS parameter area for a UTM call:

KCOP

In the KCOP field, enter the INFO operation code.

KCOM

In the KCOM field, enter the desired function of the call: CK to check the KDCS parameter area for an MPUT-, FPUT-, or PEND call.

Message area

You also have to specify the KDCS parameter area to be checked according to the rules valid for the respective call (MPUT, FPUT, PEND).

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the area containing the KDCS parameter area of the call to be checked.

Macro names

The use of C/C++ macro calls is described in detail in the section "[C/C++ macrointerface](#)".

openUTM returns:

KCRINFCC

in the KCRINFCC field, the return code expected in KCRCCC of the checked call. openUTM enters this error code only if the INFO call runs according to plan (the return code for the INFO call has the value 000). KCRINFCC has the value 78Z if the specified function form of the call to be checked (KCOP and KCOM entries in the second parameter area) is not supported by the INFO call.

KCRCCC

in the KCRCCC field, the KDCS return code.

KCRCDC

in the KCRCDC field, the internal return code of the checked call (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the INFO CK call

The following codes can be analyzed in the program:

- 000 The call specified in the 2nd parameter was checked.
- 40Z Generation error or system error (see KCRCDC).
- 42Z KCOM of the INFO call invalid.

47Z Address of 2nd parameter omitted or invalid.

An additional error code can be found in the dump:

71Z INIT not yet issued in this program unit.

Features of the call INFO CK

If KCCARD was specified, the INFO CK call in MPUT checks whether the terminal for which the message is destined was generated with an ID card reader or whether the USER is already signed on with an ID card.

On BS2000 systems, this check is also performed if a corresponding edit profile was specified.

7.12 INIT Initialize program unit

The INIT (initialize program) call is used to sign-on a program unit to openUTM. There are the following variants.

- INIT (no entry in KCOM)
Initialize program unit
- INIT PU (**P**rogram **U**nit)
Initialize program unit and request additional information.
- INIT MD (**M**odify)
Initialize program unit and modify the size of the KB program area.

The following applies for these variants.

- The INIT call initiates cooperation between the program unit run and openUTM. It is the first KDCS call allowed in a program unit run, i.e. you are not allowed to enter any other KDCS or database calls prior to the INIT call.
- You are not allowed to enter INIT or INIT PU more than once in a program unit run.
- INIT MD may be specified more than once in a program unit. If you specify the INIT MD call as the first INIT call in the program unit, it is treated like an INIT without an operation modifier.
- You may not use the communication area (KB) and the standard primary working area (SPAB) between start of the program unit run and the first INIT call.
- Following the first INIT, openUTM makes the entire communication area (KB), including the KB parameter area, available to the program unit run. This area has the length specified in KCLKBPRG/kclcapa.
- The INIT MD call enables the length of the KB program area to be adjusted during the program unit run. This may be necessary if, for example, the size of the KB program area that openUTM is to save with the PEND call is not determined until processing has started.
Example: Data that is read from a database is to be saved in the KB program area. If the length of the KB program area is adjusted to the volume of data read by INIT MD, openUTM need not save more data than necessary or less data than necessary at the synchronization point.
- If you use the INIT call with the operation modifier PU (**P**rogram **U**nit), openUTM provides the program unit additional information about application, system and communication partner in the message area.

Setting the 1st parameter (KDCS parameter area)

The following table shows the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area				
	KCOP	KCOM	KCLKBPRG /kclcapa	KCLPAB /kclspa	KCLI
Initialize program unit	"INIT"	—	Length of KB program area	Length of SPAB	—
Initialize program unit and request information	"INIT"	"PU"	Length of KB program area	Length of SPAB	Length of message area
Modify length of KB program area	"INIT"	"MD"	Length of KB program area	—	—

The specified length of the KB program area must not be greater than the maximum length defined for this application at generation (operand KB in the MAX statement for KDCDEF).

The specified length of the SPAB must not be longer than the value defined at generation (operand SPAB in the MAX statement for KDCDEF).

Setting the 2nd parameter (only necessary with INIT PU)

Here you enter the address of the message area to which openUTM is to write the requested information.

You can use language-specific data structures to structure the message area. For COBOL, they are defined in the KCINIC COPY element and for C/C++ in the *kcini.h* include file.

Specify the version number of the structure and select the return information requested from openUTM in the header of the data structure. These other fields (return information) are described in section "[Structure of the message area with INIT PU](#)".

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"INIT"
KCOM	—/ "PU"/"MD"
KCLKBPRG/kclcapa	Length in bytes
KCLPAB/kclspa	Length in bytes
KCLI	Length in bytes (with INIT PU)

Setting the header in the message area (only necessary with INIT PU)	
Field name in message area	Contents
KCVER/if_ver	Version number (7)
KCDATE/dattim_info	Request date and time (Y/N)
KCAPPL/appl_info	Request application information (Y/N)
KCLOCALE/locale_info	Request Locale information (Y/N)
KCOSITP/ositp_info	Request OSI TP information (Y/N)
KCENCR/encr_info	Request encryption information (Y/N)
KCMISC/misc_info	Request miscellaneous information (Y/N)
KCHTTP/http_info	Request HTTP information (Y/N)

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	— / Message area (with INIT PU)

C/C++ macro calls	
Macro names	Parameters
KDCS_INIT	(kclcapa,kclspa)
KDCS_INITPU	(nb,kclcapa,kclspa,kcli)
KDCS_INITMD	(kclcapa)

openUTM return information	
Message area (only with INIT PU)	Contents
	INIT PU information
KB header area	
	Current service data
Field name in KB return area	
KCRMLM (only with INFO PU)	Length of transferred data
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcrfn	Format identifier/blanks
KCRPI	Service ID/Rollback ID/blanks
KB program area	
KCKBPRG/kclcapa	Data

For the INIT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the INIT operation code.

KCOM

In the KCOM field, the operation modifier:

- PU if openUTM is to make additional information available in the message area

-
- MD if the length of the KB program area is to be changed

KCLKBPRG/kclcapa

In the KCLKBPRG/kclcapa field, enter the length of the KB program area in bytes. It must not exceed the length predefined at generation time (operand KB in the MAX statement), otherwise the generated value is taken.

Only with INIT or INIT PU:

KCLPAB/kclspa

In the KCLPAB/kclspa field, enter the length of the standard primary working area (SPAB) used in the program unit run in bytes. It must not exceed the length predefined at generation time (operand SPAB in the MAX statement).

Only with INIT PU:

KCLI

in the KCLI field, enter the length of the message area to which openUTM is to transfer the information. Enter the length in bytes. The information transferred to the message area by openUTM has a maximum length of KCLI. To obtain all available information, you must specify the value 372 in the current interface version.

Setting the header of the message area (only necessary with INIT PU):

KCVER/if_ver

In the KCVER/if_ver field, enter the version number of the data structure. The current version is version 7.

KCDATE/dattim_info

Enter Y in the KCDATE/dattim_info field if you want information on the date and time of the start of the application and the program unit run, otherwise enter N.

KCAPPL/appl_info

Enter Y in the KCAPPL/appl_info field if you want to request information about the application, system and communication partner, otherwise enter N.

KCLOCALE/locale_info

Enter Y in the KCLOCALE/locale_info field if you to want to request information about the language environment of the user ID, otherwise enter N.

KCOSITP/ositp_info

Enter Y in the KCOSITP/ositp_info field if you require OSI TP specific information, otherwise enter N.

KCENCR/encr_info

Enter Y in the KCENCR/encr_info field if you require information on the encryption methods used to encode between the client and the UTM application, otherwise enter N. (The encryption mechanism can be coordinated. See the openUTM manual "Generating Applications".)

KCMISC/misc_info

Enter Y in the KCMISC/misc_info field if you require miscellaneous information (e.g. number of queued messages in the user's queue, password validity, time of last signon), otherwise enter N.

KCHTTP/http_info

Enter Y in the **KCHTTP/http_info** field if you require HTTP specific information, otherwise enter N.

You specify the following for the KDCS call:

1st parameter

the address of the KDCS parameter area.

2nd parameter

(only necessary with INIT PU): the address of the message area to which openUTM is to write information (see ["Setting the 2nd parameter"](#)).

Macro names

The use of C/C++ macro calls is described in detail in the section ["C/C++ macro interface"](#).

openUTM returns:

Message area

only with INIT PU:

in the message area, the information transferred by openUTM up to a maximum length of the value specified in KCLI.

KB header area

in the KB header area the current data of the KB header (see table).

KCRLM

only with INIT PU: in the KCRLM field, the actual length of the information available in UTM. If a lower value has been entered in the KCLI field, the information is returned at the length specified in KCLI and KCRCCC is set to 07Z.

If KCRCCC >= 40Z, no information is transferred. Thus, in such cases KCRLM=0.

KCRCCC

in the KCRCCC field, the KDCS return code, see below

KCRCDC

in the KRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KCRMF/kcrfn

Only with INIT or INIT PU:

- For a message from a terminal:

Blanks (in line mode) or the format name (in format mode) of the last screen output, i.e. the name specified in the KCMF/kcfn field with the MPUT of the last dialog step. If the last output consisted of multiple partial formats, KCRMF/kcrfn contains the name of the first partial format into which data was entered. If no data was entered in any of the partial formats, KCRMF/kcrfn contains the name of the first partial format.

Only on BS2000 systems: If an edit profile was used in the last screen output, KCRMF/kcrfn contains this edit profile.

- for a message from a TS application or a program unit of the same application: blanks.
- if a rollback message exists (after PEND RS): blanks.
- for a message from the LU6.1 partner or UPIC client:
The format identifier of the first message segment specified by the LU6.1 partner or UPIC client on sending.

Particularity in the job-submitting service:

Blanks if a status flag exists for the service ID specified in KCRPI.

- for distributed processing via OSI TP:
If the program unit run was started because of a distributed dialog, KCRMF/kcrfn in the job-submitting service contains the name of the abstract syntax which was allocated to the message by the job submitter; if the field contains blanks, the abstract syntax of the UTD syntax is selected.
In the job-receiving service KCRMF/kcrfn contains the name of the abstract syntax which was allocated to the message by the job-receiving service described in KCRPI. If the field contains blanks, the abstract syntax of the UTD syntax is selected or an error message from the partner is present.

KCRPI

Only with INIT or INIT PU:

- For a message from a UPIC client program, terminal, a TS application or a program unit in the same application: blanks.
- If a rollback message exists: the rollback ID.
- In the job-submitting service with distributed processing:
the service ID of the job-receiving service if a message from the job receiver exists.
- In the job-receiving service with distributed processing: blanks

KCKBPRG/kclcapa

In the KCKBPRG/kclcapa (KB program area) field, the data of the service, provided the program unit run includes service-specific data from another program. If this is the first program unit run of a service, the area is undefined or set with the generated fill character. If length zero is specified in KCLKBPRG/kclcapa of the preceding program unit, no data is transferred to the follow-up program unit run.

KDCS return codes in the KCRCCC field for the INIT call

The following codes can be analyzed in the program:

- 000 Operation carried out.
For INIT PU: the requested information was transferred to the message area in full length.
- 01Z Length specified in KCLKBPRG/kclcapa exceeds value specified when the application was generated.
- 02Z For INIT or INIT PU: Length specified in KCLPAB/kclspa exceeds value specified when the application was generated.
- 07Z For INIT PU: Function was executed, the available message area is too short (length in KCLI insufficient).
No or incomplete information was returned.
- 48Z For INIT PU: Invalid data structure version.

Additional error codes can be found in the dump:

71Z For INIT or INIT PU: INIT call already issued in this program unit run.

73Z Negative length specification. With INIT PU: KCLI is invalid.

77Z Message area is missing or cannot be accessed in the specified length.

88Z Interface version is invalid.

89Z For INIT PUT or INIT MD: When the function was called, unused parameters were not set to binary zero.

openUTM return information in the header of the KDCS communication area

openUTM returns the following entries among others to the INIT call: the TAC of the service start, current TAC, date, time and the LTERM partner of the sender .

The generated length of the KB program area is located in the KCLKBPB/kclpa field. The table below shows which entries openUTM returns in the KB header:

Field name COBOL	Field name C/C++	Contents (entered by openUTM)
KCBENID	kcuserid	UTM user ID under which the service was initiated. When working without user IDs: KCBENID/kcuserid=KCLOGTER. With distributed processing via LU6.1:local session name (LSES). With distributed processing via OSI TP and Security type "N": Local name of the connection (OSI-TP association), otherwise user ID
Service-specific data:		
KCTACVG	kccv_tac	TAC used to start this service
KCTAGVG	kccv_day	Day of service start
KCMONVG	kccv_month	Month of service start
KCJHRVG	kccv_year	Year of service start
KCTJHVG	kccv_doy	Working day of service start
KCSTDVG	kccv_hour	Hour of service start
KCMINVG	kccv_minute	Minute of service start
KCSEKVG	kccv_second	Second of service start

Field name COBOL	Field name C/C++	Contents (entered by openUTM)
KCKNZVG	kccv_status	<p>Service ID</p> <ul style="list-style-type: none"> • F: First program unit run of dialog service • A: First program unit run of an synchronous service • N: Follow-up program unit run of service • C: First program unit of a chained service • R: Restart of a service • D: End of service through loss of connection (only with LTERM partners which have been generated with RESTART=NO) • Z: End of service by abort • E: Normal end of service • L: End of last process with normal termination <p>The service identifiers D, Z, E can only occur in the VORGANG exit, the service identifier L only in the SHUT exit. All other service identifiers can occur either in the KDCS call INIT or in the exit VORGANG.</p>
Program unit-specific data:		
KCTACAL	kcpr_tac	TAC used to address the program
KCSTDAL	kcpr_hour	Hour of program unit start
KCMINAL	kcpr_minute	Minute of program unit start
KCSEKAL	kcpr_second	Second of program unit start
KCAUSWEIS	kccard	ID card identifier: A (card inserted) or blanks.
KCTAIND	kctaind	Transaction indicator: F (first) or N (next transaction)
KCLOGTER	kclogter	LTERM name; for distributed processing: (OSI-)LPAP name
KCTERMN	kctermn	Communication partner identifier, for distributed processing via LU6.1: CON...,TERMN=, for distributed processing via OSI TP: OSI-LPAP...,TERMN= otherwise: PTERM ..., TERMN (see also the table by PTERM in the openUTM manual "Generating Applications")
KCLKBPB	kclpa	Maximum length of the KB program area as defined at generation time

Field name COBOL	Field name C/C++	Contents (entered by openUTM)
Data for service stack:		
KCHSTA	kchsta	Stack height, i.e. the number of stacked services as seen from the current service (0 through 15).
KCDSTA	kcdsta	Change of stack height: + (increased), - (decreased) or 0 (unchanged, also in the event of stacking after returning from an inserted service)
KCPRIND	kcprind	Program indicator: A =asynchronous service, D = dialog service
KCOF1	kcof1	OSI TP functions in an OSI TP job-receiving service.
KCCP	kccp	Indicator for the client protocol: <ul style="list-style-type: none"> • 0: Asynchronous processing • 1: LU6.1 • 2: OSI TP • 3: UPIC • 4: DTP (Unix, Linux and Windows systems) • 4: TIAM (BS2000 systems) • 5: APPLI • 6: SOCKET (USP) • 7: HTTP • 8: USP-SECURE • 9: HTTPS
KCTARB	kctarb	Information on rollback of an OSI TP transaction
KCYEARVG	kccv_year4	Year of service start (four positions)

Features of the KB program area and the SPAB

- The KB program area is assigned to a service, the SPAB to a program unit run.
- At the start of the service the contents of the KB program area and the SPAB are undefined or the areas are preset with the generated fill character.
Such a fill character can be used, for example, to facilitate error location in the test or for data protection. The SPAB and KB program area are preset with this character at the start of a process and overwritten with it at the end of a processing step, see openUTM manual “Generating Applications”.
- If, at the INIT of a program unit, a KB program area is defined with a length of n bytes and a larger KB program area of m bytes ($m > n$) is requested in the next program unit run, the last ($m - n$) bytes of the KB program area are likewise undefined or padded with the generated fill character.

Particularities of the INIT calls with distributed processing

- INIT call in the job-submitting service

If the distributed transaction is rolled back, openUTM returns the service indicator "R" at INIT of the first transaction of a follow-up transaction (in the KCKNZVG/kccv_status field of the KB header). In this case it is usually status information of the job-receiving service.

In the follow-up program unit the INIT call in the job-submitting service supplies the following additional information in the KDCS return area:

- KCRPI contains the service identifier of the job-receiving service which started this program unit.
- KCRMF/kcrfn contains the format identifier which the job-receiving service entered in the first message segment to the job-submitting service, otherwise blanks.

The first MGET call for reading the results must be issued with KCRN=KCRPI and KCMF=KCRMF (or: kcfn=kcrfn).

- INIT call in the job-receiving service

There are the following modifications for entries in the KB header:

KCBENID/kcuserid

With LU6 protocol: contains the local session name (LSES name, see the LSES statement for KDCDEF)

With OSI TP protocol with security type "N": local association name (see ASSOCIATION-NAMES operand in the KDCDEF statement OSI-LPAP), otherwise user ID

KCAUSWEIS/kccard

Contains blanks, i.e. ID card reader is not supported.

KCLOGTER

Contains the logical name of the partner application (LPAP name or (MASTER-)OSI-LPAP name, see LPAP statement for LU6.1 protocol, or OSI-LPAP statement for OSI TP protocol: for KDCDEF).

KCTERMN

Contains the identifier (**T**erminal **M**nemonic) of the partner application, (see operand TERMN= of the CON statement for LU6.1 protocol, or the OSI-LPAP statement for OSI TP protocol: for KDCDEF).

KCOF1

shows the OSI TP functions in an OSI TP job-receiving service for the dialog used to select the job submitter. The following values are possible:

Blanks The current service is not a job-receiving service or the OSI TP protocol is not used for communication with the job-submitting service.

B Basic functions

H Basis and handshake functions

C Basic and commit functions with chained transactions

O (other combination)

No standard combination of OSI TP functions was selected for the dialog with the job submitter. The selected OSI TP functions can only be read with an INIT PU call.

KCCP (client protocol)

shows the protocol used for the communication:

- 1 LU.1
- 2 OSI TP

KCTARB

shows in an OSI TP service whether a situation occurred in a previous PGWT call which requires the rollback of a transaction:

- Blanks a situation has occurred which requires the rollback of the transaction.
- Y a situation has occurred in a previous PGWT call which does not permit the commit of the transaction and the transaction has not been rolled back yet. Communication with the partner services is permitted. A call to commit the transaction results in an abnormal end of service.

The KCRMF/kcrfn field in the KB return area provides information about the partner service.

Message area returns with INIT PU

If you use the INIT call with the operation modifier PU, openUTM supplies additional information for the program unit in the message area about application, system and communication partner.

You can use language specific data structures to structure the message area. For COBOL, they are defined in the KCINIC COPY element and for C/C++ in the *kcini.h* include file. In the header of the data structure you have to define which information openUTM is to return.

openUTM supplies the following information:

- The generated lengths for the KB program area and the standard primary working area. Any variant of the INIT PU call supplies this information.
- Date and time of the application starts and the start of the program unit run.
- Information about application and system
- Information about the communication partner:
In a dialog service, this are information about:
 - name of the communication partner
 - host name of the communication partner
 - name of the UTM application via which communication with the communication partner was established (BCAMAPPL name)

In an asynchronous service blanks are transferred.

-
- Information about the language environment of the user ID who started the service.

Unix, Linux and Windows systems

This information comprises language and territory identifier as well as \$LANG variable. Language and territory identifier are retrieved from the \$LANG variable during the runtime of the program. Example: From \$LANG=En_US.ASCII openUTM creates the language identifier En and the territory identifier US.

In an asynchronous service, the language of the user who started the service is transferred.

BS2000 systems

This information comprises:

- Language and territory identifier and the character set of the user. If no user is signed on, openUTM transfers the language and territory identifier and the character set of the LTERM partner.
- Name of the character set of the message.
- Information whether the user is connected to a 7- or 8-bit terminal.

In a locally started asynchronous service, the locale of the user who started the service is transferred. In such an asynchronous service, the 8-bit terminal information contains the value "7" and the character set name of the message contains blanks.

- Information about the job-submitting service when communication is carried out via OSI TP.
- Information about the encryption method used between the UTM application and the client.
- Miscellaneous information, e.g. the number of queued messages in the user's queue, password validity, time the user last signed on, properties of the LTERM and OSI-LPAP partner which started the service with respect to LTERM groups and LTERM/LPAP bundles.
- Information about asynchronous messages for the user.

Structure of the message area with INIT PU (with KCINIC or kcini.h)

Field name COBOL	Field name C/C++	Length in bytes	Description
Header: Version number and requested information			
KCVER	if_ver	2	To be assigned before the call: Version number of the data structure (7)
KCDATE	dattim_info	1	To be assigned before the call: Request date and time (Y/N)
KCAPPL	appl_info	1	To be assigned before the call: Request application information (Y/N)
KCLOCALE	locale_info	1	To be assigned before the call: Request location information (Y/N)
KCOSITP	ositp_info	1	To be assigned before the call: Request OSI TP information (Y/N)
KCENCR	encr_info	1	To be assigned before the call: Request encryption information (Y/N)
KCMISC	misc_info	1	To be assigned before the call: Request miscellaneous information (Y/N)
KCHTTP	http_info	1	To be assigned before the call: Request HTTP information (Y/N)
		7	Reserved for future extensions
General information, which is always returned			
KCGPAB	gen_spab_lth	2	Generated length of SPAB
KCGNB	gen_nb_lth	2	Generated length of message area
Information about date and time of the start of the application and the program unit. (only if KCDATE/dattim_info=Y)			
KCADAY	as_dt_day	2	Day of application start
KCAMONTH	as_dt_month	2	Month of application start
KCAYEAR	as_dt_year	4	Year of application start
KCADOY	as_dt_doy	3	Day of year of application start
KCAHOUR	as_tm_hour	2	Hour of application start

Field name COBOL	Field name C/C++	Length in bytes	Description
Information about date and time of the start of the application and the program unit. (only if KCDATE/dattim_info=Y)			
KCAMIN	as_tm_minute	2	Minute of application start
KCASEC	as_tm_second	2	Second of application start
KCASEAS	as_season	1	Time of application start is specified in normal time (W) or summer time (S). If the operating system does not supply information about summer/normal time, blanks are output.
KCPDAY	ps_dt_day	2	Day of program start
KCPMONTH	ps_dt_month	2	Month of program start
KCPYEAR	ps_dt_year	4	Year of program start
KCPDOY	ps_dt_doy	3	Day of the year of program start
KCPHOUR	ps_tm_hour	2	Hour of program start
KCPMIN	ps_tm_minute	2	Minute of program start
KCPSEC	ps_tm_second	2	Second of program start
KCPSEAS	ps_season	1	Time of application start is specified in normal time (W) or summer time (S). If the operating system does not supply information about summer/normal time, blanks are output.
KCTMZONE	time_zone	12	<p><i>Unix, Linux and Windows systems:</i> Blanks</p> <p><i>BS2000 systems:</i> Time zone in format <i>sHH:MM-hh:mm</i>, where:</p> <p>s "+" or "-": sign of time difference between local time zone and UTC (Universal Time Coordinate, equivalent to Greenwich mean time).</p> <p>HH:MM Time difference between local time and UTC in hours (HH) and minutes (MM).</p> <p>hh:mm Time shift in hours (hh) and minutes (mm) between summer time and normal time in local time zone.</p>

Field name COBOL	Field name C/C++	Length in bytes	Description
Information about application, system and communication partner (only if KCAPPL/appl_info=Y)			
KCAPPLNM	applnm	8	UTM application name
KCHOSTNM	hostm	8	<i>BS2000 systems:</i>
			<ul style="list-style-type: none"> Name of host, where the application is running
KCPTRNM	ptrnm	8	<i>Unix, Linux and Windows systems:</i>
			<ul style="list-style-type: none"> Standalone applications: Name of the host generated with MAX HOSTNAME. UTM cluster applications: Name of the host generated with CLUSTER-NODE VIRTUAL-HOST
KCPTRNM	ptrnm	8	<p>In a dialog service:</p> <ul style="list-style-type: none"> with distributed processing via LU6.1: CON name of the communication partner; with distributed processing via OSI TP: OSI-CON name of the communication partner; otherwise: PTERM name of the communication partner. <p>In an asynchronous service: blanks</p>
KCPRONM	pronm	8	<p>In a dialog service:</p> <ul style="list-style-type: none"> in the OSI TP job receiving service: blanks; otherwise: host name of the communication partner; <p>In an asynchronous service: blanks</p>
KCBCAPNM	bcapnm	8	<p>In a dialog service:</p> <ul style="list-style-type: none"> in the OSI TP job receiving service: ACCESS-POINT name via which the association with the partner is established. otherwise: BCAMAPPL name via which the connection to the partner is established <p>In an asynchronous service: blanks</p>
KCVERS	version	6	openUTM version in form <i>Vnn.nx</i> (e.g. V07.0A)

Field name COBOL	Field name C/C++	Length in bytes	Description
Information about application, system and communication partner (only if KCAPPL/appl_info=Y)			
KCIVER	iversion	2	Version number of KDCS interface, indicates the state of the available function upgrades of the KDCS interface; in openUTM V07.0A it has the value 9
KCIVAR	ivariant	1	Identifier of product variant of openUTM: 'B' for BS2000 systems or 'X' for Unix and Linux systems or 'N' for Windows systems
KCHSTNML	hostnm_long	64	<i>BS2000 systems:</i>
			<ul style="list-style-type: none"> • Long name of the host on which the application is running.
KCHSTNML	hostnm_long	64	<i>Unix, Linux and Windows systems:</i>
			<ul style="list-style-type: none"> • Standalone applications: Long name of the host generated with MAX HOSTNAME. • UTM cluster applications: Long name of the host generated with CLUSTER-NODE VIRTUAL-HOST
KCPRONML	pronm_long	64	In a dialog service <ul style="list-style-type: none"> • OSI TP job-receiving service: Blanks • otherwise: Long host name of the communication partner In an asynchronous service: Blanks
Information about the location of the user ID which started the service (only if KCLOCALE/locale_info=Y)			
KCUSLANG	us_lang_id	2	Language identifier of the user; if no user is signed on yet: language identifier of the LTERM partner
KCUSTERR	us_terr_id	2	Territory identifier of the user; if no user is signed on yet: territory identifier of the LTERM partner
<i>Only on Unix, Linux and Windows systems:</i>			
KCUSNLSL	us_nlslang	16	\$LANG variable of the user
		10	Blanks

Field name COBOL	Field name C/C++	Length in bytes	Description
Information about the location of the user ID which started the service (only if KCLOCALE/locale_info=Y)			
<i>Only on BS2000 systems:</i>			
KCUSCCSN	us_ccsname	8	Character set of the user; if no user is signed on yet:character set of the LTERM partner
		8	Blanks
KCCSCURR	curr_ccs	8	Character set of the message received from terminal (CCSN of the character set active at the terminal)
KCDEVCAP	dev_cap	1	Information on whether the terminal is a 7- or 8-bit terminal. The specification is in the form "7" or "8" (printable)

Field name COBOL	Field name C/C++	Length in bytes	Description
OSI TP information (only with KCOSITP/ositp_info=Y)			
KCFUPOL	fupol	1	Displays whether the functional unit "Polarized Control" is selected (Y/N).
KCFUHS	fuhsh	1	Displays whether the functional unit "Handshake" is selected (Y/N).
KCFUCOM	fucom	1	Displays whether the functional unit "Commit" is selected (Y/N).
KCFUCHN	fuchn	1	Displays whether the functional unit "Chained Transactions" is selected (Y/N).
KCENDTA	endta	1	<p>This field indicates whether an end of transaction request is permitted at the end of the current processing step and, if this is the case, which calls you have to use.</p> <p>If messages are sent to job-receiving services only in this processing step, the transaction can remain open after the end of the processing step.</p> <ul style="list-style-type: none"> • Blank: no instruction for the termination of the processing step • O: no end of transaction may be requested at the end of the processing step. • R: the transaction and the dialog step must be finished, the service may not be terminated. • S: the transaction must be finished, the dialog step may not be terminated. • C: the transaction must be finished, the service may not be terminated. • F: the transaction must be finished and the service terminated.
KCSEND	send	1	<p>This field indicates whether a message may be sent to the job-submitting service in the processing step.</p> <ul style="list-style-type: none"> • Y: You have to send a message to the job submitter at the end of the dialog step. If KCENDTA is set to "S", you also have to send a message to the job submitter at the end of the transaction. • N: You cannot send an MPUT to the job submitter; you may send messages to jobreceiving services. However, in this case the transaction has to remain open after the processing step.

Field name COBOL	Field name C/C++	Length in bytes	Description
Encryption information (only with KCENCR/encr_info=Y)			
KCPTERM	pterm_enclev	1	<p>Generated minimum encryption level of the client in the associated PTERM or TPOOL statement:</p> <ul style="list-style-type: none"> • N: No minimum encryption level was generated for the client. • 3: The minimum encryption level 3 was generated for the client. • 4: The minimum encryption level 4 was generated for the client. • 5: The minimum encryption level 5 was generated for the client. • T: The minimum encryption level TRUSTED was generated for the client, i.e. the client is trustworthy.
KCCLIENT	client_enclev	1	<p>Maximum encryption mechanism supported by the client:</p> <ul style="list-style-type: none"> • N: The client does not support any encryption mechanism. • 3: The maximum encryption mechanism supported is level 3. • 4: The maximum encryption mechanism supported is level 4. • 5: The maximum encryption mechanism supported is level 5.
KCSESS	session_enclev	1	<p>Encryption mechanism defined for the current session between the client and server:</p> <ul style="list-style-type: none"> • N: No encryption mechanism was defined. • 3: An encryption mechanism of level 3 was defined. • 4: An encryption mechanism of level 4 was defined. • 5: An encryption mechanism of level 5 was defined.
KCCNVTAC	convtac_enclev	1	<p>Generated minimum encryption level of the TACs with which the service was started. There is an entry in this field even in the case of asynchronous services:</p> <ul style="list-style-type: none"> • N: No minimum encryption level has been generated for the TAC. • 2: The minimum encryption level 2 has been generated for the TAC. • 5: The minimum encryption level 5 has been generated for the TAC.

Field name COBOL	Field name C/C++	Length in bytes	Description
Encryption information (only with KCENCR/encr_info=Y)			
KCCONV	conv_enclev	1	<p>This field indicates whether encryption has been defined for the service. This value is selected by the UPIC client or by the encryption level of the transaction code of the service, not that of the session.</p> <p>This field is also supplied with a value in the asynchronous service:</p> <ul style="list-style-type: none"> • N: No encryption was defined for the service. • 3: An encryption mechanism of level 3 was defined for the service. • 4: An encryption mechanism of level 4 was defined for the service. • 5: An encryption mechanism of level 5 was defined for the service.
KCINPMSG	inputmsg_enclev	1	<p>This field indicates whether or not the dialog input message was encrypted by the client:</p> <ul style="list-style-type: none"> • N: The input message was not encrypted. • 3: The input message was encrypted with an encryption mechanism of level 3. • 4: The input message was encrypted with an encryption mechanism of level 4. • 5: The input message was encrypted with an encryption mechanism of level 5.

Field name COBOL	Field name C/C++	Length in bytes	Description
Various information about the user who started the service (KCBENID, kcuserid), the LTERM or (OSI-) LPAP from which the service was started (KCLOGTER,kclogter) and the application (only for KCMISC/misc_info=Y)			
KCUMSGS	amsgs_user	10	Number of queued messages in the user's queue.
KCPWVMAX	pw_val_max	2	<p>Number of days for which the user's password is still valid. Values with a special significance:</p> <ul style="list-style-type: none"> • 0: The password will become invalid within the next 24 hours. • -1: The password was generated without any limitation to validity. The password has unrestricted validity. • -2: The password's period of validity has expired. This value can only occur in an asynchronous service or during sign-on. • -3: The complexity or minimum length of the password has been increased and the password transferred with the KDCUPD tool may not satisfy the requirements for the generated complexity level or may be too short. This value can only occur in an asynchronous service or during sign-on.
KCPWVMIN	pw_val_min	2	<p>Number of days during which the user's password can only be modified at the administrative level but, for example, not via a SIGN CP call (minimum period of password validity). Values with a special significance:</p> <ul style="list-style-type: none"> • 0: The password may be modified. • -1: No password may be set for the user. This may occur in the following cases: <ul style="list-style-type: none"> a) Applications without users b) The user is an LU6.1-Session or OSI TP association c) Connection user (only for TS or UPIC clients) d) internal user KDCMSGUS e) <i>BS2000 systems</i>: Users generated with Kerberos authentication

Field name COBOL	Field name C/C++	Length in bytes	Description
Various information about the user who started the service (KCBENID, kcuserid), the LTERM or (OSI-) LPAP from which the service was started (KCLOGTER,kclogter) and the application (only for KCMISC/misc_info=Y)			
KCLSTSGN	last_sign	14	Date and time of the last sign-on. The date and time are specified in the form YYYYMMDDHHMMSS. The following cases return zeros: <ul style="list-style-type: none"> • During the sign-on operation, after the first successful sign on after regeneration • Internal user KDCMSGUS • User is a LU6.1 session or OSI TP association
KCBNDLMS	bundle_master	8	Name of the master of the LTERM-/LPAP bundle if the LTERM-/ (OSI-)LPAP is a slave of this bundle.
KCISGRMS	is_group_master	1	The field indicates whether the LTERM (or the master of the LTERM bundle) is the master of an LTERM group. <ul style="list-style-type: none"> • Y: (Master) LTERM is a group master. • N: (Master) LTERM is not a group master.
KCLTCP	lterm_client_prot	1	The field indicates the LTERM's client protocol <ul style="list-style-type: none"> • 0: The service is running for the internal LTERM KDCMSGLT (only in an asynchronous service) • 1: LU6.1 • 2: OSI TP • 3: UPIC • 4: DTP (Unix, Linux and Windows systems) • 4: TIAM (BS2000 systems) • 5: APPLI • 6: SOCKET (USP) • 7: HTTP • 8: USP-SECURE • 9: HTTPS

Field name COBOL	Field name C/C++	Length in bytes	Description
Various information about the user who started the service (KCBENID, kcuserid), the LTERM or (OSI-) LPAP from which the service was started (KCLOGTER,kclogter) and the application (only for KCMISC/misc_info=Y)			
KCAPPLST	application_state	1	<p>The field indicates the status of the application:</p> <ul style="list-style-type: none"> • N: The application is running normally. • G: The application has the "Graceful Shutdown" status. • W: The application has the "Shutdown Warn" status. • S: The application is being terminated normally. • T: The application is being terminated abnormally.
KCKRBCAP	kerberos_capability	1	<p>In a dialog service, the field indicates whether the client is Kerberos-capable.</p> <ul style="list-style-type: none"> • Y: The client is Kerberos-capable. • N: The client is not Kerberos-capable. <p>In an asynchronous service: Blank.</p>
KCCDINFO	info_cd_available	1	<p><i>Only on BS2000 systems:</i></p> <p>The following INFO CD information is available in a dialog service:</p> <ul style="list-style-type: none"> • C: Card information (magnetic stripe card) • K: Kerberos information • E: Kerberos information, but the Kerberos dialog returned an error or the information could not be stored at its full length because it is longer than the value generated with MAX PRINCIPAL-LTH. • N: No INFO CD information <p>INFO CD is not permitted in an asynchronous service: Blank.</p>

Field name COBOL	Field name C/C++	Length in bytes	Description
<p>HTTP information can only be supplied in dialog services, which are called by an HTTP or HTTPS client i. e. field KCCP in KBKOPF contains value 7 or 9. (only with KCHTTP/http_info=Y)</p>			
KCHTMTD	httpMethod	1	HTTP method: 1=GET, 2=PUT, 3=POST, 4=DELETE
KCHTVERS	httpVersion	1	HTTP version: 1=1.1
KCSHEME	scheme	1	Scheme: 1=HTTP, 2=HTTPS
KCHTEXIT	httpExit	1	A user specific, the system specific or no HTTP exit will be called (U/S/N)
KCCDCONV	codeConversion	1	Code conversion of input and output message: N no code conversion S system code conversion 1/2/3/4 code conversion SYS1/2/3/4

7.13 LPUT Write to log file

You use the LPUT (log file PUT) call to write a record to the user log file. UTM prefixes this record with the current contents of the KB header. The maximum length of a record is defined at generation (MAX statement, LPUTLTH operand). The records in the log file are not in exactly the same sequence as the LPUT calls in the application.

Setting the 1st parameter (KDCS parameter area)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area		
	KCOP	KCLA	Message area
Write to log file	"LPUT"	Length	Data to be logged

Setting the 2nd parameter

Here you enter the address of the message area from which openUTM is to read the data to be logged.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"LPUT"
KCLA	Length in bytes
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro call	
Macro names	Parameters
KDCS_LPUT	(nb,kcla)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the LPUT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the LPUT operation code.

KCLA

In the KCLA field, the length of the data to be transferred in bytes. openUTM prefixes the length to the data record.

Message area

In the message area, you specify the data which you want to write to the user log file.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area from which UTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ macro calls is described in detail in the section [“C/C++ macro interface”](#).

openUTM returns:

KCRCCC

in the KCRCCC field, the KDCS return code, see next section.

KCRCDC

in the KCRCDC field, the internal return code of openUTM (see the openUTM manual “Messages, Debugging and Diagnostics”).

KDCS return codes in the KCRCCC field for the LPUT call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 01Z Value specified in KCLA too large. It is shortened to the generated maximum length (LPUTLTH operand in the MAX statement).
- 40Z System cannot perform the operation (generation error or system error, timeout), see KCRCDC.
- 43Z Length entry in KCLA is invalid (e.g. negative).
- 47Z Message area missing or cannot be accessed in the specified length.

An additional error code can be found in the dump:

- 71Z INIT call missing in this program.

Features of the LPUT call

- You can still roll back the LPUT operation prior to the next synchronization point.
- The PEND ER/FR/RS and RSET calls roll back the LPUT operation.

The structure of the user log file is described on ["User log file"](#).

7.14 MCOM Define job complex

You use the MCOM (message complex) call to

- define the beginning of a job complex and set the destinations of the basic job and the associated confirmation jobs, or
- define the end of a job complex.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCRN	KCPOS	KCNEG	KCCOMID
Beginning of job complex	"MCOM"	"BC"	LTERM / TAC / Service ID / TAC queue	TAC / blanks / TAC queue	TAC / blanks / TAC queue	Complex ID
End of job complex	"MCOM"	"EC"	Binary zero	Binary zero	Binary zero	Complex ID

All the fields of the parameter area which are not used have to be set with binary zero.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"MCOM"
KCOM	"BC"/"EC"
KCRN	LTERM name / TAC / service ID / binary zero / TAC queue
KCPOS	TAC / blanks / binary zero / TAC queue
KCNEG	TAC / blanks / binary zero / TAC queue
KCCOMID	Complex ID

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	-

C/C++ macro calls	
Macro names	Parameters
KDCS_MCOMBC	(kcrn,kcpos,kcneg,kccomid)
KDCS_MCOMEC	(kccomid)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the MCOM call you make the following entries in the appropriate fields of the KDCS parameter area:

KCOP

In the KCOP field, the MCOM operation code.

KCOM

In the KCOM field, either "BC" for beginning or "EC" for end of a job complex.

KCRN

In the KCRN field, if KCOM = BC applies:

- the LTERM name of a communication partner if the basic job is an output job,
- the TAC of an asynchronous program if the basic job is a background job (without distributed processing), or
- the name of the TAC queue when the basic job is an output job in a TAC queue (without distributed processing).
- the service ID of a job-receiving service if the basic job is directed to a job-receiving service.

If KCOM = EC applies, you have to enter binary zero.

KCPOS

In the KCPOS field, if KCOM = BC is specified as the destination of the positive confirmation job, the TAC of an asynchronous program or a TAC queue, or blanks if no positive confirmation job is to be generated.

If KCOM = EC applies, you enter binary zero.

KCNEG

In the KCNEG field, if KCOM = BC is specified as the destination of the negative confirmation job, the TAC of an asynchronous program or a TAC queue, or blanks if no negative confirmation job is to be generated.

If KCOM = EC applies, you enter binary zero.

KCCOMID

In the KCCOMID field, the complex identifier (complex ID) of the job complex. It is defined for MCOM BC, may be 2 to 8 characters long and has to be prefixed with the character "*". It is to be specified for all the DPUT calls of the complex and for MCOM EC.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro names

The use of C/C++ macro calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field, the KDCS return code, see next page.

KCRCDC

in the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the MCOM call

The following codes can be analyzed in the program:

- 000 Function carried out.
- 40Z openUTM cannot perform the function: generation error or system error, or a job complex is to be started without previously terminating the preceding job complex.
- 42Z Entry in KCOM is invalid.
- 44Z Value in KCRN is invalid:
 - no TAC of an asynchronous program or a TAC queue specified, or TAC or TAC queue inhibited/illegal
 - no LTERM name or LTERM name of a UPIC or HTTP client specified
 - no valid service ID specified, or the service ID is already occupied by another message.
 - asynchronous messages for the dead letter queue (KDCDLETQ) have been created.
- 49Z Contents of unused fields of the KDCS parameter area not equal to binary zero.
- 51Z For KCOM = EC: no (confirmation) job to which user information can be related.
- 55Z Entry in KCCOMID is invalid: the name does not begin with "*" or is already assigned in the program unit or is unknown (for MCOM EC).

57Z Value in KCPOS is invalid:

- no TAC of an asynchronous program or a TAC queue specified, or TAC or TAC queue inhibited/illegal
- specification is not equal to blanks.
- acknowledgement jobs with the destination dead letter queue (KDCDLETQ) have been created.

58Z Value in KCNEG is invalid:

- no TAC of an asynchronous program or a TAC queue specified, or TAC or TAC queue inhibited/illegal, or
- specification is not equal to blanks.
- acknowledgement jobs with the destination dead letter queue (KDCDLETQ) have been created.

An additional error code can be found in the dump:

71Z INIT missing in this program unit.

Features of the MCOM call

- You have to terminate a job complex with MCOM EC before the PEND call, otherwise openUTM aborts the service with PEND ER and 86Z.
- The complex identifier has to be unique within a program unit.
- MCOM BC is only allowed after all preceding job complexes have been terminated.
- If a service identifier is occupied by a job complex, it can only be released by MCOM EC (not as otherwise by DPUT NE).
- Confirmation jobs must be directed to asynchronous program units or TAC queues of the local application.
- If an error occurs, a message complex's main job with negative acknowledgment job is (possibly after redelivery) not saved in the dead letter queue but is deleted. The negative acknowledgment job is activated.

7.15 MGET Receive dialog message

You use the MGET (message GET) call to read messages into the message area in a program unit run of a dialog service. In an asynchronous service, the MGET call is only permitted in follow-up program units or a follow-up processing step.

Messages may have the following origins:

- a terminal
- another application (via LU6.1 or OSI TP)
- a transport system application
- a HTTP client
- a UPIC client
- a previous program unit run of a service of the same service

With message segments, a separate MGET call is necessary for each message segment.

In the case of socket USP applications and HTTP clients, a message segment can be read with several MGET calls. Using KCRLM and the return code it is possible to determine whether a message segment has been read in its entirety.

In case of HTTP client the first MGET reads the query string, if available. If the input message contains no query string, the first MGET reads the message body respectively the first part of the message body.

If the message originates from an OSI partner, it can be a message segment, an error message, a handshake request or a handshake confirmation.

If a function key was pressed, two MGET calls are required: the first provides the return code, the second the data. Only terminals or UPIC clients may send function keys.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area				
	KCOP	KCOM	KCLA	KCRN	KCMF/kcfn
BS2000 systems: Message in format mode	"MGET"	—	Length	-	Format identifier
Message in line mode	"MGET"	—	Length	-	Blanks / edit profile (only on BS2000 systems)
Message from previous program unit of the same application	"MGET"	—	Length	—	Blanks
Rollback message from a program unit	"MGET"	"NT"	Length	Rollback-ID	Blanks
Dialog message from job-submitting service	"MGET"	—	Length	—	Format identifier / Blanks / Name of abstract syntax
Dialog message from job-receiving service	"MGET"	"NT"	Length	Service ID	Format identifier / Blanks / Name of abstract syntax
Status information from job-receiving service	"MGET"	"NT"	0	Service ID	Blanks

NT: message segment

Here you have to supply the address of the message area into which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"MGET"
KCOM	"NT"/-
KCLA	Length in bytes
KCRN	Service ID / Rollback ID / -
KCMF/kcfn	Format identifier / blanks / edit profile (only on BS2000 systems)

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_MGET	(nb,kcla,kcfn)
KDCS_MGETNT	(nb,kcla,kcrn,kcfn)

openUTM return information	
Message area	Contents
	Data
Field name in KB return area	
KCRDF	Screen function/0
KCRLM	Actual length
KCRMGT	Type of message
KCVGST/kcpcv_state	Service status
KCTAST/kcpta_state	Transaction status
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcfn	Format identifier / blanks / edit profile (only on BS2000 systems)
KCRPI	Service ID / Blanks

For the MGET call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the FPUT operation code.

KCOM

In the KCOM field "NT" modifier (message segment), (need only be specified for messages from a job receiver and for rollback messages).

KCLA

In the KCLA field, specify the length in which the message is to be read. This length must not exceed the message area into which the message is to be read (length zero means no message is received. Any existing messages are lost). The actual length of the message (segment) is returned in the KCRLM field.

KCRN

In the KCRN field,
(need only be specified for messages from a job receiver and for rollback messages)

- for messages from job-receiving services, the service ID of the job-receiving service
- for rollback messages, the rollback ID of the rollback message.

i For the first MGET call of a program unit you can ascertain the rollback ID or the service ID from the KCRPI field of the INIT call, for subsequent MGET calls from the KCRPI field of the previous MGET call.

KCMF/kcfn

In the KCMF/kcfn field
(irrelevant for messages from previous program unit runs of the same service)

- for messages on BS2000 systems in format mode:format identifier
- for messages in line mode:blanksalso possible on BS2000 systems: Edit profile
- when reading rollback messages:blanks
- Message from a UPIC client:format identifier that the UPIC client specified for sending
- with distributed processing via LU6.1:format identifier specified by the partner application in KCMF/kcfn when issuing the MPUT call
- for messages from OSI TP partners:Name of the abstract syntax of the message. This name was returned in the KCRMF/kcrfn field in the preceding INIT or MGET call.Here, blanks represent the abstract UDT syntax. In this case, BER is used as transfer syntax and openUTM decodes the message.If you enter a value other than blanks, openUTM transfers the message to the program unit in encoded format (i.e. in the transfer syntax corresponding to this abstract syntax) and the program unit itself must convert the message into the local representation. This is possible, for example, using an ASN.1 compiler.

i The entry in this field will always be correct if, for the first MGET call of the program unit, you enter the value returned by the INIT call in the KCRMF/kcrfn field. For subsequent MGET calls, use the value from the KCRMF/kcrfn field of the preceding MGET call.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area

2nd parameter

The address of the message area into which openUTM is to read the message. You must enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the section [“C/C++ macro interface”](#).

openUTM returns:

Message area

in the specified message area, the message (segment) in its desired length, if KCRCCC=03Z was not set. If the message was longer than specified in KCLA, the remainder will be lost.

Exception: the message originates from a socket USP application or an HTTP client. In this case, the return code 02Z is set, and the rest of the message (segment) can be obtained with the next MGET.

KCRDF

in the KCRDF field, for the first MGET of a job-receiving service with which communication was performed using the LU6.1 protocol, the value in the KCDF field of the associated MPUT call in the job-receiving service. In all other cases this field has the value zero.

KCRLM

in the KCRLM field, the actual length of the message (segment). If a smaller value was specified in KCLA, the message is returned with the length specified in KCLA. In the case of a socket USP applications or HTTP clients, the rest of the message can still be read (KCRCCC = 02Z); otherwise, the rest of the message is lost (KCRCCC = 01Z).

KCRLM=0 for empty messages and if KCRCCC=03Z.

Only on BS2000 systems: When using FHS, the value returned in KCRLM depends on the FHS start parameter KCRLM=.

KCRMGT

in the KCRMGT field, the data read by MGET:

- "M" ("message)a message. When using MGET for a partner that does not communicate via the OSI TP protocol, only the value "M" can be specified.

When using MGET for a partner that communicates via the OSI TP protocol the following output is also possible:

- "C" (confirm)a positive handshake confirmation.
- "E" (error)an error message or negative handshake confirmation.
- "H" (handshake)a handshake request.

KCVGST/kpcv_state

in the KCVGST/kpcv_state field, the service state of the (partner) service, see ["MGET Receive dialog message"](#).

KCTAST/kcpta_state

in the KCTAST/kcpta_state field, the transaction state of the partner service, see ["MGET Receive dialog message"](#).

KCRCCC

in the KCRCCC field, the KDCS return code, see ["MGET Receive dialog message"](#).

KCRCDC

in the KCRDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KCRMF/kcrfn

in the KCRMF/kcrfn field

- for a message in line mode: blanks or - on BS2000 systems - name of the edit profile
- for a message from a partner service:KCRMF/kcrfn contains the format identifier or the name of the abstract syntax of the next message (segment) which can be read by the service defined in the KCRPI field. After the MGET call for the last message (segment), this field contains the format identifier of the last message (segment).

Only on BS2000 systems:

- after reading an entire format: identifier of this format. This is always identical to the identifier of the last output format.
- after reading a partial format: identifier of the next partial format with input data. If there is no further partial format with input data, KCRMF/kcrfn contains the identifier of the most recently read partial format. In this case KCRMF=KCMF (kcrfn=kcfm).

KCRPI

in the KCRPI field

- for a message from a job-receiving service:service ID of a job-receiving service for which message segments or status information is present which has not yet been read.
- in all other cases: blanks.

Service status in the KCVGST/kcpcv_state field

Entry for dialogs without distributed processing:

- "O" (open)
The local service is open.

Entries with distributed processing after a message from a partner service:

- "C" (closed)
The job-receiving service has terminated (PEND FI).
- "D" (disconnected)
Communication with a job receiver was terminated as a result of a loss of connection (only with OSI TP).
- "E" (error)
Only when communicating via LU6.1:The job-receiving service was terminated using PEND ER or PEND FR.
- "I" (inactive)
The job-receiving service is inactive, i.e. it could not be started since, for example, the transaction code was unknown or is locked or no association could be reserved for OSI TP.
- "O" (open)
The partner service is open, you may send further messages to the partner service.

- "P" (pending end dialogue)
This status can only occur in the case of heterogeneous links and for dialogs for which the Commit functionality has not been selected: The job-receiving service wants to end the communication. If the job-submitting service does not agree, it can continue the service using MPUT EM.
- "R" (rollback)
Only when communicating via LU6.1: The job-receiving service was terminated with PEND RS.
- "T" (timeout)
The job-receiving service has been or is being terminated incorrectly, since no answer has been received from the job-receiving service within the generated wait time or it has not been possible to seize a session within the generated wait time.
- "Z" (error)
The job-receiving service has been terminated by the system using PEND ER. (e.g. KDCS call in a job-receiving service with error >= 70Z). The Z service status is also set if a program unit run was terminated with PEND ER, FR or RS in an OSI TP job-receiving service.

If you read a message which originated from a job-submitting service, the service status can only have the value "O".

With the service statuses D, E, I, R, T and Z no message is passed, i.e. the KCRLM return length is 0.

Transaction status in the KCTAST/kcpta_state field

Entries for dialogs without distributed processing:

- "O" (open)
The transaction in the local service is open.
- "C" (closed)
Either start of service or after a synchronization point.
- "R" (rollback)
A rollback message has been read.

Entries for distributed processing after a message from the partner service:

- "C" (closed)
Only when communicating via LU6.1: The transaction is finished in the partner service. This situation occurs if PEND RE or PEND FI has occurred in the partner service and PEND RE is active in the local service.
- "H" (heuristic hazard)
Only when communicating using the OSI TP protocol: The result of a transaction is undetermined since communication with at least one communication partner has been interrupted. The possibility that one of the communication partners involved in the last transaction has made a heuristic decision which conflicts with the actual result of the last transaction cannot be excluded.
- "I" (inactive)
A job receiver transaction exists because, for example, the transaction code is unknown or no connection could be reserved during the generated waiting time.
- "M" (mismatch)
It was not possible to synchronize the transaction in the remote service with the transaction in the local service. This may occur after a timeout or after termination and start of a UTM-F application. When communicating via the OSI TP protocol, this situation may occur if at least one of the communication partners involved in the last transaction has made a heuristic decision which conflicts with the actual result of the transaction.

- "O" (open)
The transaction in the partner service is open.
- "P" (prepare to commit)
The partner service has either initiated the end of transaction itself or is requesting the local service to initiate the end of transaction.
- "R" (rollback)
The transaction in the partner service has been rolled back.
- "U" (unknown)
Only possible when communicating via OSI TP without global transaction logging. The transaction status is unknown.

When you read a message from a job-submitting service, only the values "C", "O", "P" or "U" can occur.

KDCS return codes in the KCRCCC field for the MGET call

The following codes can be analyzed in the program:

- 000 Operation carried out.
The message (segment) was read in its entirety.
- 01Z Length conflict: KCLA < KCRLM; the message area is too short, the message (segment) has been truncated.
- 02Z In the case of messages from a socket USP application or an HTTP client:
Length conflict: KCLA < KCRLM; the message area is too small; the part of the message segment that was truncated can be read by means of another MGET call.
- 03Z For partial formats:
KCMF/kcfn does not contain the name of the next returned partial format.

For distributed processing and messages from UPIC clients:
KCMF/kcfn does not contain the format identifier or the name of the abstract syntax of the message (segment) which is to be read next.

No message (segment) is transferred to the message area; the KCRPI and KCRMF/kcfn fields contain a new proposition for the next message (segment).
- 05Z For single formats:
The format displayed on screen differed from the format specified in KCMF/kcfn. The message was formatted as per the format identifier of the most recent display and not as specified in KCMF/kcfn.

In line mode:
- The first character in KCMF/kcfn is not a blank
- Only on BS2000 systems:*
- The name of the edit profile is invalid.
- 10Z Message has already been completely read

12Z (Only possible in the job-submitting service)
No (more) message (segments) are present from the specified service ID. However, message (segments) are still present from other job-submitting services. The content of the message area has not been changed. The KCRPI and KCMF/kcfn fields contain a new proposition about which message (segment) can be read next.

19Z The function key has not been generated or the allocated special function is invalid.

20Z...
39Z

- The terminal user has pressed a function key to which a return code was assigned during generation,
- or the function key was triggered by a UPIC client.
- If a function key is triggered by an UPIC client or a function key to which a message has been assigned is pressed then this message must be read with a subsequent MGET call.

Only on BS2000 systems:

- KDCS xx ($01 \leq xx \leq 20$) was entered (function key simulation),

Additional return codes can be found in the dump:

70Z Operation cannot be performed by the system (system or generation error); see KCRCDC.

71Z An MGET call was entered in the first processing step of the first program unit run of an asynchronous service, or INIT is missing in this program unit run.

72Z Specification in KCOM is invalid.

73Z Length entry in KCLA is invalid.

77Z The message area is missing or cannot be accessed in the specified length.

78Z *Only on BS2000 systems:*
The FORMAT event exit reports an error.

Features of the MGET call

- Reaction to length conflicts

The actual message (segment) length is returned in the KCRLM field.

When length conflicts occur, note the following: If $KCRLM < KCLA$ only $KCRLM$ characters (bytes) are moved to the message area. The contents of the rest of the message area are undefined. Only one message (possibly consisting of two or more message segments) can be read in a program unit. If the length entry in $KCLA$ of the parameter area is shorter than the actual message (segment), the remainder ($KCRLM - KCLA$) is lost and can no longer be read with a subsequent MGET.

Exception: if, in the case of messages from a socket USP application or an HTTP client, the message area is too small ($KCLA < KCRLM$), the rest of the truncated message segment can be read by means of another MGET call.

Example

Three message segments, each of 100 bytes, are to be read using MGET calls. The table below shows the effect of different specifications in the $KCLA$ field.

User specification		UTM returns			Explanations
KCOP	KCLA	KCRLM	Transferred length in MA	KCRCCC	
MGET	100	100	100	000	The message segment as received successfully
MGET	50	100	50	01Z	The message segment was longer than specified in $KCLA$, the remainder is lost.
MGET	150	100	100	000	The message segment was received successfully
MGET	100	000	000	10Z	No fourth message segment was present

- Conversion of lower case letters

openUTM does not automatically convert lowercase letters into uppercase letters when MGET is called. However, you can perform this conversion by using the appropriate format generation.

On BS2000 systems you can also perform a conversion by using edit profiles.

- Messages of length zero

Messages of length zero are, for example, possible in the following cases:

- Only the transaction code (without any further data) was sent at the start of a service
- In a follow-up program unit a message is to be read from the preceding program unit of the same service and MPUT was specified with length 0 in the previous program unit or no MPUT was issued.
- A client program or a partner service has sent an empty message.
- The terminal user pressed a function key without assigning a message,
- Only on BS2000 systems: $KDCS_{xx}$ ($01 \leq xx \leq 20$) was entered (function key simulation).
- Only on BS2000 systems: The terminal user has sent an empty message (DUE function with empty screen)

- Removing a transaction code

If a transaction code was specified together with a message at service start and no function key was used, the following is removed from the message

- the transaction code, including trailing blanks, if the entry was unformatted(MAX statement parameter LEADING-SPACES)

Only on BS2000 systems:

- the first 8 characters of the message (transaction code) if the entry was formatted with *formats
- the first 10 characters (attribute field plus TAC) if the entry was formatted with +formats
- the first 8 characters of the message (transaction code) if the entry was formatted with +formats
- the first eight (with *formats) or ten (with +formats) characters of the first message if the entry was formatted with partial formats.

The removal of the transaction code can be prevented in an INPUT exit.

If the MGET call is used in the BADTACS event service the invalid transaction code is **not** removed from the input message. The entire message is made available. This also applies if the invalid transaction code is allocated to a function key.

- Receiving partial formats

Every partial format must be read with a separate MGET. Following INIT, openUTM supplies, in KCRMF/kcrfn, the name of the first returned partial format in which data were entered. This name must be specified in KCMF/kcfn when issuing MGET. MGET supplies, in KCRMF/kcrfn, the name of the next partial format together with input data, which must be specified in KCMF/kcfn with the following MGET. With the final partial format with input data, KCRMF/kcrfn again has the name specified in KCMF/kcfn, see also example. You recognize the last partial format by the identical entries in KCMF/kcfn and KCRMF/kcrfn or by the return code 10Z in the next MGET.

If no data was input in any of the partial formats, the first MGET call supplies KCRCCC=10Z, KCRLM=0, KCRMF=blanks in the return area.

If the name entered in KCMF/kcfn differs from the one previously supplied in KCRMF/kcrfn then

- openUTM does not write data to the message area
- openUTM sets KCRLM=0
- openUTM sets the return code 03Z in KCRCCC
- openUTM writes the 'correct' format name again in KCRMF/kcrfn.

Only on BS2000 systems: Note that the way in which partial formats are transferred also depends on the FHS start parameters, see FHS manual. If, for instance, no entry is made in any partial format, some FHS start parameters cause openUTM to return KCRCCC=10Z and KCRMF/kcrfn=blanks after the first MGET.

Example

The three partial formats *PART1, *PART2 and *PART3 are to be read using MGET calls; note the return information in KCMF.

User entries		UTM return info		Explanations
KCOP	KCMF/kcfn	KCRMF/kcrfn	KCRCCC	
INIT		*PART1	000	
MGET	*PART1	*PART2	000	Read 1st partial format
MGET	*PART2	*PART3	000	Read 2nd partial format
MGET	*PART3	*PART3	000	Read 3rd partial format
MGET	*PART3	*PART3	10Z	Message already completely read

You recognize the last partial format by the identical entries in KCMF/kcfn and KCRMF/kcrfn or by the return code 10Z in the next MGET.

Features of the MGET call with distributed processing

- When communicating via the OSI TP protocol, the format identifier for the transfer of the name of the abstract syntax is used. Here, blanks represent the abstract syntax of UDT. In all cases in which the application program unit does not work with UDT, the conversion of the message from the local representation to transfer syntax or vice versa must be performed by the application itself - in accordance with the rules of the abstract syntax. This process is termed the encoding or decoding of a message. To do this, the application can use an ASN1 compiler. openUTM carries out the encoding and decoding of messages in UDT format.

-
- When communicating via the LU6.1 protocol, openUTM transfers the format identifier. However, it does not format the message: the partner applications exchange only net data. When using MPUT, you can specify any name in the KCMF/kcfn field. This name is indicated to the reading program unit in the KCRMF/kcfn field after INIT or following a preceding MGET and must be specified in the KCMF/kcfn field when calling MGET.
 - The return codes for the function keys (19Z through 39Z) cannot occur with an MGET call in the job-receiving service, because the job-submitting service cannot forward any corresponding special functions to the job-receiving service.
 - In the KDCS return area the MGET call provides the service status and the transaction status of the partner service.
 - If you do not adhere to the bottom-up strategy (see "[Programming rules and recommendations](#)") when communicating via LU6.1, a service restart can nevertheless be initiated by sending a message from the job-submitting service to the job-receiving service. Then the follow-up program unit in the job-receiving service is started. This uses MGET to read the message from the last synchronization point and receives the service status "O" and the transaction status "C" from the job submitter. After the INIT call it recognizes from the service indicator KCKNZVG/kccv_status in the KB header that this is a service restart.

Particularities of the MGET call when communicating with a UPIC client

openUTM transfers the format identifier during communication, but it does not format the message: only net data is exchanged between the UPIC client and the application. When a message is sent, any name can be specified as the format identifier. This name is displayed in the reading program after the INIT or after a preceding MGET in the KCRMF/kcfn field and must be specified for an MGET call in the KCRMF/kcfn field.

Particularities of the MGET call when communicating with a socket USP application or an HTTP client

A message segment from a socket USP application or an HTTP client can be read by means of several MGET calls. Using the return code it is possible to determine whether a message (segment) has been read. The return code 02Z indicates that a message segment has not yet been read in its entirety. By comparing KCLA and KCRLM you can determine how large the rest of the message segment is. The return code 000 indicates that the message (segment) has been read in its entirety and that the next MGET will read a new message (segment).

Features of a rollback message

A rollback message always originates from a program unit terminated with PEND RS. Following service restart, it is supplied to the program unit which was started as a follow-up program unit after the synchronization point. The rollback message must be read with the first MGET call. It enables the program unit to react appropriately and thus avoids repeated rollback of the transaction. The program unit recognizes a service restart from the service indicator which takes the value "R". It is available in the KCKNZVG/kccv_status field after the INIT call. The rollback message is deleted after processing in the case of a loss of connection or KDCCOFF.

With the MPUT call, you specify in the KDCS parameter area, whether (KCDF = KCRESTRT) or not (KCDF contains binary zero) a screen restart is performed when the service is restarted. If no screen restart is requested, openUTM rolls back the transaction and immediately starts the program unit run specified at the last synchronization point. The rollback message can be read with MGET.

MGET call for reading status information from the job receiver

Status information takes the form of messages of length 0 which are internally created by openUTM. Their only purpose is to indicate the status of the job-receiving service when errors occur in distributed processing. The status information is read unformatted using MGET calls (blanks in KCMF/kcfn).

If it was necessary to roll back the distributed transaction then, when the service restarts, it is advisable to restart the program unit for which a message was present at the end of the last distributed transaction, or for which the next input from the terminal is intended. If a program unit is started in the job-submitting service, openUTM sends status information to this program, if necessary. Here you have to consider the following:

- The status information relates to the job receivers which caused the distributed transaction to be rolled back and were or are subsequently being terminated.
- If the input message at service restart is for the program unit, then the input message has to be read with the 1st MGET and the status information with the second MGET. If, however, the input message originates from the job-receiving service and is not sent by the job receiver, then you only receive the status information of the job receiving service.
- If the input message at service restart is for the job-receiving service and if this service cannot be started within a generated wait time (e.g. because of loss of connection), openUTM starts the follow-up program unit in the job-submitting service instead and sends the job-submitting service status information which has to be read with the first MGET.
- If, after service restart of the job-submitting service, a job-receiving service is addressed again and if an error reoccurs, then the job-submitting service can be rolled back several times to the same synchronization point. Since the status information is retained from the preceding rollback, you may receive two or more bits of status information. In this case you obtain with each MGET the service ID of a subsequent service for which there is status information.
- There may be status information available from different job-receiving services. This status information has to be read in the order suggested by openUTM (KCRPI).
- "Substitute messages" are received with distributed processing via OSI TP, even if there is no service restart. If global transaction logging is not active, the transaction in the job-submitting service is **not** rolled back if an error occurs in the job-receiving service (e.g. timeout). If global transaction logging is active, the transaction in the job-submitting service is not rolled back only if no distributed transaction with the job receiver is open, e.g. if the timer for the association allocation has expired.

Special KDCS functions (BS2000 systems)

The KDCS interface provides "special KDCS functions" as a particular way of entering data at the terminal. The terminal user activates these functions by entering the string (KDCSxx) xx= 01,...,20 when UTM expects to receive input for a follow-up program unit run. A maximum of 20 special KDCS functions are therefore possible. The special KDCS functions are intended to be replacement inputs for terminals that do not have the appropriate keys.

7.16 MPUT Send dialog message

You use the MPUT (message put) call:

- to send a dialog message (segment) to a client
- to send a message (segment) to a subsequent program unit in the same dialog step or in a linked service
- to send a rollback message for the service restart after PEND RS
- to send the last screen output of a stacked service to the terminal
- with distributed processing, in the job-submitting service, to send a message (segment) to a job-receiving service, or
- with distributed processing, in the job-receiving service, to send a message (segment) to the job-submitting service
- to request a processing confirmation from an OSI TP partner
- to send a negative processing confirmation or an error message to an OSI TP partner.
- to create an error message that is sent to a UPIC client, a socket USP application or an HTTP client in the event of abnormal termination of a service (system PEND ER) initiated by openUTM

In an asynchronous service, an MPUT message can only be sent to a job-receiving service or to a follow-up program unit.

The call cannot be used in an MSGTAC program.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCLM	KCRN	KCMF/kcfn	KCDF
BS2000 systems: Message in format mode	"MPUT"	"NT"/ NE"	Length	Blanks	Format identifier	Screen function
BS2000 systems: Message in line mode	"MPUT"	"NT"/ NE"	Length	Blanks	Blanks / edit profile	Screen function
Unix, Linux and Windows systems: Message in line mode	"MPUT"	"NT"/ NE"	Length	Blanks	Blanks	—
Message to program unit	"MPUT"	"NT"/ NE"	Length	TAC	—	—
Last screen output of stacked service	"MPUT"	"PM"	Length	Blanks	Format identifier / Blanks	Screen function
Send rollback message	"MPUT"	"RM"	Length	Rollback ID	binär null	binary null / KCRESTRT
Message to job-receiving service now(LU6.1)	"MPUT"	"NT"/ NE"	Length	Service ID	Format identifier / Blanks	binary null
Message to job-submitting service (LU6.1)	"MPUT"	"NT"/ NE"	Length	Blanks	Format identifier / Blanks	any value
Message to job-receiving service (OSI TP)	"MPUT"	"NT"/ NE"	Length	Service ID	Blanks / abstract syntax	0
Message to job-submitting service (OSI TP)	"MPUT"	"NT"/ NE"	Length	Blanks	Blanks / abstract syntax	0
Request a dialog confirmation	"MPUT"	"HM"	0	Service ID / blanks	Blanks	0
Error message or neg. confirmation	"MPUT"	"EM"	0	Service ID / blanks	Blanks	0
Error message for UPIC clients, socket USP applications or HTTP clients	"MPUT"	"ES"	Length	Blanks	Blanks / Format identifier	0

NT: message segment

NE: last message segment or complete message.

For KCOM = HM/EM/ES/PM/RM you have to set binary zero for all the fields not used in the KDCS parameter area.

Setting the 2nd parameter

Here you have to supply the address of the message area from which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"MPUT"
KCOM	"NT"/"NE"/"PM"/"RM"/"HM"/"EM"/"ES"
KCLM	Length in bytes
KCRN	Blanks/TAC/Rollback ID/service ID
KCMF/kcfn	Format identifier / blanks / Name of abstract syntax / edit profile (only on BS2000 systems)
KCDF	Screen function/binary zero
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS message area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_MPUTNT/KDCS_MPUTNE	(nb,kclm,kcrn,kcfn,kcdf)
KDCS_MPUTPM	(nb,kclm,kcfn,kcdf)
KDCS_MPUTRM	(nb,kclm,kcfn)
KDCS_MPUTHM/KDCS_MPUTEM	(nb,kcrn)
KDCS_MPUTES	(nb,kclm,kcfn)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the MPUT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the "MPUT" operation code.

KCOM

In the KCOM field:

- NT for message segment.
- NE for complete message or final message segment.
- PM for the last screen output of a stacked service or the request for a service restart in the sign-on service.
- RM for a rollback message.
- HM for requesting a processing confirmation from OSI partners.
- EM for an error message or a negative processing confirmation to OSI partners.
- ES for creating an error message to a UPIC client, a socket USP application or an HTTP client.

KCLM

In the KCLM field, the length of the message in the message area which is to be sent (length zero is also permitted).

KCRN

In the KCRN field, depending on message recipient:

- the transaction code of a follow-up program if this MPUT sends a message to a follow-up program in the same application (this also applies for a PEND FC call).
- blanks if this MPUT sends a dialog message to a client.

-
- the rollback identification (rollback ID) if a rollback message is to be sent for the service restart. The rollback ID must begin with "<" (see chapter "MGET Receive dialog message", section "Features of a rollback message").
 - blanks if this MPUT creates an error message for a UPIC client.
 - blanks for a response to the job-submitting service.
 - the service ID of a job-receiving service if this MPUT call is directed to a job-receiving service.

KCMF/kcfn

In the KCMF/kcfn field

- blanks for a message in line mode
- blanks for KCOM = PM with KCLM = 0
- blanks or format identifier for messages to a UPIC client or a LU6.1 partner.
- Blanks or name of the abstract syntax
The name of the abstract syntax of the message must be specified in the case of messages to OSI TP partners. Here, blanks represent the abstract syntax of UDT. In this case, the BER transfer syntax is used and the encoding of the message is performed by openUTM.
If you enter a value other than blanks, the message must be transferred to openUTM in encoded format, i.e. in the transfer syntax corresponding to this abstract syntax.

Only on BS2000 systems:

- a format identifier for a message in format mode or for KCOM = PM with KCLM > 0. If a screen is to be refreshed, the specified format must be a component of the screen to be refreshed.
- edit profile for a message in line mode

In all other cases, irrelevant

KCDF

In the KCDF field, a screen function, if the receiver is a terminal.

In the following cases you have to set binary zero in the field:

- KCMF/kcfn contains the name of a #format.
- The message is intended for a job-receiving service.
- The message is intended for an OSI TP job-submitting service.
- MPUT PM with KCLM = 0 is used.
- Only on BS2000 systems: KCMF/kcfn contains the name of the edit profile.

When sending a rollback message (KCOM = RM), you must specify KCRESTRT or binary zero.

Message area

You enter in the message area the message you want to output.

You enter the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area from which openUTM is to read the message (or user information). You enter the address of the message area even if you have entered the length 0 in KCLM.

Macro names

The use of C/C++ calls is described in detail in the [section "C/C++ macro interface"](#).

openUTM returns:

KCRCCC

In the KCRCCC field, the KDCS return code.

KCRCDC

In the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the MPUT call

The following codes can be analyzed in the program:

000 Function carried out

41Z Too many MPUT calls:

- another MPUT NT/NE after MPUT NE/HM
- another MPUT after or before an MPUT PM
- more than one MPUT RM
- MPUT RM in the first transaction of a service or unpermitted change of entry in KCRN (if there are multiple message segments, the TAC of the follow-up program must always be the same).
- MPUT HM issued as the first call to an OSI TP partner
- following a CTRL call, an MPUT HM was issued to the same partner
- following a CTRL AB call, an MPUT was issued to the same partner
- only in an OSI TP job-receiving service: an MPUT was issued to the job submitter and KCSEND has the value N.
- 254 MPUT NT calls to an HTTP client already done and the output message will be formatted by an HTTP exit program

45Z The value specified in KCMF/kcfn is invalid. Possible cause: The specified abstract syntax has not been generated for the OSI-LPAP partner

Additional error codes can be found in the dump:

70Z The system cannot perform the operation (system or generation error), see KCRCDC.

71Z MPUT call in an MSGTAC program unit or no INIT in program unit.

72Z Entry in KCOM is invalid or MPUT-PM was entered in an asynchronous program unit.

73Z Length entry in KCLM is invalid.

74Z Value in KCRN is invalid, because

- in a dialog service KCRN contains a value, which is not a TAC of a dialog program unit nor a valid service ID
- in an asynchronous service KCRN contains a value, which is not a TAC of an asynchronous program unit nor a valid service ID
- the user is not entitled to use the program unit run
- in an asynchronous program unit, KCRN is filled with blanks
- with MPUT HM, the destination in KCRN is not an OSI TP partner
- with MPUT EM, the destination in KCRN is not an OSI TP partner.
- with MPUT ES in KCRN, no blanks have been specified.

75Z Value in KCMF/kcfn is invalid. Possible causes:

- Format identifier in KCMF/kcfn changes or is invalid.

Only on BS2000 systems:

- The edit profile has not been generated or the edit profile changes for message segments (MPUT NT).

77Z The message area is missing or cannot be accessed in the specified length.

89Z Contents of fields not used in the KDCS parameter area are not equal to binary zero for KCOM PM/RM/HM /EM/ES.

Features of the MPUT call

- The message area is left unchanged when openUTM executes the call.
- Maximum message length for MPUT NT/NE
For messages to terminals, to transport system applications of type APPLI or to a subsequent program unit, the total message may be no longer than the value generated in the NB operand of the MAX control statement.
Otherwise, the length of a message segment is limited to 32,767 bytes and the length of the total message is unlimited.
- You can use screen functions for outputs in format mode (see "[Screen output functions in format mode \(BS2000 systems\)](#)").
Only on BS2000 systems: If you use edit profiles, KCDF must be set to binary zero, otherwise openUTM returns 70Z.
- You can display multiple messages in a processing step, provided that the messages are issued to job-receiving services and the transaction remains open at the end of the processing step. In all other cases a maximum of **one** message may be displayed.

- A message can consist of two or more message segments, e.g. two or more MPUT NT followed by an MPUT NE with the same KCRN. You can create messages in parallel for job-receiving services, i.e. the service ID in KCRN can change. Any other change to the message destination is not permitted, because it creates an end of message for all messages not yet terminated. Following an unpermitted change of message destinations, no further MPUT is permitted. After terminating a message with MPUT NE or MPUT HM, no further MPUT is permitted with KCRN.
- With PEND KP/RE/FI/ER/FR and PGWT KP/CM, the entire message is transmitted to the communication partner (formatted, if applicable).
- With PEND PA/PR/FC/SP, the message or message segments are passed to the follow-up program whose TAC was specified in KCRN (PEND and MPUT calls). The follow-up program must read each message segment with a separate MGET.
- At the end of a processing step all messages not yet terminated are closed implicitly by openUTM.
- In a program unit run, ending with PEND PA/PR, PS, SP or FC, the MPUT call can be omitted. In a program unit run ending with PEND KP/RE or PGWT KP, at least one MPUT must be entered. Equally, in a dialog service, at least one MPUT have been entered before PEND FI/ER or FR. However, this does not apply, if the KCSSEND field contains the value "N" in an OSI TP server service.
The MPUT is not required in the sign-on service when it is to be followed by a service restart. openUTM then terminated the service that is ready to be restarted abnormally.
- In an asynchronous service, no MPUT may be issued before a PEND FI/ER or FR.
- Empty messages, i.e. KCLM=0, are permitted.

If the empty message is sent to the terminal in format mode, it causes an empty format or partial format to be output.

On BS2000 systems, any dependencies must be taken into account by the FHS start parameters. See the FHS manual.

Empty messages are also permitted in the case of distributed processing.

- An empty message to a transport system application of the type APPLI will not be sent.
- In the case of message segments to socket USP partners, each message segment must be sent by means of a separate MPUT NT. A separate message segment is created for each MPUT NT/NE.
In the case of MPUT calls with KCLM=0, no messages are sent unless automatically created USP headers (see ["Output messages of openUTM"](#)) are used. In this case, the header is also sent in the case of MPUT NE/NT with a length of zero. Exception: if the program unit contains only a single MPUT NE/NT and KCLM=0, no header is sent.
- In case of HTTP clients all message segments created with MPUT NT will be sent in the message body of the HTTP response.
- If the receiver is not a terminal, the message is sent transparently, i.e. the message may contain any bit pattern.
- An empty message to a UPIC application is sent since the permission to send has been transferred.
- Sending message segments

A message can consist of a number of message segments, e.g. multiple MPUT NT followed by an MPUT NE with the same KCRN. You can create messages in parallel for job-receiving services, i.e. the service ID in KCRN can change. Any other change to the message destination is not permitted, because it creates an end of message for all messages not yet terminated. If the last message segment is not identified by "NE" in KCOM, the message terminates automatically when PEND occurs.

If there is a change between line and formatted modes or a change of the edit profile, openUTM responds with 75Z and aborts the service.

-
- Sending partial formats

With a terminal in format mode, a screen can be set up from multiple partial formats. Each of these partial formats must be output with MPUT NT; the last one can be output with MPUT NE.

- Screen functions (KCDF) can only be specified with the **first** MPUT NT. For subsequent MPUT calls, KCDF must contain binary zeros. Otherwise, UTM will terminate the service with 70Z in KCRCCC and K606 in KCRCDC.

Screen functions permitted with partial formats:

KCREPL Delete screen. This function must be specified when a screen is to be set up anew. If KCREPL is not set, any partial format existing on the screen will be overwritten by a new one. If the same partial format is output again, only the contents of the fields will be replaced (same as KCERAS).

KCALARM Audible alarm.

KCREPR Print on hardcopy printer.

KCERAS Delete unprotected fields; see section [“Using partial formats \(BS2000 systems\)”](#).

- Special features of the MPUT RM call

MPUT RM is also permitted if preceded by MPUT NT/NE or MPUT PM calls. The length of the MPUT-RM message is limited to 32,767 bytes.

Only one rollback message can be output in a program unit run. Other MPUT calls are permitted before or after MPUT RM. Rollback messages are deleted when the user signs off. After a service restart, the field KCRPI contains blanks.

- Special features of the MPUT PM call

openUTM uses MPUT PM to output the last output message of a stacked service on the screen. The following holds:

- for KCLM = 0 the output appears unchanged on the screen, for KCLM > 0 it is overwritten (not exceeding the specified length), but sent in its entirety. The length of the MPUT-PM message is limited by the value generated in the NB operand of the MAX control statement.
 - for output messages in line mode you must always specify KCLM = 0 (and KCMF/kcfn = blanks)
 - the program unit must terminate with PEND FI, otherwise UTM aborts the service with 82Z
 - the sign-on service must use this variant at the end of the service if a service restart is to be executed.
- Abstract syntax with distributed processing via the OSI TP protocol

If you specify a value not equal to blanks in KCMF/kcfn when communicating with a partner via the OSI TP protocol, then you have to generate this value as the name of an abstract syntax for the partner. In this case, the application program unit has to transfer the message to openUTM in encoded form, i.e. the application must convert the message to the transfer syntax allocated to the abstract syntax. To do this, the application can use an ASN1 compiler. Abstract syntaxes with the name "CCR" or "OSITP" are not permitted.

- When communicating via a UPIC client or the LU6.1 protocol, openUTM transfers the format identifier. However, it does not format the message: the partner applications exchange only net data. When using MPUT you can specify any name in the KCMF/kcfn field. This name is indicated to the reading program unit in the KCRMf/kcrfn field after INIT or following a preceding MGET and must be specified in the KCMF/kcfn field when calling MGET.
 - MPUT call in the job-submitting service
-

- An MPUT call can be used by a job-submitting service to start a job-receiving service in a partner application, or to send a message to a job-receiving service which has already started.
You have to specify the service ID, which was allocated to the job-receiving service when APRO DM was called, in the KCRN field as target.
- In a program unit run of the job-submitting service you can only use MPUT to send messages either to the LTERM partner (KCRN=blanks), to the follow-up program unit (KCRN=TAC) or to one or more job-receiving services (KCRN=service ID).
- In the job-submitting service KCDF must contain binary 0 for MPUT.
- Each message segment output with MPUT NT to a job-receiving service has to be read there with a separate MGET.
- In a program unit run, no messages (message segments) may be sent to a job-receiving service prior to PEND PR or PA, otherwise openUTM aborts the job-submitting service with the error code KCRCCC=82Z.
- MPUT call in the job-receiving service
 - Setting the KDCS parameter area is the same as for the MPUT call for a terminal.
 - When communicating via LU6 protocol, the KCDF field may contain any value which has been passed to the job-submitting service in MGET as screen function. For message segments, only the KCDF value of the first message segment is transferred.
You have to set KCDF to binary zero when communicating via the OSI TP protocol.
 - Each message segment output with MPUT NT to a partner service has to be read there with a separate MGET.
- Particularities of the MPUT HM call
With MPUT HM, a program run can request a processing confirmation from an OSI TP partner. The following rules apply when using MPUT HM:
 - The call can only be used, if the handshake function was selected for communication; otherwise openUTM aborts the service with 72Z. With INIT, the KB header indicates to the job-receiving service whether the handshake is permitted.
 - An MPUT HM to a partner, which does not have O or U transaction status, is rejected by openUTM with 72Z.
 - At least one MPUT NT to the partner must have been entered prior to MPUT HM.
 - MPUT HM produces an end of message for the communication partner.
 - No data can be passed to the call (KCLM = 0).
 - Following MPUT HM only one PEND KP or one PGWT KP is permitted. With all other PEND variants, UTM responds with the return code 82Z.
 - Following MPUT HM you may not issue a further CTRL PR/PE call to the same partner.
- Particularities of the MPUT EM call
 - Using the MPUT EM call you can report an error to an OSI TP partner. If a handshake request is confirmed negatively with the call, MPUT EM must be entered as the first MPUT to the partner that requires a processing confirmation. The call must be issued in the same transaction in which the handshake request was read. Otherwise a positive confirmation is sent.
 - No data can be passed to the call (KCLM = 0).
 - An MPUT EM to a partner, which does not have O or U transaction status, is rejected by openUTM with 72Z.
- Particularities of the MPUT ES call

-
- The MPUT ES (error system) call can be used in a dialog program unit to create an error message for a UPIC client, a socket USP application or an HTTP client. This error message is only sent when the service is terminated abnormally by openUTM (system PEND ER).
 - An error message created with MPUT ES remains valid, provided it is not overwritten with another MPUT ES, until the service is terminated with the output of a dialog message to the UPIC client, socket USP application or an HTTP client. In the case of service concatenation (PEND FC), the error message is thus also valid in the concatenated service.
 - Each subsequent MPUT ES overwrites the error message written last. An MPUT ES with a length of 0 deletes the error message.
 - The length of the MPUT ES message is limited by the value generated in the NB operand of the MAX control statement.
 - If the transaction is rolled back, the error message is rolled back to the state of the last synchronization point.

7.17 PADM Administer printouts and printers

The PADM (printer administration) call is used to administer the printers associated with an LTERM printer control.

PADM provides you with the following functions:

- activate or deactivate confirmation mode for an LTERM printer control.
Unix, Linux and Windows systems
This function applies globally to the cluster in UTM cluster applications.
- confirm or repeat a printout
- modify the assignment of a printer to an LTERM partner.
Unix, Linux and Windows systems
This function is not permitted in UTM cluster applications.
- modify the printer status, i.e. lock and release printer, set up or clear connection to a printer.
Unix, Linux and Windows systems
Locking and releasing apply globally to the cluster in UTM cluster applications.
- read information about a printer into the message area
- read information about printouts to be confirmed.

i A sample program which you can use here is supplied with openUTM. See the section dealing with the KDCPADM program unit in the openUTM manual “Administering Applications” for further details.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area						
	KCOP	KCOM	KCLA	KCRN	KCLT	KCACT	KCADRLT
Confirm printout	"PADM"	"OK"	0	Control ID	LTERM name	Binary zero	Binary zero
Repeat printout	"PADM"	"PR"	0	Control ID	LTERM name	Binary zero	Binary zero
Change confirmation mode	"PADM"	"AT"/"AC"	0	Control ID / blanks	LTERM name	Binary zero	Binary zero
Change printer assignment	"PADM"	"CA" <i>Unix, Linux and Windows systems not permitted for UTM cluster applications</i>	0	Control ID	LTERM name	Binary zero	LTERM name
Change printer status	"PADM"	"CS"	0	Control ID	LTERM name	ON/OFF /CON/DIS	Binary zero
Information on printout	"PADM"	"AI"	44	Control ID / blanks	LTERM name	Binary zero	Binary zero
Information on printer	"PADM"	"PI"	34	Control ID / blanks	LTERM name	Binary zero	Binary zero

You must set binary zero in all the fields not used in the KDCS parameter area

Setting the 2nd parameter

Here you supply the address of the message area to which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"PADM"
KCOM	"OK"/"PR"/"AT"/"AC"/"CA"/"CS"/"AI"/"PI"
KCLA	Length in bytes / 0
KCRN	Control ID / blanks
KCLT	LTERM name of control terminal
KCACT	"ON"/"OFF"/"CON"/"DIS"/binary zero
KCADRLT	Binary zero/ LTERM name

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_PADMOK/KDCS_PADMPR/KDCS_PADMAT/KDCS_PADMAC	(nb,kcrn,kclt)
KDCS_PADMCA	(nb,kcrn,kclt,kcadrlt)
KDCS_PADMCS	(nb,kcrn,kclt,kcact)
KDCS_PADMAI/KDCS_PADMPI	(nb,kcla,kcrn,kclt)

openUTM return information	
Message area	Contents
	Data/-
Field name in the KB return area	
KCRLM	Actual length
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcrfn	Follow-up control ID/blanks

For the PDAM call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the PADM operation code.

KCOM

In the KCOM field

- OK: confirm printout
- PR: repeat printout
- AC: activate acknowledgement mode.
Unix, Linux and Windows systems
AC applies globally to the cluster in UTM cluster applications.
- AT: deactivate acknowledgement mode, i.e. switch back to automatic mode.
Unix, Linux and Windows systems
AT applies globally to the cluster in UTM cluster applications.
- CA: assignment to a different LTERM.
Unix, Linux and Windows systems
CA is not permitted in UTM cluster applications.
- CS: change the state of a printer.
Unix, Linux and Windows systems
CS for locking and releasing applies globally to the cluster in UTM cluster applications.
- AI: read information about printouts to be confirmed
- PI: read information about printer

KCLA

In the KCLA field, the length of the data to be transferred to the message area.

- if KCOM=AI: 44
- if KCOM=PI: 34

and 0 for all other variants.

KCRN

In the KCRN field

- for KCOM = OK/PR/CA/CS the control ID of a printer as generated in the PTERM statement with KDCDEF
- for KCOM = AT/AC/AI/PI the control ID of a printer (as per PTERM statement) or blanks if the operation is to be valid for all printers assigned to the printer control terminal.

KCLT

In the KCLT field, the LTERM name of the LTERM printer control. If your own terminal is not the printer control terminal, your user ID must have administration privileges.

KCACT

In the KCACT field, if KCOM = CS the action to be performed:

- ON: the printer is unlocked (STATUS = ON);
Unix, Linux and Windows systems
applies globally to the cluster in UTM cluster applications.
- OFF: the printer is locked (STATUS = OFF);
Unix, Linux and Windows systems
applies globally to the cluster in UTM cluster applications.
- CON: set up virtual connection to printer
- DIS: clear virtual connection to printer.

Enter binary zero for all other variants.

KCADRLT

In the KCADRLT field with KCOM = CA, the name of the LTERM partner to which the printer is to be reassigned. The printer is identified by its control ID specified in KCRN. For all other variants binary zero is entered.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area to which UTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

Message area

For KCOM = AI/PI: in the specified message area the message in its actual length but not exceeding the desired length.

KCRLM

In the KCRLM field, the actual length of the message which may differ from the length specified in KCLA of the parameter area.

KCRCCC

In the KCRCCC field, the KDCS return code, see next page.

KCRCDC

in the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KCRMF/kcrfn

in the KCRMF/kcrfn field, if KCOM = AI/PI, the control ID of the next printer which is assigned to the printer control LTERM or blanks if it is the last assigned printer.

KDCS return codes in the KCRCCC field for the PADM call

The following codes can be analyzed in the program:

- 000 Operation carried out (for KCOM = AI/PI) or the administration job is accepted (for KCOM = OK/PR/CA/CS /AT/AC).
- 01Z Length conflict: KCLA < KCRLM, the message is truncated.
- 40Z System cannot perform the operation (generation error or system error, no authorization for this call), see KCRCDC.

Only on Unix, Linux and Windows systems:
The operation is not permitted in a UTM cluster application.
- 42Z Entry in KCOM is invalid.
- 43Z Length entry in KCLA is negative or invalid.
- 44Z Control ID specified in KCRN is invalid or there is no printer with this control ID in the area of the control terminal.
- 46Z Entry in KCLT is invalid because no LTERM printer control has been defined for this name.
- 47Z Message area missing or cannot be accessed in the specified length.
- 49Z Contents of fields not used in the KDCS parameter area not equal to binary zero.
- 55Z Entry in KCACT is invalid.

56Z Entry in KCADRLT is invalid.

An additional return code can be found in the dump:

71Z INIT missing in this program.

Return information in the message area for PADM AI

You can use a language-specific data structure to structure the message area when calling PADM AI. For COBOL this is defined in the KCPADC COPY element and for C/C++ in the *kcpad.h* include file. It has the following structure: No negative confirmation job

Byte	Field name COBOL/C/C++	Meaning	
1 - 8	KCACKCID	Control ID of the printer	
9 - 16	KCGENUID	UTM user ID of the job originator	
17 - 24	KCDPUTID	Job ID (assigned by openUTM)	
25 - 33	KCGENTIM ¹	Time of the FPUT/DPUT call in the form <i>dddhhmss</i> .	
25 - 27	KCGENDOY	<i>ddd</i>	Day of the year (value range 001 - 366)
28 - 29	KCGENHR	<i>hh</i>	Hour (value range 00 - 23)
30 - 31	KCGENMIN	<i>mm</i>	Minute (value range 00 - 59)
32 - 33	KCGENSEC	<i>ss</i>	Second (value range 00 - 59)
34 - 42	KCSTTIM ¹	For time-delayed jobs the required start time <i>dddhhmss</i> .	
34 - 36	KCSTDOY	<i>ddd</i>	Day of the year (value range 001 - 366)
37 - 38	KCSTHR	<i>hh</i>	Hour (value range 00 - 23)
39 - 40	KCSTMIN	<i>mm</i>	Minute (value range 00 - 59)
41 - 42	KCSTSEC	<i>ss</i>	Second (value range 00 - 59)
		Blanks are entered for a job without time delay.	
43	KCPOSMSG	Y	Positive confirmation job
		N	No positive confirmation job
44	KCNEGMSG	Y	Negative confirmation job
		N	No negative confirmation job

¹ For C/C++ the summary fields KCGENTIM and KCSTTIM are not defined. However, the specific fields for day /month/year/working day/hour/minute/second are defined.

If there is no printout to be confirmed, openUTM writes blanks in the message area.

Return information in the message area for PADM PI

You can use a language-specific data structure to structure the message area when calling PADM PI. For COBOL this is defined in the KCPADC COPY element and for C/C++ in the *kcpad.h* include file. It has the following structure:

Byte	Field name COBOL/C /C++	Meaning
1 - 8	KCPRTCID	Control ID of the printer
9 - 11	KCSTATE	Status of the printer: ON or OFF
12	KCCON	Printer connection: Y = printer connected N = printer disconnected
13 - 14	KCPRTMOD	Print mode: AT = automatic mode AC = confirmation mode
15 - 22	KCLTRMNM	LTERM name of the assigned printer
23 - 28	KCFPMSG	Number of output jobs for this printer (without number in KCDPMSG)
29 - 34	KCDPMSG	Number of time-driven jobs pending for this printer whose target time has not yet been reached.

Features of the PADM call

- PADM calls with the modification AT/AC are not executed until the end of the transaction. For the calls PADM OK /PR/CS/CA, a check is made only at the end of the transaction as to whether the call can be executed at all. Thus KCRCCC = 000 after such a call does not necessarily guarantee that the call can be successfully executed, because in the meantime there might be loss of connection to the printer, for example. You can issue a PADM AI or PADM PI call in a subsequent transaction to check whether a PADM OK/PR/CS/CA call has been successful.
- If there is no printout to confirm for a PADM OK/PR call, then PADM OK or PADM PR provides the return code 40Z.
- The printer assignment with PADM CA may only be changed if the two participating LTERMs are not connected with the application at call time, otherwise openUTM responds with 40Z.
- When the printer is locked, openUTM responds with 40Z to reject a PADM CS call designed to set up a connection (KCACT = CON).

7.18 PEND Terminate program unit

You use the PEND (program end) call to terminate a program unit. All UTM program units, including the event services (BADTACS, MSGTAC, SIGNON) must be exited via the PEND call (exception: event exits). Depending on the type of program involved one of the variants of the PEND call is used.

With distributed processing, the PEND calls of job-submitting services and job-receiving services have to be matched, see also chapter [“Program structure in distributed processing”](#).

The abbreviations in the KCOM field are derived from the following terms:

PS	program and sign(on)
PA/PR	program
KP	keep
RE	return
SP	synchronization point
FI	finish
FC	finish and continue
RS	roll back
ER	error
FR	finish and roll back

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area		
	KCOP	KCOM	KCRN
Continue sign-on service after authorization check in follow-up program unit	"PEND"	"PS"	TAC of the follow-up program unit
Continue processing step in the follow-up program unit	"PEND"	"PA"/ "PR"	TAC of the follow-up program unit
Terminate processing step without terminating trans.	"PEND"	"KP"	TAC of the follow-up program unit
Terminate processing step and transaction	"PEND"	"RE"	TAC of the follow-up program unit
Terminate transaction; continue processing step	"PEND"	"SP"	TAC of the follow-up program unit
Terminate processing step, transaction and service	"PEND"	"FI"	—
Terminate transaction and service; continue proc. step in concatenated service	"PEND"	"FC"	TAC of the follow-up program unit
Roll back transaction	"PEND"	"RS"	Blanks
Abort service, roll back the transaction, request dump and restart the application program	"PEND"	"ER"	—
Abort service and roll back the transaction no dump and no application program restart	"PEND"	"FR"	Blanks

i If KCOM = PS/FC/SP/RS, all fields not used in the KDCS parameter area must be set to binary zero.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"PEND"
KCOM	"PS"/"PA"/"PR"/"KP"/"RE"/"FI"/"FC"/"RS"/"ER"/"FR"/"SP"
KCRN	Follow-up transaction code/blank/—

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	—

C/C++ macro calls	
Macro names	Parameters
KDCS_PENDER/KDCS_PENDFI/KDCS_PENDFR/KDCS_PENDRS	()
KDCS_PENDFC/KDCS_PENDKP/KDCS_PENDPA/KDCS_PENDPR/KDCS_PENDPS /KDCS_PENDRE/KDCS_PENDSP	(kcrn)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the PEND call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the PEND operation code.

KCOM

In the KCOM field, the PEND call variants:

- PS: continuation of the sign-on service in a follow-up program
- PR/PA: continuation of the processing step in a follow-up program
- KP: end of the dialog step without transaction end
- RE: end of the dialog step with transaction end
- SP: end of transaction; continuation of the processing step in a follow-up program
- FI: end of service
- FC: end of service with concatenation of services
- RS: transaction rollback (with subsequent service restart if synchronization point exists)
- ER: end of service because of error; the service is terminated abnormally, the transaction is rolled back and a dump is written
- FR: end of service because of error. The service is terminated abnormally, the transaction is rolled back (without dump).

KCRN

In the KCRN field, according to variant

- for PEND KP/RE:
the TAC of the follow-up program unit in which processing should be continued after receiving the next input message.
- for PEND PA/PR/PS/SP:
the TAC of the follow-up program unit in which processing of the same step should be continued.
- for PEND RS/FR:
blanks
- for PEND ER/FI:
irrelevant.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code, see below.

KCRCDC

in the KRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the PEND call

These error codes can only to be found in the dump:

- 000 Operation carried out (with requested PEND ER).
- 70Z Operation PEND cannot be performed (system or generation error, deadlock, timeout), see KRCDC.
- 71Z No INIT entered in this program unit run.

72Z KCOM contains an invalid operation modifier in a call

- in the MSGTAC program
- in the sign-on service
- outside of the sign-on service
- in the server service
- in the asynchronous service

or the operation modifier conflicts with

- the database transaction
- the communication protocol used
- the status of the sign-on service
- waiting for a DGET message

74Z the KCRN field contains a value that is not a TAC or a follow-up TAC

- the user is not authorized to use the TAC
- a switch between a dialog TAC and an asynchronous TAC is pending
- a switch between program units with KDCS API and X/OPEN API is pending
- KCRN does not contain SPACES in a PEND RS,FR
- when waiting for a DGET message, the TAC specified in KCRN is not in a TAC class

81Z KCRN entry in PEND PA/PR/FC/SP/PS (TAC of the follow-up program) conflicts with KCRN in MPUT (e.g. MPUT TAC 1 and PEND xx TAC2).

82Z KCOM or KCRN entry in PEND conflicts with entries in the preceding MPUT:

- MPUT with KCRN=blanks for PEND PA/PR/PS/FC
- MPUT with KCRN=TAC for PEND KP/RE/FI/ER/FR
- MPUT with KCRN=rollback ID and no PEND RS
- MPUT with KCRN=service ID for PEND PA/PR/FI/ER/FR.
- MPUT with KCRN=blanks to an HTTP client and no PEND FI

83Z A MPUT call is missing:

- a dialog program did not issue an MPUT prior to a PEND KP/RE/FI/ER/FR
- no rollback message was sent with MPUT RM prior to a PEND RS in a follow-up transaction
- no MPUT PM issued prior to a program unit terminated with PEND FI in a sign-on service with service restart.

86Z Missing KDCS call in message queuing:

- job complex not terminated at the time of PEND call
- no job associated with DPUT NI call generated
- no asynchronous job sent to a service addressed with APRO AM.

87Z PEND call conflicts with transaction or service status of a remote service.

89Z Contents of fields not used in the KDCS parameter area are not equal to binary zero (only if KCOM = PS/FC /RS/SP).

The table below shows the PEND variants and the associated actions.

Variants	Meaning	openUTM actions
PS	Sign-on service to be continued in follow-up program No synchronization point	<ul style="list-style-type: none"> • Checks authorization data • Possibly executes intermediate dialog to query password/ID card information. • Provides this program unit's MPUT for the follow-up program unit or saves it in the page pool if an intermediate dialog is required. • Takes over the follow-up program unit's TAC from the KCRN field and starts the follow-up program either immediately or on termination of the intermediate dialog.
PA or PR	Processing step to be continued in the follow-up program The transaction remains open No synchronization point	<ul style="list-style-type: none"> • Provides MPUT of this program unit to the follow-up program • Takes TAC of the follow-up program from the KCRN field. When TAC class control is used the follow-up program unit is started immediately if it belongs to the same TAC class, otherwise it is started with delay. If a DGET message is to be waited for, openUTM does not start the follow-up program unit until a message arrives for this queue or is placed back in the queue (redelivery) or if the maximum wait time has expired or if the queue was deleted (see DGET call).
SP	Termination of transaction. However, processing step should be continued in the next program unit. Synchronization point!	<ul style="list-style-type: none"> • Closes DB transaction • Executes DPUT, FPUT, LPUT, PTDA, SPUT and SREL of the transaction. • Deletes the FGET message in the first transaction of an asynchronous service. • Deletes messages processed with DGET from their queues. • Executes MPUT of this program unit • Takes TAC of the follow-up program from KCRN field. When TAC class control is used the follow-up program unit is started immediately if it belongs to the same TAC class, otherwise it is started with delay.
KP	End of the processing step without terminating the transaction. It is to be continued in the next processing step. No synchronization point	<ul style="list-style-type: none"> • Executes MPUT of this program unit (if necessary formats message). • If necessary, takes data in KB and transfers it to the follow-up program as soon as it is initialized. • Takes TAC of the follow-up program from KCRN field and starts follow-up program as soon as the next message arrives.

Variants	Meaning	openUTM actions
RE	<p>End of a processing step and simultaneous end of the transaction.</p> <p>The service is to be continued in a follow-up program.</p> <p>Synchronization point</p>	<ul style="list-style-type: none"> • Closes DB transaction. • Executes DPUT, FPUT, LPUT, PTDA, SPUT and SREL of the transaction. • Deletes the FGET message in the first transaction of an asynchronous service. • Deletes messages processed with DGET from their queues. • Executes MPUT of this program unit (formats message if necessary). • Releases resources. • Takes TAC of the follow-up program unit from KCRN field and starts follow-up program unit as soon as the next message arrives. • If necessary, fetches data from KB and transfers it to the follow-up program unit as soon as it is initialized.
FI	<p>End of service and end of the transaction.</p> <p>Synchronization point!</p>	<ul style="list-style-type: none"> • Closes DB transaction. • Executes DPUT, FPUT, LPUT, PTDA, SPUT and SREL (for GSSB) of the transaction. • Deletes the FGET message in the first transaction of an asynchronous service. • Deletes messages processed with DGET from their queues. • Releases LSSBs of the service. • Executes MPUT of this program unit (formats message if necessary). • Releases resources

Variants	Meaning	openUTM actions
FC	<p>End of service and end of the transaction, the processing step is to be continued in the concatenated service</p> <p>Synchronization point!</p>	<ul style="list-style-type: none"> • Closes DB transaction. • Executes DPUT, FPUT, LPUT, PTDA, SPUT and SREL (for GSSB) of the transaction. • Deletes messages processed with DGET from their queues. • Releases LSSBs of the service. • Transfers MPUT of this program unit to the first program unit of the concatenated service. • Releases resources
RS	<p>Roll back a transaction to the last synchronization point</p>	<p>In the first transaction of a service:</p> <ul style="list-style-type: none"> • Rolls back UTM and DB transaction • Terminates service (with message K034 to the client). • only for terminals and TS applications: Outputs last output message of the preceding service (if available). • Restart asynchronous services and follow-up services (if chained services are used) following a rollback. <p>In a follow-up transaction of service:</p> <ul style="list-style-type: none"> • Rolls back UTM and DB transaction to the last synchronization point and, if necessary, restarts screen with message K034. • Starts the program unit addressed at the last synchronization point. • Transfers rollback message to this program unit. <p>For all the transactions in a service:</p> <ul style="list-style-type: none"> • Messages processed with DGET can be processed again if the maximum number of redeliveries specified in the generation has not yet been reached. Otherwise they are deleted or, in the case of TAC queue messages, may be saved in the dead letter queue. • If PGWT calls are allowed for the current TAC and the PEND RS was not called by the program unit: Restarts application program

Variants	Meaning	openUTM actions
ER (ERror)	End of service with dump and restart of the application program Rollback to last synchronization point (exception: MPUT)	<ul style="list-style-type: none"> • Writes the UTM dump. • Rolls back the UTM and DB transaction. • Messages processed with DGET can be processed again if the maximum number of redeliveries specified in the generation has not yet been reached. Otherwise they are deleted or, in the case of TAC queue messages, may be saved in the dead letter queue. • In the first transaction of an asynchronous service: The FGET message can be processed again if the maximum number of redeliveries specified in the generation has not yet been reached. Otherwise it is deleted or may be saved in the dead letter queue. • Causes dump of the application program. • Executes MPUT of this program unit (formats message if necessary) • Restarts application program. • Releases resources.
FR	End of service, no dump, the application program remains loaded Rollback to last synchronization point (exception: MPUT)	<ul style="list-style-type: none"> • Rolls back the UTM and DB transaction. • Messages processed with DGET can be processed again if the maximum number of redeliveries specified in the generation has not yet been reached. Otherwise they are deleted or, in the case of TAC queue messages, may be saved in the dead letter queue. • In the first transaction of an asynchronous service: The FGET message can be processed again if the maximum number of redeliveries specified in the generation has not yet been reached. Otherwise it is deleted or may be saved in the dead letter queue. • Executes MPUT of this program unit (formats message if necessary) • Releases resources.

Features of the PEND call

- Following a PEND, no branch is made back to the calling program. Thus, the KDCS return code cannot be evaluated there.
- In case of error, if PEND executes abnormally, openUTM calls PEND ER internally.
 - With dialog processing, an error message is sent to the client. The transaction is rolled back and the service is terminated. A new service can be started.
 - An asynchronous service is aborted and a message is written to the system log file SYSLOG.
- If another call led to a KDCS return code $\geq 70Z$, openUTM calls PEND ER internally.

- If a program unit calls PENDING/FR in a dialog service, you must first use MPUT to send a message to the client or the job-submitting service - with one exception: This does not apply to a OSI TP job-submitting service for which KCSSEND contains the value "N". If openUTM calls PENDING internally (KCRCCC >= 70Z), a default message is issued. However, if a separate error message was created by means of MPUT ES in communication with the UPIC client, this error message is sent to the UPIC client instead.
- A rollback message has to be sent with MPUT RM prior to a PENDING call in a follow-up transaction. Thus a PENDING should not be issued in the first transaction of a service otherwise no rollback message can be read. Unlike PENDING, PENDING does not cause a dump to be written.
- If the PENDING call is used for communication with a UPIC client, you must note the following:
 - If the preceding transaction was terminated with PENDING SP or PENDING FC, then the local transaction is rolled back and the service with the follow-up program unit specified in PENDING SP or PENDING FC continues execution when PENDING is called.(local service restart)
 - If the preceding transaction was **not** terminated with PENDING SP/FC and the service is running under a user ID **with** the restart property, then the service is rolled back to the last synchronization point and the dialog with the UPIC client is terminated. A new OSI TP dialog can be started under the user ID and the service restart requested.
 - In all other cases, openUTM terminates the service with PENDING FR.
- If PENDING is used for distributed processing via the OSI TP protocol without commit functionality, you must note the following:
 - if called in a job-receiving service:
 - If the preceding transaction was terminated with PENDING SP, then the local transaction is rolled back and the service with the follow-up program unit specified in PENDING SP continues execution when PENDING is called (local service restart). If the preceding transaction was **not** terminated with PENDING SP and the service is running under a user ID **with** the restart property, then the service is rolled back to the last synchronization point and the dialog with the UPIC client is terminated. A new OSI TP dialog can be started under the user ID and the service restart requested.
 - In all other cases, openUTM terminates the service with PENDING FR.
 - if called in a job-submitting service, all job-receiving services of this service are terminated using PENDING FR.
- If a PENDING call is issued in a transaction previously terminated with PGWT CM, the service is terminated with PENDING FR.
- Any messages or message segments which openUTM maintained for the program following INIT, but which were not read in the program with MGET or FGET, are lost with PENDING (likewise with PENDING PA or PR). The same applies when no all of a DGET message is read: the remaining parts of the message that were not read are lost.
- If a DB transaction was terminated prior to a PENDING RE/SP/FI/FC, execution is delayed until PENDING RE/SP/FI/FC.
- PENDING KP locks resources (LSSBs, GSSBs, TLS, ULS and, if applicable, database areas) beyond a dialog step. Except in the case of distributed processing, it is therefore advisable
 - to use the PENDING KP sparingly in order to keep global resource occupancy times short
 - not to reserve the global resources until the final dialog step when using PENDING KP.

-
- If the transaction is rolled back then any MPUT output to be performed by a PEND KP is lost. The service is rolled back to the last synchronization point. A service restart is performed immediately provided that the user is still signed on.

If the user is signed off, e.g. because the connection to the client has been lost, then a service restart is performed when the user signs on provided that the user ID (in applications without user IDs, the LTERM partner) has been generated with the restart property (generation operand RESTART=YES in the LTERM or USER statement, see openUTM manual “Generating Applications”).

Following the end of an application then, in the case of standalone UTM applications, a service restart is only possible in UTM-S applications.

- PEND SP is only permitted in distributed processing via LU6.1 if no partner services with open transactions are available.
- If a message to an HTTP client has been issued, the service has to be terminated with PEND FI because a service for an HTTP client may only consist of one dialogue step.
- A PEND PA/PR or SP can cause a task switch in a dialog or asynchronous service if the follow-up program unit is in a different TAC class than the program unit run calling PEND (see the openUTM manual “Generating Applications”, TAC classes), or if the application was generated with the TAC-PRIORITIES statement.
- A PEND PS call may only be specified in the sign-on service and only if the status of the sign-on service allows this.
- If the PEND PA/PR or PS call is executed without calling MPUT beforehand in the signon service for a UPIC client after receiving a message from the client, then the follow-up program unit can still read unread message (segments) from the UPIC client.
- PEND FC terminates the UTM service, but not the UPIC conversation. If the PEND PA/PR or PS call is executed without calling MPUT beforehand in the signon service for a UPIC client after receiving a message from the client, then the follow-up program unit can still read unread message (segments) from the UPIC client. In this case the first program unit of the chained service receives the value F (first), and not C (chained) as its service indicator in the KBKOPF because it contains a message from the client.
- If an asynchronous service or a follow-up service concatenated with PEND FC is interrupted during the first transaction, then openUTM restarts the service.
- Program unit runs in asynchronous services can only use PEND KP and RE if they have previously supplied a message for a job-receiving service with MPUT.
- Note that, if PEND ER/FR is called in the job-receiving service, you cannot send a message to the job-submitting service (as with PEND ER/FR to the terminal). Nevertheless, you have to issue an MPUT call before a PEND ER /FR as otherwise openUTM terminates the service. The job-submitting service then receives status information with service status Z (instead of E).
- When using distributed processing, you have to take account of the service and transaction status of the partner when calling PEND. For further information see chapter “[Program structure in distributed processing](#)”.
- If a DGET message is to be waited for, PEND PA/PR or PGWT PT must follow.

7.19 PGWT Set wait point in program without terminating program unit

The PGWT call (program wait) sets the program unit to an internal wait point **without** terminating the unit. You can

- terminate the processing step without terminating the transaction.
- neither terminate the processing step nor the transaction in order to wait for a message at a service-controlled message queue (no previous MPUT permitted).
- terminate the transaction. If an MPUT message was sent previously, the processing step is terminated; otherwise, it is continued.
- roll back the transaction and continue the processing step.

The program unit is always continued by the same process (process ID remains the same). The PGWT call is comparable to a PEND call followed by an implicit INIT call.

If you enter a value greater than 0 for the parameter KCLI in the KDCS parameter area, then openUTM supplies information about the application, the system and the communication partner. The PGWT call is then comparable to a PEND KP call followed by an implicit INIT PU call.

The following table shows the meaning of the PGWT call and the associated actions:

Variant	Meaning	openUTM actions
PGWT KP	End of processing step without program unit or transaction end; if necessary request information (KCLI > 0)	<ul style="list-style-type: none"> • Send MPUT message • Continue program as soon as response received • For KCLI > 0: Make requested information available in message area
PGWT PR	Wait without terminating processing step, program unit or transaction; if necessary request information (KCLI > 0)	<ul style="list-style-type: none"> • Continue program as soon as there is a message at the queue • For KCLI > 0: Make requested information available in message area
PGWT CM	Terminate transaction without terminating the program unit; if necessary request information (KCLI > 0)	<ul style="list-style-type: none"> • If MPUT was issued: Send MPUT message and continue program as soon as response received. • Without MPUT: Continue processing without waiting, exception for OSI TP see "PGWT call in a distributed OSI TP service with Commit". • For KCLI > 0: Make requested information available in message area
PGWT RB	Roll back transaction; if necessary request information (KCLI > 0)	<ul style="list-style-type: none"> • Roll back transaction • Continue processing, exception for OSI TP see "PGWT call in a distributed OSI TP service with Commit". • For KCLI > 0: Make requested information available in message area

i On all PGWT calls, the local process continues to be occupied during the waiting time or during the communication. In addition, resources continue to be locked on PGWT KP/PR calls. You should therefore only use PGWT calls sparingly and when they are genuinely necessary.

Setting the KDCS parameter area (1st parameter)

Function of the call	Entries in the KDCS parameter area		
	KCOP	KCOM	KCLI
Terminate processing step without end of program unit or transaction	"PGWT"	"KP"	0 / Length of the message area
Wait without terminating processing step and transaction	"PGWT"	"PR"	0 / Length of the message area
Terminate transaction without end of program unit	"PGWT"	"CM"	0 / Length of the message area
Roll back transaction and continue processing step	"PGWT"	"RB"	0 / Length of the message area

Setting the 2nd parameter (only necessary if KCLI > 0)

Here you enter the address of the message area into which openUTM is to write the requested information. To structure the message area you can use the same data structure as for the INIT PU call, i.e. the KCINIC COPY element for COBOL, the *kcini.h* include file for C/C++.

In the header of the data structure, you specify the version number of the structure and select which information openUTM is to supply.

For a detailed description of the data structure, see the INIT PU call, "[INIT Initialize program unit](#)".

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"PGWT"
KCOM	"KP"/"PR"/"CM"/"RB"
KCLI	0/Length in bytes

Setting the header of the message area (only necessary if KCLI > 0)	
Field name in message area	Contents
KCVER/if_ver	Version number (7)
KCDATE/dattim_info	Request date and time (Y/N)
KCAPPL/appl_info	Request application information (Y/N)
KCLOCALE/locale_info	Request Locale information (Y/N)
KCOSITP/ositp_info	Request OSI TP information (Y/N)
KCENCR/encr_info	Request encryption information (Y/N)
KCMISC/misc_info	Request miscellaneous information (Y/N)
KCHTTP/http_info	Request HTTP information (Y/N)

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area (only necessary if KCLI > 0)

C/C++ macro calls	
Macro names	Parameters
KDCS_PGWTKP	()
KDCS_PGWTKP_PU / KDCS_PGWTPR/ KDCS_PGWTCM / KDCS_PGWTRB	(nb,kcli)

openUTM return information	
Message area	Contents
	Data (only if KCLI > 0)
Field name in KB return area	
KCRLM	Length of transferred data (only if KCLI > 0)
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcrfn	Format identifier/blanks
KCRPI	Service ID/Rollback ID/blanks

For the PGWT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, enter the "PGWT" operation name.

KCOM

In the KCOM field, the variant of the PGWT call:

- KP: End of processing step without transaction end
- PR: Wait without terminating the processing step and transaction
- CM: End of the transaction
- RB: Rollback of the transaction

KCLI

in the KCLI field, enter the length of the message area to which openUTM is to transfer the information. Enter the length in bytes. The value entered in KCLI specifies the maximum number of bytes of information that openUTM transfers to the message area.

If KCLI is greater than zero, then you must specify the address of the message area in the 2nd parameter when you call PGWT. The information is equivalent to that for the INIT PU call.

All unused fields of the parameter area must contain binary zero.

Setting the header of the message area (only necessary if KCLI > 0):

KCVER/if_ver

In the KCVER/if_ver field, enter the version number of the data structure. The current version is version 7.

KCDATE/dattim_info

Enter Y in the KCDATE/dattim_info field if you want information on the date and time of the start of the application and the program unit run, otherwise enter N.

KCAPPL/appl_info

Enter Y in the KCAPPL/appl_info field if you want to request information about the application, system and communication partner, otherwise enter N.

KCLOCALE/locale_info

Enter Y in the KCLOCALE/locale_info field if you to want to request information about the language environment of the LTERM partner, otherwise enter N.

KCOSITP/ositp_info

Enter Y in the KCOSITP/ositp_info field if you require OSI TP-specific information, otherwise enter N.

KCENCR/encr_info

Enter Y in the KCENCR/encr_info field if you require information about the encryption methods used between the client and the UTM application, otherwise enter N. (The encryption mechanism can be coordinated. See the openUTM manual "Generating Applications".)

KCMISC/misc_info

Enter Y in the KCMISC/misc_info field if you require miscellaneous information (e.g. number of queued messages in the user's queue, password validity, time of last signon), otherwise enter N.

KCHTTP/http_info

Enter Y in the **KCHTTP/http_info** field if you require HTTP specific information, otherwise enter N.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

(only necessary if KCLI is not equal to 0): The address of the message area to which openUTM is to write information. For return information you can use the KCINIC data structure in COBOL and the *kcini.h* include file in C/C++ (description see ["INIT Initialize program unit"](#)).

Macro names

The use of C/C++ macro calls is described in detail in the section ["C/C++ macro interface"](#).

openUTM returns:

Message area

only if KCLI > 0:

in the message area, the information in its actual length, up to a maximum length of the value specified in KCLI. The data supplied by the PGWT call corresponds to the return information of the INIT PU call and is described on ["INIT Initialize program unit"](#).

KCRLM

only if KCLI > 0:

in the **KCRLM** field, the length of the information actually transferred by openUTM, provided that KCRCCC = 000. In the case of 07Z, KCRLM contains the length of data which is totally available. If KCRCCC >= 40Z then KCRLM = 0.

KCRCCC

in the KCRCCC field, the KDCS return code (length 3 bytes). For possible return codes and their meaning, see below.

KCRCDC

in the KRCDC field, the internal return code of openUTM (see openUTM manual "Messages, Debugging and Diagnostics").

KCRMF/kcrfn

only for PGWT CM with preceding MPUT and PGWT KP (similar to the INIT call):

- for a message from a terminal:

Blanks (in line mode) or the format name (in format mode) of the last screen output, i.e. the name specified in the KCMF/kcfn field with the MPUT of the last dialog step. If the last output consisted of multiple partial formats, KCRMF/kcrfn contains the name of the first partial format into which data was entered. If no data was entered in any of the partial formats, KCRMF/kcrfn contains the name of the first partial format.

Only on BS2000 systems: If an edit profile was used in the last screen output, KCRMF/kcrfn contains this edit profile.

- for a message from a TS application: Blanks
- for a message from a LU6.1 partner or a UPIC client:

The format identifier of the first message segment specified by the LU6.1 partner or UPIC client on sending Particularity in the LU6.1 job submitting service:Blanks blanks if a status flag exists for the service ID specified in KCRPI.

- for distributed processing via OSI TP:

If the program unit run was started because of a distributed dialog, KCRMF/kcrfn in the job-submitting service contains the name of the abstract syntax which was allocated to the message by the job submitter; if the field contains blanks, the UTD syntax is selected as the abstract syntax.

In the job-receiving service, KCRMF/kcrfn contains the name of the abstract syntax which was allocated to the message by the job-receiving service described in KCRPI. If the field contains blanks, the UTD syntax is selected as the abstract syntax or an error message from the partner is present.

KCRPI

only for PGWT CM with preceding MPUT and PGWT KP (similar to the INIT call):

- For a message from a LTERM partner: blanks.
- In the job-submitting service with distributed processing:
the service ID of the job-receiving service if a message from the job receiver exists.

-
- In the job-receiving service with distributed processing:
blanks

KDCS return codes in the KCRCCC field for the PGWT call

The following codes can be analyzed in the program:

- 000 Operation carried out successfully. If a message area was specified for the call (KCLI > 0), the requested information was transferred to the message area in its full length.
- 07Z Function was executed, the available message area is too short (Length in KCLI insufficient). No or incomplete information was returned.
- 40Z For PGWT CM: The function was not executed. An error that does not permit continuation of the current transaction has occurred. The transaction is rolled back implicitly with PGWT RB.
- 48Z Only when KCLI is greater than zero: Invalid data structure version.

Additional return codes can be found in the dump:

- 70Z The PGWT operation could not be performed (system or generation error, deadlock, timeout).
- 71Z In this program no INIT has yet been issued or the call was issued by an MSGTAC program.
- 72Z Entry in KCOM is invalid or KCOM = CM/RB was specified and a partner communicating with the LU6.1 protocol is involved in the current distributed transaction.
- 77Z The address of the message area specified when the call was issued is invalid.
- 82Z An MPUT was issued to a program unit run before a PGWT KP.
- 83Z The program unit did not issue an MPUT before a PGWT KP or an MPUT was issued before a PGWT PR.
- 87Z The PGWT call conflicts with the transaction or service status.
- 88Z Interface version of the data structure (for KCLI > 0) is invalid.
- 89Z When the function was called, unused parameters were not set to binary zero.

Features of the PGWT call

- Any messages or message segments which are held by openUTM for the program following INIT and which are not read by the program using MGET are lost.
- PGWT KP and PR

-
- A PGWT KP call corresponds to a PEND KP with a following INIT/INIT PU. PGWT KP is always allowed, if a PEND KP call is allowed.
 - A PGWT PR call corresponds to a PEND PA/PR with a following INIT/INIT PU. PGWT PR is meaningful only if preceded by a DGET call with wait and if it is necessary to wait for a message for the specified queue. After PGWT PR the program waits until a message arrives for this queue.
 - PGWT KP and PR do not produce a synchronization point! Dialog messages initiated by MPUT for PGWT KP calls are output. The remaining output operations LPUT, FPUT, SPUT, PTDA and the release action SREL remain stored until the next synchronization point.
 - PGWT KP and PR lock resources (LSSBs, GSSBs, TLS, ULS, and possibly database areas) outside the processing dialog step. Calls from other transactions (SGET, SPUT, SREL, PTDA or GTDA) that wish to access these resources are rejected with a return code (40Z and KCR CDC code). Therefore, it is recommended when using PGWT KP/PR to first allocate the global resources before use, and to release them again immediately afterwards.
 - If a DB transaction began prior to a PGWT KP or PR, this transaction is not terminated! The transaction is only terminated if a PEND RE, SP, FI, FC or a PGWT CM call is issued. RSET, PEND, RS FR, ER or PGWT RB roll back the transaction.
 - If the transaction is rolled back then any MPUT output to be performed by a PGWT KP is lost. The service is rolled back to the last synchronization point. A service restart is performed immediately provided that the user is still signed on. If the user is signed off, e.g. because the connection to the client has been lost, then a service restart is performed when the user signs on provided that the user ID (in applications without user IDs, the LTERM partner) has been generated with the restart property (generation operand RESTART=YES in the LTERM or USER statement, see openUTM manual "Generating Applications").
Following the end of an application then, in the case of standalone UTM applications, a service restart is only possible in UTM-S applications.
 - PGWT CM and RB
 - PGWT CM with an MPUT message is always allowed whenever a PEND RE is allowed. PGWT CM then corresponds to PEND RE with a following INIT/INIT PU.
 - PGWT CM without an MPUT message is always allowed whenever a PEND SP is allowed. PGWT CM then corresponds to PEND SP with a following INIT/INIT PU.
 - PGWT CM sets a synchronization point while preserving the program context. With regard to database transactions PGWT CM behaves in the same way as PEND SP or PEND RE.
 - PGWT CM and PGWT RB are not allowed if the LU6.1 protocol is used for communication with a partner in the current transaction.
 - PGWT RB rolls back the transaction. In contrast to RSET or PEND RS the program context is preserved. The program context includes, for example, the KB program area, SPAB and local data areas.
 - No rollback message may be generated before PGWT RB.
 - No service restart is possible at a synchronization point set using PGWT CM. The follow-up transaction can therefore be rolled back only with PGWT RB without terminating the abnormal service.
 - If the PGWT call cannot be executed successfully, openUTM calls PEND ER internally.
 - Continuation of processing

-
- After a PGWT KP call or a PGWT CM call with MPUT a return is made to the calling program as soon as all responses are available.
 - Processing is continued immediately after a PGWT CM without MPUT and after a PGWT RB, exception see distributed processing with OSI TP on "[PGWT Set wait point in program without terminating program unit](#)".
 - After a PGWT PR call processing is continued as soon as a message arrives in the queue. A DGET call must be used to read such messages.

i Use this call sparingly, because the task remains occupied and cannot process any other job during the wait period. This applies especially if the PGWT call is waiting for an entry from a terminal. In this case, the task is blocked until an entry is input via the keyboard!

PGWT call in a distributed OSI TP service with Commit

If the Commit functionality was selected with distributed processing via OSI TP, PGWT CM without MPUT and PGWT RB **always** result in a wait point, i.e.:

- for PGWT CM without MPUT, processing is not continued until the transaction end has been confirmed by all partners or the transaction has been rolled back, e.g. due to an error.
- for PGWT RB, processing is not continued until rollback has been confirmed by all partners.

A return is also made to the program unit if

- for an PGWT KP call, a situation is detected which makes it impossible to commit the transaction.
- for a PGWT CM or RB call, the current transaction was committed or rolled back and the present situation does not allow the current transaction or the follow-up transaction to be committed.

This situation is indicated to the program via the KCTARB field in the KB header:

KCTARB

In an TP service this indicates whether a situation has occurred which makes it necessary to roll back the transaction.

Blanks No situation has occurred which makes it necessary to roll back the transaction.

Y A situation has occurred which makes it impossible to commit the transaction. Communication with partner services is still permitted. A call to commit the transaction results in an abnormal end of service.

7.20 PTDA Write to TLS

You use the PTDA (put data) call to write a block from a specified storage area to a terminalspecific long-term storage area (TLS) of an LTERM/LPAP/OSI-LPAP/Master-LPAP partner.

A program unit run of a dialog service can only write to blocks of its “own” TLS, i.e. blocks of the LTERM/LPAP/OSI-LPAP partner, via which the service was started.

A program unit run of a asynchronous service can write to the blocks of any LTERM/LPAP/OSI-LPAP/Master-LPAP partner of the UTM application.

Setting the 1st parameter (KDCS parameter area)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area			
	KCOP	KCLA	KCRN	KCLT
Write to a TLS block (in the dialog program)	"PTDA"	Length	Block name	—
Write to TLS (in the asynchronous program)	"PTDA"	Length	Block name	LTERM / LPAP / OSI-LPAP / Master-LPAP name

Setting the 2nd parameter

Here you have to supply the address of the message area which contains the message to be written.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"PTDA"
KCLA	Length in bytes
KCRN	Block name
KCLT	Name of LTERM / LPAP / OSI-LPAP / Master-LPAP partner
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro call	
Macro name	Parameters
KDCS_PTDA	(nb,kcla,kcrn,kclt)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the PTDA call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the "PTDA" operation code.

KCLA

In the KCLA field, the length of the data which openUTM is to write to the TLS. The length specified here becomes the new length of the TLS block.

KCRN

In the KCRN field, the name of the TLS block to which openUTM is to write the data.

KCLT

Only for asynchronous programs: in the KCLT field, the name of the LTERM/LPAP/OSI-LPAP/Master-LPAP partner containing the TLS to which openUTM is to write data (this field is not evaluated by dialog programs).

Message area

In the message area you enter the message which you want to write to the TLS

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area from which openUTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code, see below.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the PTDA call

The following codes can be analyzed in the program:

- 000 Function carried out.
- 40Z System cannot perform the operation (generation error or system error, deadlock, timeout), see KCRCDC.
- 41Z Call issued in the first segment of the sign-on service, although this is not allowed by the generation.
- 43Z Length entry in KCLA is negative or invalid.
- 44Z Name of the block in KCRN is unknown or invalid.
- 46Z LTERM/LPAP/OSI-LPAP/Master-LPAP name in KCLT is invalid (only for asynchronous programs).
- 47Z Message area missing or cannot be accessed in the specified length.

An additional return code can be found in the dump:

- 71Z No INIT issued in this program.

Features of the PTDA calls

- At the end of transaction (PEND RE/FI/FC/SP), the changes made to the TLS block are carried out and the block is unlocked. Other transactions can then make use of it again. With PEND RS/ER/FR or RSET the changes made to the TLS blocks are cancelled and the blocks are unlocked.
- The lock may apply for a longer period in the following cases:
 - PEND KP and PGWT KP
 - PEND PA/PR with a task change due to TAC class control
 - PEND PA/PR with waiting for a DGET message
- A PTDA call locks access to a TLS block until the next synchronization point. No other TLS blocks of the addressed LTERM/ LPAP/ OSI-LPAP partner are locked.

Note that the current length of a TLS block is the length in which it was written with the last PTDA call.

How UTM reacts when the desired TLS block is locked is described in the section ["Action with locked storage areas \(TLS, ULS and GSSB\)"](#).

7.21 QCRE Create temporary queue

The QCRE (queue create) call is used to create a temporary queue dynamically.

The prerequisite for a successful QCRE call is that enough table spaces for QUEUE objects must have been reserved at generation by means of the QUEUE statement.

In the QCRE call you can either assign a name for the queue to be created or specify that openUTM assigns a name automatically, which is then entered in the KCRQN (queue name) return field.

openUTM creates queue names that follow on from each other from printable digits. If the queue names are assigned by openUTM, the same queue name is not used again for 100 million QCRE calls. This ensures that long-running services for communication do not inadvertently use a temporary queue whose name has been reassigned after being deleted.

The format of the QCRE call is described in detail below. You will find more information on the subject of “message queuing” in section “[Message Queuing \(asynchronous processing\)](#)”.

Setting the KDCS parameter area (1st parameter)

The following table shows the entries required in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area					
	KCOP	KCOM	KCRN	KCLA	KCMF /kcfn	KCQMODE
Create queue without name	"QCRE"	"NN"	Blanks	Queue level	Blanks	"S" / "W" / binary zero
Create queue with name	"QCRE"	"WN"	Queue name	Queue level	Blanks	"S" / "W" / binary zero

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"QCRE"
KCOM	"NN"/"WN"
KCRN	Blanks / name of the queue
KCLA	Queue level of the queue
KCMF / kcfn	Blanks
KCQMODE	"S" / "W" / binary zero

KDCS call	
1st parameter	
KDCS parameter area	

C/C++ macro call	
Macro names	Parameters
KDCS_QCRENN	(kcla,qmode)
KDCS_QCREWN	(kcla,kcrn,qmode)

openUTM return information	
Field name in the KB return area	Contents
KCRQN	Name assigned by openUTM
KCRCCC	Return code

In the KDCS parameter area you make the following entries for the QCRE call:

KCOP

In the KCOP field, enter the QCRE operation code.

KCOM

In the KCOM field:

- NN (no name)
if openUTM is to create the name of the queue automatically
- WN (with name)
if you assign the name yourself

KCRN

In the KCRN field, enter the name of the queue (KCOM=WN) or blanks (KCOM=NN). A name you assign must not begin with a digit and must adhere to the conventions for generatable names. In other words, it can consist only of the characters A...Z, a...z, 0...9, \$, #, @. If necessary, it must be filled with blanks.

KCLA

In the KCLA field, enter the queue level. In other words, you enter the maximum number of messages that can be stored in this queue.

If you specify zero, openUTM uses the value or default value of the QLEV parameter from the QUEUE statement of the generation.

KCMF / kcfn

The KCMF/kcfn field must be supplied with blanks.

KCQMODE

In the KCQMODE field:

- S (standard)
if further messages are to be rejected when the queue level is reached
- W (wrap)
if a new message overwrites the oldest existing message when the queue level is reached
- Binary zero
openUTM uses the value or default value of the QMODE parameter from the QUEUE statement of the generation.

In the KDCS call, specify:

1st parameter

The address of the KDCS parameter area.

Macro names

How to use macro calls for C/C++ is described in detail in the section [“C/C++ macro interface”](#).

openUTM returns:

KCRQN

in the KCRQN field the name generated automatically (when KCOM=NN).

KCRCCC

in the KCRCCC field the KDCS return code (see next page).

KDCS return codes in the KCRCCC field for the QCRE call

The following codes can be analyzed in the program:

000 The operation was executed.

16Z KCOM=WN: The queue name already exists.

KCOM=NN: openUTM could not find a free name. In this case, you can try to find a free queue name with another QCRE NN call.

Note on name assignment:

openUTM assigns names consisting only of digits and remembers the last name it assigned. When QCRE is specified with KCOM=NN, openUTM searches the next 100 names consisting of digits for a free entry. If these names are all occupied, openUTM terminates the search with 16Z. At the next QCRE NN call, the next 100 names are searched.

40Z The operation cannot be executed because:

- there is no free table space left for temporary queues
(what to do: increase the value for NUMBER in the QUEUE statement and regenerate, or use QREL to delete temporary queues that are no longer required).
- because there is no free table space left in the process-specific buffer for restart data
(what to do: increase the value of MAX RECBUF=(..., *length*) and regenerate).

42Z The value in KCOM is invalid.

43Z The value in KCLA (queue level) is negative or invalid.

44Z The queue name begins with a digit (KCOM=WN), or KCRN does not contain any blanks (KCOM=NN).

45Z KCMF/kcfn was not supplied with blanks.

46Z The value in KCQMODE is invalid.

49Z Unused fields have a value other than binary zero.

An additional return code can be found in the dump:

71Z An INIT has not yet been called in the program unit run.

Features of the QCRE call

- No administration authorization is required to create a temporary queue.
- If the queue names are assigned by openUTM, they are not used again for 100 million QCRE calls.
- If a temporary queue is created with QCRE, messages can be written in this queue in the same transaction. However, these messages cannot be read and administered until the transaction is successfully completed.
- In the case of UTM-S, temporary queues and their messages are preserved after the end of the application run until they are deleted explicitly by means of a QREL call. In the case of UTM-F, temporary queues are deleted automatically at the end of the application run. All the messages still stored in the queue are lost.

7.22 QREL Delete temporary queue

The QREL (queue release) call is used to delete a temporary queue dynamically.

All the messages in the queue are deleted, and the name and the table space of the queue are made available.

Services that wait for DGET messages of this queue are continued.

The format of the QREL call is described in detail in the following. You will find more information on the subject of message queuing in section [“Message Queuing \(asynchronous processing\)”](#).

Setting the KDCS parameter area (1st parameter)

The following table shows the entries required in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area			
	KCOP	KCOM	KCRN	KCMF/kcfn
Delete temporary queue	"QREL"	"RL"	Name of the queue	Blanks

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"QREL"
KCOM	"RL"
KCRN	Name of the queue
KCMF/kcfn	Blanks

KDCS call	
1st parameter	
KDCS parameter area	

C/C++ macro call	
Macro names	Parameters
KDCS_QRELRL	(kcrn)

openUTM return information	
Field name in the KB return area	Inhalt
KCRCCC	Return code

In the KDCS parameter area, make the following entries for the QREL call:

KCOP

In the KCOP field, enter the QREL operation code.

KCOM

In the KCOM field, enter the RL modifier.

KCRN

In the KCRN field, enter the name of the queue to be deleted.

KCMF/kcfn

The KCMF/kcfn field must be supplied with blanks.

For the KDCS call, specify:

1st parameter

The address of the KDCS parameter area.

Macro names

How to use macro calls for C/C++ is described in detail in the section [“C/C++ macro interface”](#).

openUTM returns:

KCRCCC

in the KCRCCC field the KDCS return code (see below).

KDCS return codes in the KCRCCC field for the QREL call

The following codes can be analyzed in the program:

- 000 The operation was executed.
- 40Z There is no more space in the process-specific buffer for restart data.
Bottlenecks can result because openUTM executes a separate DADM call for each message read by means of DGET in a transaction that is not yet completed and has to write a processing item to the buffer.
What to do: Increase the value of MAX RECBUF=(..., *length*) and regenerate.
- 42Z The value in KCOM is invalid.
- 44Z There is no temporary queue with the name specified in KCRN.
- 45Z KCMF/kcfn was not supplied with blanks.
- 49Z Unused fields (except KCMF) have a value other than binary zero.

An additional return code can be found in the dump:

- 71Z An INIT has not yet been called in the program unit run.

Features of the QREL call

- No administration authorization is required to delete a temporary queue.
- After the QREL call, messages in the deleted queue can no longer be read or administered. New messages cannot be created for this queue.
- After a QREL call and the successful conclusion of the transaction, a new temporary queue can be created with the same name.

7.23 RSET Roll back transaction

You use the RSET (roll back transaction) call to roll back changes and operations of local transactions. Open database transactions are also rolled back. All output operations since the last local synchronization point are cancelled. Control is returned to the program unit. The program unit is continued after the RSET call. Further KDCS calls and database calls are subsequently possible (except INIT).

You can use the RSET call to react to application errors with specific actions. You can roll back a transaction and at the same time pass control back to the application program.

This approach is useful for errors which are not program errors (e.g. as a response to error codes $\geq 40Z$). You can react specifically in the program unit, e.g. by

- sending a message to the appropriate client or to the administrator (MPUT)
- writing an item of logging information (LPUT)
- sending an output job, e.g. to a printer (FPUT/DPUT)

The RSET call may, for example, also be useful in the event that database accesses yield unexpected return codes (e.g. “data record does not exist”) and UPDATE operations have already been performed.

Setting the 1st parameter (KDCS parameter area)

For the RSET call, you only have to enter the “RSET” operation code in the KCOP field.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"RSET"

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	—

C/C++ macro calls	
Macro name	Parameters
KDCS_RSET	()

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the RSET call you make the following entries in the KDCS parameter area:

KCOP

in the KCOP field, the RSET operation code.

openUTM does not evaluate any other operands of the parameter area.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro name

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the RSET call

The following codes can be analyzed in the program:

000 Operation carried out

Additional return codes can be found in the dump:

70Z System cannot perform the operation (generation error or system error), see KCRCDC.

71Z INIT missing in this program.

Features of the RSET call

- All resources occupied by this transaction up to the RSET call are released.
- All service-specific data is rolled back to the last synchronization point. In this way, the KB program area, all LSSBs and GSSBs and TLS and ULS blocks are again made available with their original contents.
- Data in SPAB and in program-specific working storage areas is not changed.
- An open DB transaction is rolled back.
- Each rollback of a DB transaction has the same effect as an RSET call, and thus implicitly causes the UTM transaction to be rolled back.
- The program unit again regains control following the RSET call and continues the program run with the next statement after the RSET call. It is then possible to issue additional KDCS (except INIT) and DB calls in the program unit.

-
- After this, it is no longer possible to read a dialog input message which was read prior to the RSET call, but it is possible to read a dialog input message which was not yet read prior to the RSET call.
 - Input messages read with FGET or DGET can again be read following an RSET. With DGET messages this is possible only if the maximum number of redeliveries specified at generation has not been reached. For more information refer to the openUTM manual “Generating Applications”, REDELIVERY operand in the MAX control statement.

If the maximum number of redeliveries has been reached then the message is either deleted or saved in the dead letter queue by UTM (only possible in the case of messages to a TAC queue), see openUTM manual “Generating Applications”, DEAD-LETTER-Q operand in the TAC statement.

Features of the RSET call with distributed processing

The behavior of openUTM following an RSET call in a program unit run belonging to a distributed transaction is governed by the RSET generation parameter of the UTMD statement (see the openUTM manual “Generating Applications”):

- If RSET=LOCAL is generated, then the RSET call has no effect on the distributed transaction. Here, inconsistencies may occur in the distributed databases, if some of the local transactions participating in the distributed transactions are continued and others rolled back. With this generation, the global data consistency is no longer guaranteed by the relevant system components, but is the responsibility of the application program units. These must decide the situations in which it is more practical to terminate the distributed transaction and the situations in which it must be rolled back.
- If RSET=GLOBAL is generated, then openUTM forces termination of the program unit run with a PEND variant which causes the distributed transaction to be rolled back (see also the section "[PEND Terminate program unit](#)").

7.24 SGET Read from secondary storage area

You use the SGET (storage get) call to read data from a secondary storage area into a storage area of the program unit. The following may occur as secondary storage areas:

- the global secondary storage area (GSSB)
- the local secondary storage area (LSSB)
- the user-specific long-term storage area (ULS)

If an LSSB is no longer required, it can be deleted at the same time by entering KCOM=RL. The contents of a ULS can only be deleted by writing (SPUT) with KCLA=0.

A GSSB must be deleted with a separate call (SREL); it remains locked until the end of the transaction or service. For further information, see the description of the SREL call.

A GSSB or ULS can be unlocked explicitly with the UNLK call.

Unix, Linux and Windows systems

In UTM cluster applications, GSSB or ULS areas are available throughout the cluster.

Setting the KDCS parameter area (1st parameter)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area				
	KCOP	KCOM	KCLA	KCRN	KCUS
Read from LSSB	"SGET"	"KP"	Length	Name of the LSSB	—
Read from LSSB and delete LSSB	"SGET"	"RL"	Length	Name of the LSSB	—
Read from GSSB (and lock GSSB)	"SGET"	"GB"	Length	Name of the GSSB	—
Read from ULS (and lock ULS)	"SGET"	"US"	Length	Block name	User ID / LSES name / association name / blanks

For KCOM = US, all the fields not used in the KDCS parameter area are to be set with binary zero.

Setting the 2nd parameter

Here you have to supply the address of the message area into which openUTM is to read the message.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"SGET"
KCOM	"KP"/"RL"/"GB"/"US"
KCLA	Length in bytes
KCRN	Name of the area
KCUS	User ID / LSES name / association name / blanks

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_SGETKP/KDCS_SGETRL/KDCS_SGETGB	(nb,kcla,kcrn)
KDCS_SGETUS	(nb,kcla,kcrn,kcus)

openUTM return information	
Message area	Contents
	Data
Field name in the KB return area	
KCRLM	Actual block length
KCRCCC	Return code
KCRCDC	Internal return code

For the SGET call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the SGET operation code.

KCOM

In the KCOM field:

- KP (keep) to read from an LSSB - the area is retained
- RL (release) to read from and delete an LSSB
- GB to read from a GSSB
- US to read a ULS block

KCLA

In the KCLA field, length of data to be transferred to the message area.

KCRN

In the KCRN field, name of the LSSB/GSSB or of the ULS block to be read from.

KCUS

In the KCUS field, user ID / LSES name / association name if a ULS block of a foreign user ID / LSES / association is to be read, otherwise blanks (if blanks are specified, the ULS block of the user / LSES / association who started the service is read).

If a foreign user ID / LSES / association is entered in KCUS, your own user ID / LSES / association must have administration privileges.

Irrelevant for KCOM = KP/RL/GB.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area to which UTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

Message area

the desired data in the specified message area.

KCRLM

in KCRLM, the actual length of the data in the LSSB/GSSB/ULS (in bytes). This enables you to detect deviations from the KCLA entry (important if specified KCLA value is smaller).

Exception: for KCLA = 0 UTM always returns KCRLM = 0.

KCRCCC

KCRCCC: the KDCS error code, see next page.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the SGET call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 14Z No area exists with the name specified in KCRN (only for KP, RL, GB).
- 40Z System cannot perform the operation (generation error or system error, deadlock, timeout); see KCRCDC.
- 41Z The call was issued in the first segment of the sign-on service although this is not allowed by the generation.
For KCOM=US: The call was issued in the first segment of the sign-on service or in the sign-on service after a SIGN ON and before the PEND PS call.
- 42Z Entry in KCOM is invalid.
- 43Z Length entry in KCLA negative or invalid.
- 44Z Name in KCRN invalid. It is invalid if it consists solely of blanks or binary zero or has not been generated (in the case of ULS).
- 46Z Name in KCUS is invalid.
- 47Z Message area missing or cannot be accessed in the specified length.
- 49Z Contents of fields not used in the KDCS parameter area not equal to binary zero (only for KCOM = US).

An additional error code can be found in the dump:

- 71Z INIT missing in this program.

Features of the SGET call

- The area is transferred in its actual length, but at the most in the length specified in KCLA. The actual length of the data in the GSSB, LSSB or ULS is returned in the KCRLM field.
 - If the length specified in KCLA is smaller than the actual length of the record to be read, the data is truncated at the right-hand side. You can capture this situation in a program unit (KCLA < KCRM).
 - If the length specified in KCLA is greater than the actual length of the record to be read (KCLA > KCRLM), the surplus part of the message area is undefined after the SGET call.
- If an attempt is made in a program unit to perform an SGET read operation on a nonexistent storage area, the program unit will receive the error code 14Z ("No area with this name exists").
- If SGET is used to access a GSSB or ULS, the following applies:
 - An SGET call for a GSSB or ULS locks the GSSB or ULS until the next synchronization point or rollback point, i.e. until PEND SP/RE/FI/FC/RS/ER/FR or RSET. If, following SGET, the processing step is terminated in a program unit with a PEND KP, PGWT KP, PGWT PR or with a PEND PA/PR call with a task change due to TAC class control or a wait for a DGET message, the access lock remains until the next synchronization point, unless the lock is cancelled beforehand with an UNLK call.
 - Reading from a non-existent GSSB has the same effect as creating a GSSB with simultaneous deletion (SPUT, SREL sequence).
 - The name of this GSSB remains locked until the next synchronization point or rollback point.
 - If the generated maximum number of GSSBs is already reached, the program unit receives the return code 40Z with KCR CDC K804.

Unix, Linux and Windows systems

In a UTM cluster application, reading from a non-existent GSSB requires four additional file accesses (to increment and decrement the GSSB counter). Consequently, in UTM cluster applications, it is advisable for performance reasons not to use any empty GSSBs but instead, for instance, a GSSB of length 1 for the serialization of program units, for example.

In section "[Action with locked storage areas \(TLS, ULS and GSSB\)](#)" there is a description of how openUTM reacts when the desired GSSB or ULS block is locked.

- When an SGET is used to access an LSSB, the following applies:
 - SGET KP causes the LSSB to remain available in the follow-up transaction of the service, i.e. after the subsequent PEND RE/SP.
 - SGET RL reads the LSSB and deletes it at the end of transaction (i.e. with PEND RE/SP/FI/FC/RS/ER/FR). Attempts to access in the meantime are rejected with 14Z.
You should always use this variant if the LSSB is no longer needed after reading in the current service.

7.25 SIGN Control sign-on and sign-off, check authorization data, change passwords

You use the SIGN (sign on) call to

- query the status of the sign-on service in the sign-on service or transfer the authorization data to openUTM
- change the password for the current user ID
- have the authorization data checked
- initiate in the program the effect of the commands KDCOFF and KDCOFF BUT.

The SIGN call is only allowed in dialog program units (exception: SIGN CK).

For BS2000 systems, you can additionally use the SIGN CL (Change Locale) call to change the location of the current user ID. This call is described as of "[SIGN CL - Change locale of user ID \(BS2000 systems\)](#)".

Setting the KDCS parameter area (1st parameter)

The table below shows the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area			
	KCOP	KCOM	KCLA	KCUS
Query status of the sign-on service	"SIGN"	"ST"	120	Binary zero
Transfer authorization data to openUTM	"SIGN"	"ON"	16	User ID
Change password	"SIGN"	"CP"	32	Binary zero
Check authorization data (without sign-on)	"SIGN"	"CK"	16	User ID
Initiate effect of the KDCOFF command	"SIGN"	"OF"	0	Binary zero
Initiate effect of the KDCOFF BUT command	"SIGN"	"OB"	0	Binary zero

All the fields not used in the KDCS parameter area have to be set to binary zero.

Setting the 2nd parameter

Here you have to supply the address of the message area from which openUTM is to read the data.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"SIGN"
KCOM	"ST"/"ON"/"CP"/"CK"/"OF"/"OB"
KCLA	120/16/32/16/0/0
KCUS	User ID/binary 0
Message area	
	Data/ -

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_SIGNST/KDCS_SIGNOF/KDCS_SIGNOB	(nb)
KDCS_SIGNON/KDCS_SIGNCK	(nb,kcla,kcus)
KDCS_SIGNSTLA/KDCS_SIGNCP	(nb,kcla)

openUTM return information	
Field name in the KB return area	Contents
KCRSIGN1	Sign-on status
KCRSIGN2	Additional information
KCRUS	Name of user ID
KCRCCC	Return code
KCRCDC	Internal return code
KCRMF/kcrfn	Format identifier of start format/blanks
KCRLM	Validity period of password

For the SIGN call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the SIGN operation code.

KCOM

In the KCOM field

- ST: query status of the sign-on service
- ON: check authorization data (with sign-on)
- CP: change password
- CK: check authorization data (without sign-on)
- OF: initiate effect of the KDCOFF command
- OB: initiate effect of the KDCOFF BUT command.

KCLA

In the KCLA field

- 120 for KCOM=ST:
This is the length of the message area into which openUTM transfers the information. openUTM provides a data structure for structuring of the message area, see description on "[Features of the SIGN call](#)". Specify the version number of the structure in the data structure header.
- 16 for KCOM = ON/CK:
This is the length of the password that is transferred in the message area for this call.
- 32 for KCOM = CP:
This is the length of the old and new password that is transferred in the message area for this call.
- 0 for KCOM = OF/OB

KCUS

In the KCUS field, the user ID if, with KCOM = ON/CK, authorization data is to be transferred to UTM. Enter binary zero for all other variants.

Message area

In the message area you have to enter the data you wish to transfer to openUTM or receive from openUTM. The password (16 characters) is made available for KCOM = ON/CK, the old and the new password (32 characters) are made available for KCOM = CP.

For KCOM = ST, the following information is exchanged when KCLA > 0 (maximum of 120 characters):

- the desired version of the data structure is passed (2 characters)
- data for the sign-on service (e.g. validity period of the password) is returned.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area from which UTM is to read the data. You enter the address of the message area even if you have entered the length 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRSIGN1

KCRSIGN2

Additional information in the KCRSIGN1 and KCRSIGN2 fields (nothing is entered unless KCRCCC = 000):

- for KCOM = ST, the current status of the sign-on procedure, see table on "[Return information of the SIGN ST call in the KCRSIGN1 and KCRSIGN2 fields](#)".
- for KCOM = CK, the result of the check, see table on "[Return information of the SIGN CK call in the KCRSIGN1 and KCRSIGN2 fields](#)".

KCRUS

in the KCRUS field, the name of the user ID if:

- KCRSIGN1=U, i.e. it was not possible to sign-on the user ID successfully, or
- KCRSIGN1=I, i.e. sign-on was not terminated successfully, an intermediate dialog must be performed for the user

KCRCCC

in the KCRCCC, the KDCS return code, see "[KDCS return codes for the SIGN call](#)".

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KCRMF/kcrfn

in the KCRMF/kcrfn field, for KCOM = ST the format identifier of the start format or blanks if no start format was generated. When used with USER and if the sign-on was successful, the identifier of the user-specific start formats is returned. If sign-on has not yet been completed successfully or if the application is generated without USER, then KCRMF/kcrfn contains the identifier of the LTERM-specific start format.

KCRLM

in the KCRLM field, for KCOM = ST:

- for KCRCCC < 40Z: KCRLM contains the length of the information actually available in openUTM.
- for KCRCCC >= 40Z, 0 is returned.

SIGN ST call return information in the fields KCRSIGN1 and KCRSIGN2

For SIGN ST, openUTM delivers the following information about the current status of the sign-on procedure in fields KCRSIGN1 and KCRSIGN2:

KCRSIGN1	KCRSIGN2	Meaning
C	01	Connection established (as K002)
	02	KDCOFF BUT command issued (as K018)
	03	KDCOFF BUT issued from program
U	01	Specified USER not generated (as K004)
	02	Specified USER locked (as K005)
	03	Someone already signed on with this USER (as K007)
	04	Specified old password is invalid (as K006)
	01	Specified USER not generated (as K004)
	02	Specified USER is locked (as K005)
	03	Someone already signed on with this USER (as K007)
	04	Specified old password is invalid (as K006)
	05	Entries for new password unusable
	06	The terminal has no card reader (as K030)
	07	Card information is invalid (as K031)
	08	Sign-on not possible at present because of resource bottleneck or no further users can sign on at present, since the maximum possible number of simultaneous users has been reached, or it was not possible to change the password, since an inverse KDCDEF is currently running.
	09	Only on BS2000 systems: Sign-on not possible because of missing Kerberos support (as K110).
10	The current LTERM is not authorized to continue the service (as K123)	
11	The period of validity for the password has been exceeded (as K120)	
12	The new password does not fulfill the requirements of the complexity level generated (as K097)	
13	The new password is too short (as K097)	

KCRSIGN1	KCRSIGN2	Meaning
U	14	The password transferred by KDCUPD does not fulfill the requirements of the complexity level generated (as K125)
	15	A transaction restart is required for the specified user ID (as K145)
	16	The open service cannot be continued from within this LTERM partner (like K123)
	17	The administrator issued a SHUT WARN; Normal users cannot sign on any more to the application (as K016); administrators can still sign on.
	18	The encryption mechanism required for the continuation of the open service is not available in the connection (as K123)
	19	The period of validity of the password has been exceeded but the password can still be changed because the application is generated with SIGNON GRACE=YES.
	20	Only on BS2000 systems: Error in the Kerberos authentication (as K108)
	21	Only on BS2000 systems: Invalid Kerberos principal (as K109)
	22	Only on Unix, Linux and Windows systems: The specified USER does not exist in the cluster user file (as K004).
	23	Somebody has already signed onto a different node application under this USER (as K007).
	24	Only on Unix, Linux and Windows systems: It is currently not possible to sign on because the cluster user file could not be locked in the generated time (CLUSTER statement, parameter FILE-LOCK-TIMER-SEC, parameter FILE-LOCK-RETRY) (as K091).
	25	It is not possible to sign on at this node application because the user has a service that is bound to another node application and which may not be terminated (as K189).
	26	Sign-on rejected because the user's open service has a transaction in PTC state but no service restart has been requested.

KCRSIGN1	KCRSIGN2	Meaning
I	01	The USER is known but intermediate dialog is required (only for automatic KDCSIGN)
A	01	Sign-on successful because generated without USER (as K001)
	02	Sign-on successful (as K008)
	03	Only on BS2000 systems: Sign-on successful (via distributor)
	04	Sign-on successful (from the connection user ID, only for TS applications or UPIC client). It is possible to sign on with a "genuine" user ID using the SIGN ON call.
	05	Sign-on successful, password changed via intermediate dialog
	06	Only on BS2000 systems: Sign-on successful (via distributor), the password was changed via distributor
R	01	as A01, but after service restart
	02	as A02, but after service restart
	03	as A03, but after service restart (only on BS2000 systems)
	04	as A04, but after service restart
	05	as A05, but after service restart
	06	as A06, but after service restart (only on BS2000 systems)

KCRSIGN1 provides a rough classification:

- C: Connected but not signed on.
Status following connection setup or KDCOFF BUT
- U: Sign-on Unsuccessful.
A preceding attempt to sign on was rejected.
- I: Sign-on Incomplete.
Intermediate dialog is required to obtain additional data (password, ID, chipcard)
- A: Sign-on Accepted.
Without subsequent service restart
- R: Sign-on accepted + Restart.
With subsequent service restart.

Return information of the SIGN CK call in the KCRSIGN1 and KCRSIGN2 fields

openUTM returns the following information for SIGN CK in the KCRSIGN1 and KCRSIGN2 fields:

KCRSIGN1	KCRSIGN2	Meaning
A	02	Authorization data is correct and complete
U	01	The specified USER does not exist
	02	The specified USER is locked
	04	The specified old password is incorrect
	06	The terminal has no card reader (only on BS2000 systems)
	07	The card information is invalid (only on BS2000 systems)
	09	No Kerberos support (only on BS2000 systems)
	11	The validity period of the password has expired
	14	The password transferred by KDCUPD does not satisfy the complexity level requirement or is too short
21	Invalid Kerberos principal (only on BS2000 systems)	

KDCS return codes in the KCRCCC field for the SIGN CK/CP/OB/OF/ON/ST calls

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 01Z For SIGN ST: The function was executed, the message area provided is too short, though (the value in KCLA is too small). No information or incomplete information was returned.
- 40Z System cannot perform the operation (generation error or system error).
- 41Z Call is not allowed at this point:
 - SIGN OF/OB call already issued, or
 - SIGN call in an asynchronous service and call is not SIGN CK , or
 - SIGN ST/ON call outside a sign-on service, or
 - SIGN CP/CK call prior to successful sign-on, or
 - SIGN ON/CP/CK call in an application which was generated without user IDs, or
 - SIGN OB/OF in a job-receiving service (with distributed transaction processing).
- 42Z Entry in KCOM is invalid.
- 43Z Length entry in KCLA is negative or invalid.
- 44Z For KCOM=CP: entry for old password incorrect, password not changed
- 45Z For KCOM=CP: entry for new password incorrect, password not changed. The more precise cause provides KCRCDC.
- 47Z Message area missing or cannot be accessed in the specified length.
- 48Z For KCOM=ST: invalid interface version
- 49Z Contents of fields not used in the KDCS parameter area not equal to binary zero.

An additional return codes can be found in the dump:

- 71Z INIT call still missing in the program unit run.

Features of the SIGN call

- Message area for SIGN ST with KCLA > 0:

Field name COBOL	Field name C/C++	Length in bytes	Description
Call information:			
KCVER	if_version	2	Version number of the data structure (4)
Return information:			
KCRPWVAL	rpwval	2	Validity period of the password
KCRPWMIN	rminpw	2	Minimum validity period of the password
KCRUSER	ruser	8	User ID
KCRTAC	rtac	8	Transaction code from the UPIC protocol
KCFILLER	filler	8	
KCRPSWRD	rpassword	8	Password from the UPIC protocol
KCLSTSGN	rlstsgn	14	Date/time of the last sign-on
KCDSPMSG	rdispmsg	1	Message present (Y/N)
KCTAPTC	rtainptc	1	Transaction in PTC state (Y/N)
KCCLNODE	rclusternode	64	Only on Unix, Linux and Windows systems: Host name of the node to which the open service is bound
KCRPASSL	rpassword16	16	Password from the UPIC protocol
KCSGRES	reserved	10	Reserved for future extensions

The following mean:

KCVER

Version number of the data structure. The number 4 is to be entered here for this version of openUTM.

KCRPWVAL

If the sign-on was successful (KCRSIGN1 = A/R) or has not yet been successful (KCRSIGN1 = I), then this field contains the number of days that the password for this user is still valid.

The value -1 means that there was no validity period generated for the password.

The value 0 means that the password will become invalid within the next 24 hours.

The value -2 means that validity of the password has run out. The password must be changed if the sign-on service is to terminate successfully. This values can only be returned if grace sign-ons are permitted (SIGNON statement in the generation, parameter GRACE = YES).

In the case of KCRSIGN1 = I, the value -3 means that the complexity level or minimum length of the password has been increased and that the password transferred with the KDCUPD tool may possibly no longer meet the requirements.

Otherwise the value -3 means that the password passed by the KDCUPD tool does not meet the complexity level requirements or is too short. The password must be changed with SIGN CP if the sign-on service is to terminate successfully.

This values can only be returned if grace sign-ons are permitted (SIGNON statement in the generation, parameter GRACE = YES).

KCRPWMIN

If the sign-on is successful (KCRSIGN1 = A/R) or has not yet been successful (KCRSIGN1 = I), then this field contains the number of days that the password for this user may not be changed using a SIGN CP call. The value 0 means that the password may be changed.

KCRUSER

After an unsuccessful or not yet completed sign-on (KCRSIGN1 = U/I), this field contains the name of the user that was rejected (KCRSIGN1 = U) or for whom an intermediate dialog must be executed first (KCRSIGN1 = I), otherwise it contains blanks.

KCRTAC

This field contains the name of the transaction code (TP_Name) passed in the UPIC protocol in the sign-on service for the UPIC client, otherwise it contains blanks. openUTM does not check if the transaction code is valid or not.

KCLSTSGN

This field contains the date and time of the last successful sign-on of this user to the application after the user has successfully signed on (KCRSIGN1 = A/R) or has not yet signed on successfully (KCRSIGN1 = I). The date and time are passed in the format YYYYMMDDHHMMSS. Printable nulls are returned after the first successful sign-on after a regeneration.

KCDSPMSG

After the successful sign-on (KCRSIGN1 = A/R) of a user, the field contains the following value:

Y

If there is an open dialog service for the user (KCRSIGN1=R) or a dialog message that can be output with MPUT PM

N

in all other cases

KCTAPTC

When the user has successfully signed on with a subsequent service restart (KCRSIGN1 = R), the field has the following value:

Y

If there is a transaction in the state P(repare) T(o) C(ommit) for the user. In this case, the service restart cannot be prevented.

N

in all other cases.

KCCLNODE

If the sign-on was not successful (KCRSIGN1 = U) due to the existence of a service bound to another node application (KCRSIGN2 = 25), the field contains the host name of the node to which the open service is bound.

KCRPASSL

This field contains the password of a user generated without a password that was passed in the UPIC protocol in the sign-on service for the UPIC client after a successful sign-on (KCRSIGN1 = A/R), otherwise it contains blanks.

- Entries in the message area for SIGN ON and SIGN CP
- For SIGN ON, write an 16 byte password to the message area. Blanks mean "user ID without password".
- For SIGN CP, write the old and new passwords at 16 byte length to the message area as follows:

old password ¹	new password ¹
---------------------------	---------------------------

¹Blanks mean "user ID without password"

The new password must consist of characters which are allowed in the UTM partner application, see openUTM manual "Generating Applications", USER statement.

If the call has the correct syntax, then openUTM overwrites the data area with blanks.

You do not need administration authorization for this call.

- With SIGN ON openUTM checks whether the user is able to sign on from this client at this time.
- With SIGN CK openUTM checks whether the authorization data is adequate for successful sign-on from this client but does not check whether sign-on is possible at this time.
- SIGN OF and SIGN OB may only be issued in program units terminated with PEND RE or PEND RE or PEND FI and which issue the dialog message to the terminal, the UPIC client or the transport system application. Otherwise, openUTM aborts the service with PEND ER.

SIGN OB to UPIC clients or transport system applications has the same effect as SIGN OF.

SIGN OF and SIGN OB only take effect at the next input from the terminal. In other words, the user is not signed off until after the next input (SIGN OB), or the connection to the terminal is not cleared until after the first input (SIGN OF). In the case of UPIC clients or transport system applications, the connection clear-down is initiated immediately.

- SIGN ST and SIGN ON are only allowed in the sign-on service.

i SGN is used as symbolic name instead of the operation code SIGN in the COBOL data structure because SIGN is a reserved COBOL word.

7.25.1 SIGN CL - Change locale of user ID (BS2000 systems)

SIGN CL (Change Locale) can be used to change the user-specific locale of the current user ID, i.e. the language identifier, the territory identifier and the name of the employed character set can be rolled back provided that the current user ID is a genuine user ID (not a connection user ID).

SIGN CL is only permitted in dialog program units of a UTM application which is configured using user IDs. Administration privileges is not necessary.

If the call is successful, then the new locale is valid as of the next end of transaction. All messages in the current transaction are processed using the old character set name. It is therefore advisable to terminate the program unit at the end of transaction, but without issuing a dialog message to the terminal if the character set name of the user has changed.

If you only want to change specific components of the location, you have to set binary zero for the remaining components.

Modifications performed with SIGN CL remain valid after a KDCUPD run. KDCUPD implicitly transfers the current values of a user location to the new KDCFILE.

SIGN CL is an upwards compatible extension of DIN 66265.

Setting the KDCS parameter area (1st parameter) with SIGN CL

Function of the call	Entries in the KDCS parameter area				
	KCOP	KCOM	KCLANGID	KCTERRID	KCCSNAME
Change locale of user ID	SIGN	CL	New language identifier of user ID	New territory identifier of user ID	CCS name of new character set for user ID

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"SIGN"
KCOM	"CL"
KCLANGID	Language identifier of user / binary zero
KCTERRID	Territory identifier of user / binary zero
KCCSNAME	Character set name of user / binary zero

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	—

C/C++ macro call	
Macro name	Parameters
KDCS_SIGNCL	(nb,kclangid,kcterrid,kccsname)

openUTM return information	
Field name in KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the SIGN call with CL operation modifier you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the SIGN operation name.

KCOM

In the KCOM field, the operation modifier

- CL: Change locale of user ID.

KCLANGID

In the KCLANGID field, the new language identifier which is to be assigned to the user ID from which the service was started. The length of the language identifier is 2 bytes. Enter binary zero in KCLANGID if you do not want to change the language identifier.

KCTERRID

In the KCTERRID field, the new territory identifier which is to be assigned to the user ID from which the service was started. The length of the territory identifier is 2 bytes. Enter binary zero in KCTERRID if you do not want to change the territory identifier.

KCCSNAME

In the KCCSNAME field, the CCS name of the new character set to be assigned to the user ID. The length of the CCS name is 8 bytes maximum.

Enter binary zero in KCCSNAME if you do not want to assign a new character set.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro name

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field, the KDCS return code (length 3 bytes). See below for possible return codes and their meaning.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the SIGN CL call

The following codes can be analyzed in the program:

- 000 Operation carried out, the specified component(s) of the location have been changed.
- 40Z The system was not able to perform the operation (generation error).
- 41Z SIGN CL is not allowed at this point:
 - the call was issued before a successful sign-on
 - the call was issued in an application without user ID.
- 46Z Specifications for the new locale are incorrect. The location of the user ID is not changed. openUTM returns the precise cause in the KCRCDC field.
- 49Z When the function was called, unused fields in the KDCS parameter area were not set to binary zero.

An additional return codes can be found in the dump:

- 71Z No INIT call issued in the program unit.

7.26 SPUT Write to secondary storage area

You use the SPUT (storage put) call to write data from a specified area to a

- global secondary storage area (GSSB) or a
- local secondary storage area (LSSB) or a
- user-specific long-term storage area (ULS).

Note that the name of a ULS block is defined at generation (ULS statement for KDCDEF), whereas you can select the names of GSSBs and LSSBs arbitrarily when you call SPUT.

Unix, Linux and Windows systems

In UTM cluster applications, GSSB or ULS areas are available throughout the cluster.

Setting the 1st parameter (KDCS parameter area)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the calls	Entries in the KDCS parameter area				
	KCOP	KCOM	KCLA	KCRN	KCUS
Write to LSSB	"SPUT"	"DL"/ "MS"/"ES" (all have same effect)	Length	Name of LSSB	—
Write to GSSB	"SPUT"	"GB"	Length	Name of GSSB	—
Write to ULS	"SPUT"	"US"	Length	Block name	User ID / LSES name/ association name/ blanks

For KCOM = US all the fields not used in the KDCS parameter area are to be set to binary zero.

Setting the 2nd parameter

Here you have to supply the address of the message area which contains the message to be written.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"SPUT"
KCOM	"GB"/"DL"/"MS"/"ES"/"US" ("DL", "MS" and "ES" have the same effect)
KCLA	Length in bytes
KCRN	Name of the area
KCUS	User ID / LSES name / association name / blanks
Message area	
	Data

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_SPUTGB/KDCS_SPUTDL/KDCS_SPUTMS/KDCS_SPUTES	(nb,kcla,kcrn)
KDCS_SPUTUS	(nb,kcla,kcrn,kcus)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the SPUT call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the SPUT operation code.

KCOM

In the KCOM field, the entry indicating

- whether writing should be to an LSSB ("DL" or "MS" or "ES"), or
- whether writing should be to a GSSB ("GB"), or
- whether writing should be to a ULS block ("US").

The entries "MS" and "ES" have the same effect as "DL" for openUTM.

KCLA

In the KCLA field, the length of the data which you make available in the message area. The length is not written to the LSSB/GSSB/ULS.

KCRN

In the KCRN field, the name of the LSSB/GSSB or ULS block to be initialized or to which the data is to be written. Blanks and binary zero are invalid entries.

KCUS

In the **KCUS** field, the user ID / LSES name / association name (for KCOM = US), if a ULS block of a foreign user ID / session / association is to be written, otherwise blanks. If you enter a foreign user ID / LSES name / association name in KCUS, your own user ID must have administration privileges.

For KCOM = DL/MS/ES/GB: irrelevant.

Message area

In the message area you have to enter the message which you want to output.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

2nd parameter

The address of the message area from which openUTM is to read the message. You enter the address of the message area even if you have entered the length 0 in KCLA.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code, see next page.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the SPUT call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 40Z System cannot perform the operation (generation error or system error, deadlock, timeout), see KCRCDC.
- 41Z Call issued in the first segment of the sign-on service, although this is not allowed by the generation.
For KCOM=US: the call was issued in the first segment of the sign-on service or after a SIGN ON and before the PEND PS call.
- 42Z Entry in KCOM is invalid.
- 43Z Length entry in KCLA is negative or invalid.
- 44Z Name in KCRN invalid if it consists solely of blanks or binary zero or has not been generated (in the case of ULS).
- 46Z Entry in KCUS is invalid.
- 47Z Message area missing or cannot be accessed in the specified length.
- 49Z Contents of fields not used in the KDCS parameter area not equal to binary zero (only for KCOM = US).

An additional error code can be found in the dump:

- 71Z INIT missing in this program

The following table describes the effect of the call sequences SPUT ... RSET and SPUT ... PEND/PGWT on GSSBs, ULSs and LSSBs.

Call		Effect on GSSBs/ULSs	Effect on LSSBs
SPUT		locks: GSSBs are created if not already present, existing GSSBs are replaced	creates or replaces
...	PEND KP PGWT KP/PR	leaves resettable and locked	leaves resettable
...	PEND RE/SP/ PGWT CM	sets valid (they are then no longer resettable) and unlocks (i.e. other transactions can use them)	sets valid (they are then no longer resettable)
...	PEND FI /FC		deletes (they are no longer available)
...	RSET/ PEND RS/ PGWT RB	cancels changes and unlocks; a GSSB is deleted if created in this transaction	cancels changes
...	PEND ER/FR		deletes

Please note the following features of GSSBs, ULSs and LSSBs:

- A GSSB is available to all program units in an application, i.e. it can be overwritten by all program units. To avoid unintentional overwriting of GSSBs by other program units, you must ensure that their names are unique.
- *Unix, Linux and Windows systems*
In UTM cluster applications, GSSB and ULS areas are available throughout the cluster. I.e. any GSSB or ULS that you create/write with SPUT exists in all node applications where it can be read using SGET.
- An LSSB is assigned uniquely to a service.
- GSSBs, LSSBs and ULS blocks always take the length of the last SPUT called. This length cannot exceed 32767 bytes.
- The name of a ULS block is defined at generation (as a TLS block).
- The maximum number of GSSBs or LSSBs is defined at generation

Features of the SPUT call

- The SPUT call for a GSSB/ULS locks this GSSB or ULS block until the end of the transaction, i.e. until PEND RE, SP, FI, FC, RS or ER/FR.

Following an SPUT call, a GSSB/ULS block remains locked by this transaction; a subsequent PEND KP or PGWT KP call or a PEND PA/PR or PGWT PR (in the case of a wait for a DGET message) retains the lock beyond the end of the processing/dialog step.

Another transaction that wants to process this GSSB/ULS block with SGET, SPUT or SREL will be rejected in the following cases.

- PEND KP and PGWT KP
- PEND PA/PR with a task change due to TAC class control
- PEND PA/PR or PGWT PR with waiting for a DGET message

At the end of a transaction or when there is a rollback operation, all locked GSSBs and ULS blocks are released.

In the section [“Action with locked storage areas \(TLS, ULS and GSSB\)”](#) there is a description of how openUTM reacts when the desired GSSB or ULS block is locked.

- GSSB areas are permitted with length 0 in KCLA. These GSSBs can be used for communication between application programs; all that is evaluated is whether the GSSB is locked or not. However, openUTM deletes a GSSB with length 0 the next time the application is started. KDCUPD likewise does not transfer GSSBs with length 0 to a new KDCFILE (see the openUTM manual “Generating Applications”, changing KDCFILE).
- You can also use a SPUT call with KCLA=0 to delete the contents of ULS blocks.

7.27 SREL Delete secondary storage area

You use the SREL (storage release) call to delete a secondary storage area. A secondary storage area can be

- the global secondary storage area (GSSB)
- the local secondary storage area (LSSB)

Blocks of a ULS (user-specific long-term storage) **cannot** be deleted using SREL, since their names are specified when the application is generated. If you want to delete the contents of a ULS block, you have to overwrite the block with length zero.

Unix, Linux and Windows systems

In UTM cluster applications, a GSSB is valid throughout the cluster. Its deletion with SREL therefore also applies throughout the cluster.

Setting the 1st parameter (KDCS parameter area)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area		
	KCOP	KCOM	KCRN
Delete LSSB	"SREL"	"LB"	Name of the LSSB
Delete GSSB	"SREL"	"GB"	Name of the GSSB

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"SREL"
KCOM	"LB"/"GB"
KCRN	Name of the area

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	—

C/C++ macro call	
Macro names	Parameters
KDCS_SRELGB / KDCS_SRELLB	(kcrn)

openUTM return information	
Field name in the KB return are	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the SREL call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, the SREL operation code.

KCOM

In the KCOM field

- LB to delete an LSSB, or
- GB to delete a GSSB

KCRN

In the KCRN field, the name of the LSSB/GSSB to be deleted

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field: the KDCS return code.

KCRCDC

in the KCRCDC field: the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the SREL call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 14Z No area exists with the name specified in KCRN.
- 40Z System cannot perform the operation (generation error or system error, deadlock, timeout), see KCRCDC.

42Z Entry in KCOM is invalid.

44Z Name in KCRN invalid (if it consists solely of blanks or binary zero).

An additional error code can be found in the dump:

71Z INIT missing in this program.

Features of the SREL call

- openUTM does not execute SREL until the end of the current transaction.
- SREL is not executed
 - for service interrupt via PEND ER/FR, or
 - if there is a subsequent PEND RS or RSET call.
- An SREL call locks the area called until the end of the transaction or UNLK or until the next rollback operation. In other words, openUTM rejects subsequent SGET calls to this area with the return code 14Z. However, if an SREL call is followed by an SPUT call with the same area name, this area (LSSB or GSSB) is set up anew. The lock continues to apply after the end of a processing/dialog step when the program unit run is terminated or interrupted with:
 - PEND KP and PGWT KP
 - PEND PA/PR with a task change due to TAC class control
 - PEND PA/PR or PGWT PR with waiting for a DGET messageIf this area is a GSSB, then other services cannot access this GSSB either with SGET or with SPUT until the end of the transaction. The section [“Action with locked storageareas \(TLS, ULS and GSSB\)”](#) describes how openUTM reacts in this case
- At the end of a service (PEND FI/FC) or service interrupt (PEND ER/FR, possibly also PEND RS), openUTM automatically deletes all LSSBs. SREL calls to LSSBs are therefore superfluous in transactions which terminate services.
- *Unix, Linux and Windows systems*

In UTM cluster applications, an SREL call deletes a GSSB throughout the entire cluster, i.e. as soon as the SREL call takes effect, the GSSB can no longer be read in any of the node applications.

The following table describes the effect of the call sequences SREL ... RSET and SREL ... PEND on GSSBs and LSSBs.

Call		Effect on GSSB	Effect on LSSB
SREL		deletes and locks (operation remains resettable)	deletes (operation remains resettable)
...	RSET PEND RS PGWT RB	resets and unlocks	resets
...	PEND KP PGWT KP	leaves the operation resettable	leaves the operation resettable
...	PEND RE PEND SP PGWT CM	deletes and unlocks (operation not resettable)	deletes (operation not resettable)
...	PEND FI PEND FC		deletes all LSSBs
...	PEND ER PEND FR	resets and unlocks	deletes all LSSBs
...	PEND PA/PR ¹ PGWT PR ¹	lock remains, operation resettable	lock remains, operation resettable

¹ With a task change due to TAC class control or with waiting for a DGET message

7.28 UNLK Unlock TLS, ULS or GSSB

You use the UNLK (unlock) call to unlock one of the following storage areas:

- the global secondary storage area (GSSB).
- a block of the terminal-specific long-term storage area (TLS).
- a block of the user-specific long-term storage area (ULS).

The area is not unlocked unless it was only read in the current transaction

Unix, Linux and Windows systems

In UTM cluster applications, GSSB and ULS areas are valid throughout the cluster. As a result, unlocking a GSSB or ULS with UNLK is effective throughout the cluster.

Setting the 1st parameter (KDCS parameter area)

The table below shows the various options and the necessary entries in the KDCS parameter area.

Function of the call	Entries in the KDCS parameter area			
	KCOP	KCOM	KCRN	KCLT or KCUS
Unlock TLS (in dialog programs)	"UNLK"	"DA"	Block name	—
Unlock TLS (in asynchronous programs)	"UNLK"	"DA"	Block name	LTERM name / LPAP name / OSI- LPAP name / Master-LPAP name
Unlock GSSB	"UNLK"	"GB"	Name of GSSB	—
Unlock ULS	"UNLK"	"US"	Block name	User ID / LSES name / association name / blanks

For KCOM = US, all the fields not used in the KDCS parameter area are to be set to binary zero.

Setting the parameters	
Field name in the KDCS parameter area	Contents
KCOP	"UNLK"
KCOM	"GB"/"DA"/"US"
KCRN	Name of the area/block name
KCLT or KCUS	LTERM name / LPAP name / OSI- LPAP name / Master-LPAP name or user ID / LSES name / association name / blanks

KDCS call	
1st parameter	2nd parameter
KDCS parameter area	Message area

C/C++ macro calls	
Macro names	Parameters
KDCS_UNLKGB	(kcrn)
KDCS_UNLKDA	(kcrn,kclt)
KDCS_UNLKUS	(kcrn,kcus)

openUTM return information	
Field name in the KB return area	Contents
KCRCCC	Return code
KCRCDC	Internal return code

For the UNLK call you make the following entries in the KDCS parameter area:

KCOP

In the KCOP field, UNLK operation code.

KCOM

In the KCOM field, the type of storage to be unlocked:

- GB for a global secondary storage area (GSSB).
- DA for terminal-specific long-term storage area (TLS).
- US for a user-specific long-term storage area (ULS).

KCRN

In the KCRN field, the name of the storage area to be unlocked.

KCLT

KCUS

Depending on the type of storage:

- for unlocking a TLS in an asynchronous program: in the KCLT field, the name of the LTERM or (OSI) LPAP partner, whose TLS is to be unlocked.
- for unlocking a TLS in a dialog program: irrelevant, the corresponding block of the associated TLS is always accessed.

-
- for unlocking a ULS block: in the KCUS field, the user ID if a ULS block of a foreign user ID is to be unlocked or blanks for a ULS block of your own user ID. If you enter a foreign user ID in KCUS, your own user ID must have administration privileges.
If you want to unlock a ULS block of a remote session/association, you have to specify its name.
 - for unlocking a GSSB: irrelevant.

You specify the following for the KDCS call:

1st parameter

The address of the KDCS parameter area.

Macro names

The use of C/C++ calls is described in detail in the section "[C/C++ macro interface](#)".

openUTM returns:

KCRCCC

in the KCRCCC field, the KDCS return code.

KCRCDC

in the KCRCDC field, the internal return code of openUTM (see the openUTM manual "Messages, Debugging and Diagnostics").

KDCS return codes in the KCRCCC field for the UNLK call

The following codes can be analyzed in the program:

- 000 Operation carried out.
- 14Z No GSSB/TLS exists with the name specified in KCRN.
- 16Z GSSB/TLS/ULS not locked by your own transaction or GSSB created or changed in same transaction or TLS changed in same transaction.
- 40Z System cannot perform the operation (generation error or system error, deadlock, timeout).
- 42Z Entry in KCOM is invalid.
- 44Z For GSSB: entry in KCRN is invalid (blanks or binary zero).
For TLS and ULS: name of the block in KCRN is unknown or invalid.
- 46Z LTERM or LPAP partner in KCLT is invalid (only for asynchronous programs and TLS) or the user ID is unknown (only for ULS).
- 49Z Contents of fields not used in the KDCS parameter area not equal to binary zero (only for KCOM = US)

An additional error code can be found in the dump:

- 71Z INIT missing in this program.

Features of the UNLK call

- An UNLK call to a TLS/ULS/GSSB is only useful after a read call (GTDA or SGET). If the area is changed in the current transaction with PTDA, SPUT or SREL (with GSSBs), openUTM rejects the call with KCRCCC = 16Z; the area remains locked until the end of transaction.
- An UNLK call is useful, for example, before entering PEND KP or PGWT KP/PR. This causes TLS/ULS blocks and GSSBs to be released prior to the next synchronization point. This makes them available to the other transactions.
- An UNLK call for an area not locked by your own transaction is rejected (return code 16Z).
- *Unix, Linux and Windows systems*
In UTM cluster applications, an UNLK call unlocks a GSSB or ULS throughout the cluster, i.e. as soon as the UNLK call takes effect, transactions in other node applications are again able to access the unlocked area.

8 Program interface UTM-HTTP

This chapter contains all the information you need to use the UTM-HTTP programming interface in your program. With the UTM-HTTP program interface, openUTM provides you with C functions that you can use in your program units and in the "Event exit HTTP".

This chapter also contains detailed information on communication with HTTP clients.



For an overview of communication with HTTP clients, please refer to the chapters "Accessing UTM Applications from the Internet" and "Communication with HTTP clients" in the openUTM manual "Concepts and Functions".

8.1 Overview of all UTM-HTTP functions

The functions of the UTM-HTTP program interface are divided into two groups, the `kcHttpGet` and the `kcHttpPut` functions. They can be called both by an HTTP exit program (see chapter "Event Exit HTTP") and - with exception of the functions `kcHttpGetMputMsg`, `kcHttpPutMgetMsg`, `kcHttpPutRspMsgBody` - by UTM program units. Furthermore there are the two auxiliary functions `kcHttpPercentDecode` and `kcHttpGetRc2String`.

UTM program units may call these functions not before the KDCS call INIT. The `kcHttpGet` functions may only called in the first program unit run of a (not chained) service.

If a program unit calls the functions `kcHttpPutHeader` or `kcHttpPutStatus`, it also has to supply a message for the HTTP client with MPUT and has to finish the service, else the provided status or header information will be lost. For use of these functions in the HTTP exit program see chapter "Event Exit HTTP" .

Input parameters of the C functions that are of type `char *` must be passed by the caller as a null-terminated string. UTM also returns null-terminated strings in output parameters of type `char *`.

If the execution was not successful all functions except the help function `kcHttpGetRc2String` return negative number constants defined as C data type `enum` as function result. If the execution was successful, either the number constant 0 or a positive function value is returned.

The following functions are available:

Function	Description
<code>kcHttpGetHeaderByIndex</code>	returns name and value of the HTTP header field with the specified index
<code>kcHttpGetHeaderByName</code>	returns the value of HTTP header field with the specified HTTP header name
<code>kcHttpGetHeaderCount</code>	returns the number of HTTP header fields of the HTTP request
<code>kcHttpGetMethod</code>	returns the HTTP method of the HTTP request
<code>kcHttpGetMputMsg</code>	returns the MPUT message created by the program unit
<code>kcHttpGetPath</code>	returns the normalized path of the HTTP request
<code>kcHttpGetQuery</code>	returns the normalized query of the HTTP request
<code>kcHttpGetRc2String</code>	Help function to convert a function result of type <code>enum</code> into a printable null-terminated string
<code>kcHttpGetReqMsgBody</code>	returns the message body of the HTTP request
<code>kcHttpGetScheme</code>	returns the scheme of the HTTP request
<code>kcHttpGetVersion</code>	returns the HTTP version of the HTTP request
<code>kcHttpPercentDecode</code>	converts characters in percent-decoding to their normal one-character representation
<code>kcHttpPutHeader</code>	passes an HTTP header field for the HTTP response
<code>kcHttpPutMgetMsg</code>	passes a message for the program unit which can be read with MGET

Function	Description
kcHttpPutRspMsgBody	passes a message for the message body of the HTTP response
kcHttpPutStatus	passes an HTTP status code for the HTTP response

The following returncodes are defined:

Returncodes

In the description of the individual functions, the function parameters are identified as follows:

- >> Input parameter Input value or an address containing an input value when the function is called.
- << Output parameter Address containing an arbitrary value when the function is called and an output value when the function returns.
- <> Input/Output parameter Address containing an input value when the function is called and an output value when the function returns.

The individual functions are described in detail in the following chapters.

8.1.1 Function kcHttpGetHeaderByIndex

The function `kcHttpGetHeaderByIndex` returns name and value of the HTTP header field with the specified index.

This function may be called both in program unit and HTTP exit program.

In the program unit the function may only called in the first program unit run of a service.

Function declaration `kcHttpGetHeaderByIndex`

```
kc_http_retcode kcHttpGetHeaderByIndex( int    headerIndex,
                                         char *  headerName,
                                         int *   headerNameLth,
                                         char *  headerValue,
                                         int *   headerValueLth
                                         );
```

This function has following parameters:

- >> `headerIndex` The index of the HTTP header field to read.
- << `headerName` The pointer to a buffer in which the name of the HTTP header is returned. The length of the buffer must be at least `headerNameLth` bytes.
- <> `headerNameLth` The pointer to a variable in which the length of the buffer for the name of the HTTP header is passed and the actual length of the name is returned.
- << `headerValue` The pointer to a buffer in which the value of the HTTP header is returned. The length of the buffer must be at least `headerValueLth` bytes.
- <> `headerValueLth` The pointer to a variable in which the length of the buffer for the value of the HTTP header is passed and the actual length of the value is returned.

Meaning of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run after message reception from the HTTP client or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_INVALID_INDEX`

The specified index `headerIndex` is invalid (less or equal 0 or greater than number of HTTP header fields contained in HTTP request).

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the header name `headerName` or the pointer to the length of the header name `headerNameLth` or the pointer to the buffer for the header value `headerValue` or the pointer to the length of the header value `headerValueLth` is NULL.

KC_HTTP_INVALID_LENGTH

The value of the length of header name `headerNameLth` or value of the length of header value `headerValueLth` is lower or equal 0.

KC_HTTP_RESULT_TRUNCATED

The length of the buffer for the header name and/or header value is less than the actual length of the name and /or value. The character strings are truncated and the actual lengths are returned.

8.1.2 Function kcHttpGetHeaderByName

The function `kcHttpGetHeaderByName` returns the value of an HTTP header field which is specified by its name. The header field `Authorization` can not be read.

This function may be called both in program unit and HTTP exit program. In the program unit the function may only called in the first program unit run of a service.

Function declaration `kcHttpGetHeaderByName`

```
kc_http_retcode kcHttpGetHeaderByName( char * headerName,
                                       char * headerValue,
                                       int * headerValueLth
                                       );
```

This function has following function parameter:

- >> `headerName` The name of the HTTP header field to be read.
- << `headerValue` The pointer to a buffer in which the value of the HTTP header field is returned. The length of the buffer must be at least `headerValueLth` bytes.
- <> `headerValueLth` The pointer to a variable in which the length of the buffer for the value of the HTTP header is passed and the actual length of the value is returned.

Description of returned value of function call:

KC_HTTP_OK

The function has successfully terminated.

KC_HTTP_FUNCTION_CALL_NOT_ALLOWED

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

KC_HTTP_NO_HTTP_CLIENT

The calling service was not initiated by an HTTP client.

KC_HTTP_HEADER_NAME_NULL_OR_EMPTY

The pointer to the header name `headerName` is NULL or the name is empty.

KC_HTTP_PARAM_VALUE_NULL

The pointer to the buffer for the header value `headerValue` or the pointer to the length of the header value `headerValueLth` is NULL.

KC_HTTP_INVALID_LENGTH

The value of the length of header value `headerValueLth` is lower or equal 0.

KC_HTTP_HEADER_NOT_FOUND

There is no HTTP header with the name specified in `headerName`.

KC_HTTP_RESULT_TRUNCATED

The length of the buffer for the header value is less than the actual length of the value. The header value is truncated and the actual length is returned.

8.1.3 Function kcHttpGetHeaderCount

The function `kcHttpGetHeaderCount` returns the number of HTTP header fields contained in the HTTP request. Any `Authorization` header field contained in the HTTP request is not counted, since this header field cannot be read.

This function may be called both in program unit and HTTP exit program.
In the program unit the function may only called in the first program unit run of a service.

Function declaration `kcHttpGetHeaderCount`

```
int kcHttpGetHeaderCount( void);
```

Meaning of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

8.1.4 Function kcHttpGetMethod

The function `kcHttpGetMethod` returns the HTTP method of the HTTP request.

This function may be called both in program unit and HTTP exit program.

In the program unit the function may only called in the first program unit run of a service.

Function declaration `kcHttpGetMethod`

```
kc_http_retcode kcHttpGetMethod( char *  methodName,
                                int *   methodNameLth
                                );
```

This function has following function parameter:

- << `methodName` The pointer to a buffer in which the method of the HTTP request is returned. The length of the buffer must be at least `methodNameLth` bytes.
- <> `methodNameLth` The pointer to a variable in which the length of the buffer for the method of the HTTP request is passed and the actual length of the method is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the method `methodName` or the pointer to the length of the method `methodNameLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of the length of method `methodNameLth` is lower or equal 0.

`KC_HTTP_RESULT_TRUNCATED`

The length of the buffer for the method is less than the actual length of the method. The method is truncated and the actual length is returned.

8.1.5 Function kcHttpGetMputMsg

The function `kcHttpGetMputMsg` returns the pointer to MPUT message provided by the program unit and its length.

This function may only called by an HTTP exit program when processing the output message.

Function declaration `kcHttpGetMputMsg`

```
kc_http_retcode kcHttpGetMputMsg( void **  mputMessage,  
                                  int *    mputMessageLth  
                                  );
```

This function has following function parameter:

- << `mputMessage` The pointer to a variable where the pointer to the MPUT message is returned.
- << `mputMessageLth` The pointer to a variable where the length of the MPUT message is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was not called by an HTTP exit program during processing the output message.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the variable `mputMessage` or the pointer to variable `mputMessageLth` is NULL.

8.1.6 Function kcHttpGetPath

The function `kcHttpGetPath` returns the path of the HTTP request normalized with `KC_HTTP_NORM_UNRESERVED`.

This function may be called both in program unit and HTTP exit program.
In the program unit the function may only be called in the first program unit run of a service.

Function declaration `kcHttpGetPath`

```
kc_http_retcode kcHttpGetPath( char * httpPath,  
                               int * httpPathLth  
                               );
```

This function has following function parameter:

- << `httpPath` The pointer to a buffer in which the path of the HTTP request is returned. The length of the buffer must be at least `httpPathLth` bytes.
- <> `httpPathLth` The pointer to a variable in which the length of the buffer for the path of the HTTP request is passed and the actual length of the path is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the path `httpPath` or the pointer to the length of the path `httpPathLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of the length of path `httpPathLth` is lower or equal 0.

`KC_HTTP_RESULT_TRUNCATED`

The length of the buffer for the path is less than the actual length of the path. The path is truncated and the actual length is returned.

8.1.7 Function kcHttpGetQuery

The function `kcHttpGetQuery` returns the query of the HTTP request normalized with `KC_HTTP_NORM_UNRESERVED`.

This function may be called both in program unit and HTTP exit program.
In the program unit the function may only called in the first program unit run of a service.

Function declaration `kcHttpGetQuery`

```
kc_http_retcode kcHttpGetQuery( char * httpQuery,
                               int * httpQueryLth
                               );
```

This function has following function parameter:

- << `httpQuery` The pointer to a buffer in which the query of the HTTP request is returned. The length of the buffer must be at least `httpQueryLth` bytes.
- <> `httpQueryLth` The pointer to a variable in which the length of the buffer for the query of the HTTP request is passed and the actual length of the query is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the query `httpQuery` or the pointer to the length of the query `httpQueryLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of the length of query `httpQueryLth` is lower or equal 0.

`KC_HTTP_RESULT_TRUNCATED`

The length of the buffer for the query is less than the actual length of the query. The query is truncated and the actual length is returned.

8.1.8 Function kcHttpGetRc2String

The help function `kcHttpGetRc2String` returns as function result the name of the passed value followed by this value in parenthesis as printable null-terminated string.

Function declaration `kcHttpGetRc2String`

```
char * kcHttpGetRc2String( kc_http_retcode httpRc);
```

This function has following parameters:

>> `httpRc` Value from enum `kc_http_retcode`.

Example

```
printf("Return code is %s.", kcHttpGetRc2String( KC_HTTP_HEADER_NAME_TOO_LONG));
```

Output

```
Return code is KC_HTTP_HEADER_NAME_TOO_LONG (-7).
```

8.1.9 Function kcHttpGetReqMsgBody

The function `kcHttpGetReqMsgBody` returns the pointer to the message body of an HTTP request and its length.

This function may be called both in program unit and HTTP exit program.

In the program unit the function may only called in the first program unit run of a service and in the HTTP exit program only when processing the input message.

Function declaration `kcHttpGetReqMsgBody`

```
kc_http_retcode kcHttpGetReqMsgBody( void ** reqMessageBody,  
                                     int *   reqMessageBodyLth  
                                     );
```

This function has following function parameter:

- << `reqMessageBody` The pointer to a variable where the pointer to the message body of the HTTP request is returned.
- << `reqMessageBodyLth` The pointer to a variable where the length of the message body of the HTTP request is returned.

Description of returned value of function call:

KC_HTTP_OK

The function has successfully terminated.

KC_HTTP_FUNCTION_CALL_NOT_ALLOWED

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or by an HTTP exit program during processing of the output message.

KC_HTTP_NO_HTTP_CLIENT

The calling service was not initiated by an HTTP client.

KC_HTTP_PARAM_VALUE_NULL

The pointer to the variable `reqMessageBody` or the pointer to the variable `reqMessageBodyLth` is NULL.

8.1.10 Function kcHttpGetScheme

The function `kcHttpGetScheme` returns the scheme of the HTTP request. The scheme is returned in the form in which it is contained in the URL, e.g. 'https'.

This function may be called both in program unit and HTTP exit program.

In the program unit the function may only be called in the first program unit run of a service.

Function declaration `kcHttpGetScheme`

```
kc_http_retcode kcHttpGetScheme( char *  scheme,
                                int *   schemeLth
                                );
```

This function has following function parameter:

- << `scheme` The pointer to a buffer in which the scheme of the HTTP request is returned. The length of the buffer must be at least `schemeLth` bytes.
- <> `schemeLth` The pointer to a variable in which the length of the buffer for the scheme of the HTTP request is passed and the actual length of the scheme is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the scheme `scheme` or the pointer to the length of the scheme `schemeLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of the length of scheme `schemeLth` is lower or equal 0.

`KC_HTTP_RESULT_TRUNCATED`

The length of the buffer for the scheme is less than the actual length of the scheme. The scheme is truncated and the actual length is returned.

8.1.11 Function kcHttpGetVersion

The function `kcHttpGetVersion` returns the version of the HTTP request. The version is returned in the form in which it is contained in the HTTP protocol, e.g. 'HTTP/1.1'.

This function may be called both in program unit and HTTP exit program.

In the program unit the function may only be called in the first program unit run of a service.

Function declaration `kcHttpGetVersion`

```
kc_http_retcode kcHttpGetVersion( char *  httpVersion,
                                int *   httpVersionLth
                                );
```

This function has following function parameter:

- << `httpVersion` The pointer to a buffer in which the version of the HTTP request is returned. The length of the buffer must be at least `httpVersionLth` bytes.
- <> `httpVersionLth` The pointer to a variable in which the length of the buffer for the version of the HTTP request is passed and the actual length of the version is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or not in the first program unit run or outside an HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the buffer for the version `httpVersion` or the pointer to the length of the version `httpVersionLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of the length of version `httpVersionLth` is lower or equal 0.

`KC_HTTP_RESULT_TRUNCATED`

The length of the buffer for the version is less than the actual length of the version. The version is truncated and the actual length is returned.

8.1.12 Function kcHttpPercentDecode

The function `kcHttpPercentDecode` converts percent-encoded characters, which are contained in the given character strings, in their normal one-character representation.

In the URL of an HTTP request, individual characters can be contained in their percent-encoded representation. This mechanism is described in more detail in RFC 3986 "Uniform Resource Identifier". Certain US ASCII characters are represented in their sedecimal representation. Such a substitute representation is preceded by a percent sign ("%"); e.g. a space can be represented as %20 or the character tilde ("-") by the character string %7E. The function `kcHttpPercentDecode` can be used to normalize the query of an HTTP request.

Function declaration kcHttpPercentDecode

```
typedef enum
{
    KC_HTTP_NORM_MINIMUM                = 1
    , KC_HTTP_NORM_SPACE_ONLY           = 2
    , KC_HTTP_NORM_UNRESERVED           = 4
    , KC_HTTP_NORM_RESERVED             = 8
    , KC_HTTP_NORM_ALL_BUT_PERCENT      = 16
    , KC_HTTP_NORM_ALL                  = 32
} kc_http_norm;

kc_http_retcode kcHttpPercentDecode( kc_http_norm  normFlags,
                                     char *        bufferUrl,
                                     int            inputLth,
                                     int *         outputLth
                                     );
```

This function has following parameters:

- >> `normFlags` Value from enum `kc_http_norm` which determines the scope of the requested decoding.
- << `bufferUrl` The pointer to a buffer in which the encoded string is passed and the decoded string is returned. The buffer must be at least `inputLth` bytes long.
- >> `inputLth` The length of the encoded string.
- << `outputLth` The pointer to a variable in which the length of the decoded string is returned.

The parameter `normFlags` defines the scope of the requested decoding.

`normFlags` can have the following values:

KC_HTTP_NORM_MINIMUM

With this value, only "case normalization" is performed, i.e. the two letters following a % character are converted to capital letters..

KC_HTTP_NORM_SPACE_ONLY

With this value, in addition to `KC_HTTP_NORM_MINIMUM`, all "%20" encodings are replaced by spaces.

KC_HTTP_NORM_UNRESERVED

With this value, in addition to `KC_HTTP_NORM_SPACE_ONLY`, all percent-encoded Unreserved Characters are replaced by their "normal" one-character representation. For the definition of Unreserved Characters see RFC 3986 "Uniform Resource Identifier".

KC_HTTP_NORM_RESERVED

With this value, in addition to KC_HTTP_NORM_UNRESERVED, all percent-encoded Reserved Characters are replaced by their "normal" one-character representation. For the definition of Reserved Characters see RFC 3986 "Uniform Resource Identifier".

KC_HTTP_NORM_ALL_BUT_PERCENT

With this value, in addition to KC_HTTP_NORM_RESERVED, all percent-encoded characters except %25 ("%") are replaced by their "normal" one-character representation.

KC_HTTP_NORM_ALL

With this value, all percent-encoded characters are replaced by their "normal" one-character representation.

Meaning of returned value of function call:

KC_HTTP_OK

The function has successfully terminated.

KC_HTTP_PARAM_VALUE_NULL

The pointer to the buffer `bufferUrl` or the pointer to the length of the decoded string `outputLth` is NULL.

KC_HTTP_INVALID_LENGTH

The length of the encoded string `inputLth` is lower 0 or the encoded string contains a null byte (0).

KC_HTTP_NORMALIZATION_ERROR

An invalid value was passed in parameter `normFlags` or an error occurred during normalization.

KC_HTTP_PARAM_INVALID_URLSTRING

The encoded string contains a percent sign ("%") but one of the next two characters is not a printable hexadecimal number.

8.1.13 Function kcHttpPutHeader

You can use the function `kcHttpPutHeader` to pass the name and value of an HTTP header field for the HTTP response.

The length of the header name and the length of the header value are each limited to 256 bytes. The number of header fields for an HTTP response is limited to 100. The total length of the headers, including the control characters (CLRF), is limited to 7,000 bytes.

The header name can be specified in any upper/lower case and is sent as it was specified. It is not recognized if the same header is passed multiple times. The values are therefore not summarized, but all headers are sent individually.

i Some HTTP header fields are set by openUTM, if they are not passed by the application program. Some HTTP header fields are always set by openUTM and must not be passed by the application program. See details in chapter "[Setting of HTTP Headers](#)".

This function may be called both in program unit and HTTP exit program. In the HTTP exit program, the function can only be called when processing the output message.

If this function is called in a program unit run, in the same program unit run an output message has to be supplied by MPUT and the service has to be finished else the header information is lost.

Function declaration kcHttpPutHeader

```
kc_http_retcode kcHttpPutHeader( char * headerName,
                                char * headerValue
                                );
```

This function has following function parameter:

>> `headerName` The pointer to the name of the HTTP header field for the HTTP response.

>> `headerValue` The pointer to the value of the HTTP header field for the HTTP response.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or outside the HTTP exit program.

`KC_HTTP_NO_HTTP_CLIENT`

The calling service was not initiated by an HTTP client.

`KC_HTTP_HEADER_NAME_NULL_OR_EMPTY`

The pointer to the header name `headerName` is NULL or the header name is empty.

`KC_HTTP_HEADER_VALUE_NULL_OR_EMPTY`

The pointer to the header value `headerValue` is NULL or the header value is empty.

KC_HTTP_HEADER_NAME_TOO_LONG

The specified header name is too long.

KC_HTTP_HEADER_VALUE_TOO_LONG

The specified HTTP header value is too long.

KC_HTTP_HEADER_NOT_ALLOWED

The specified HTTP header name must not be passed to UTM.

KC_HTTP_MAX_HEADER_COUNT

The maximum number of headers was exceeded.

KC_HTTP_MAX_HEADER_TOTAL_LENGTH

The maximum length of all headers including control characters was exceeded.

KC_HTTP_HEADER_NAME_NOT_PRINTABLE

The name contains a non-printable character.

KC_HTTP_HEADER_VALUE_NOT_PRINTABLE

The value contains a non-printable character.

8.1.14 Function kcHttpPutMgetMsg

An HTTP exit program can use the function `kcHttpPutMgetMsg` to create a message for the program unit, which can be read with MGET.

The message can be built up successively with several calls of the function, without the caller himself having to take care of the request and administration of the required memory. How to structure this message into message segments that can be read in the program unit with MGET NT is described in chapter "[Event exit HTTP](#)".

This function may only called by an HTTP exit program when processing the input message.

Function declaration `kcHttpPutMgetMsg`

```
kc_http_retcode kcHttpPutMgetMsg( void *   mgetMessage,
                                   int     mgetMessageLth,
                                   void **  totalMgetMessage,
                                   int *    totalMgetMessageLth
                                   );
```

This function has following function parameter:

>> <code>mgetMessage</code>	The pointer to the passed (part of) message.
>> <code>mgetMessageLth</code>	The length of the passed (part of) message.
<< <code>totalMgetMessage</code>	The pointer to a variable in which the pointer to the complete message built so far is returned.
<< <code>totalMgetMessageLth</code>	The pointer to a variable in which the length of the complete message built so far is returned.

Description of returned value of function call:

KC_HTTP_OK

The function has successfully terminated.

KC_HTTP_FUNCTION_CALL_NOT_ALLOWED

The function was not called by an HTTP exit program during processing the input message.

KC_HTTP_PARAM_VALUE_NULL

The pointer to the passed message `mgetMessage`, the pointer to the variable `totalMgetMessage` or the pointer to variable `totalMgetMessageLth` is NULL.

KC_HTTP_INVALID_LENGTH

The value of parameter `mgetMessageLth` is lower or equal 0.

KC_HTTP_MEMORY_INSUFFICIENT

No further memory could be allocated for the complete message.

8.1.15 Function kcHttpPutRspMsgBody

You can use the function `kcHttpPutRspMsgBody` to create the message body of the HTTP response. The message body can be built up successively with several calls of the function, without the caller himself having to take care of the request and administration of the required memory.

This function may only be called by an HTTP exit program when processing the output message.

Function declaration `kcHttpPutRspMsgBody`

```
kc_http_retcode kcHttpPutRspMsgBody( void *   rspMessageBody,
                                     int     rspMessageBodyLth,
                                     void ** totalRspMessageBody,
                                     int *   totalRspMessageBodyLth
                                     );
```

This function has following function parameter:

- >> `rspMessageBody` The pointer to the passed (part of) message body.
- >> `rspMessageBodyLth` The length of the passed (part of) message body.
- << `totalRspMessageBody` The pointer to a variable in which the pointer to the complete message body built so far is returned.
- << `totalRspMessageBodyLth` The pointer to a variable in which the length of the complete message body built so far is returned.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was not called by an HTTP exit program during processing the output message.

`KC_HTTP_PARAM_VALUE_NULL`

The pointer to the passed message `rspMessageBody`, the pointer to the variable `totalRspMessageBody` or the the pointer to variable `totalRspMessageBodyLth` is NULL.

`KC_HTTP_INVALID_LENGTH`

The value of parameter `rspMessageBodyLth` is lower or equal 0.

`KC_HTTP_MEMORY_INSUFFICIENT`

Memory allocation failed.

8.1.16 Function kcHttpPutStatus

You can use the function `kcHttpPutStatus` to pass an HTTP status code for the HTTP response. Additionally a reason phrase may be passed.

The length of the reason phrase is restricted to 256 bytes. If NULL is passed for the reason phrase UTM will supply a default reason phrase for the specified status code.

The following status codes must not be passed:

- 100 Continue
- 101 Switching Protocols
- 203 Non-Authoritative Information
- 301 Moved Permanently
- 302 Found
- 307 Temporary Redirect
- 401 Unauthorized
- 407 Proxy Authentication Required
- 408 Request Timeout
- 411 Length Required
- 413 Request Entity Too Large
- 417 Expectation Failed
- 502 Bad Gateway
- 504 Gateway Timeout
- 505 HTTP Version Not Supported

This function may be called both in program unit and HTTP exit program. In the HTTP exit program, the function can only be called when processing the output message.

If this function is called in a program unit run, in the same program unit run an output message has to be supplied by MPUT and the service has to be finished else the header information is lost.

Function declaration kcHttpPutStatus

```
kc_http_retcode kcHttpPutStatus( int    statusCode,
                                char *  reasonPhrase
                                );
```

This function has following function parameter:

- >> `statusCode` Status code for the HTTP response.
- >> `reasonPhrase` Pointer to the buffer containing the reason phrase for the HTTP response or NULL.

Description of returned value of function call:

`KC_HTTP_OK`

The function has successfully terminated.

`KC_HTTP_FUNCTION_CALL_NOT_ALLOWED`

The function was called by the KDCS program unit before the KDCS call INIT was executed or outside the HTTP exit program.

KC_HTTP_NO_HTTP_CLIENT

The calling service was not initiated by an HTTP client.

KC_HTTP_INVALID_STATUS_CODE

The specified status code is invalid.

KC_HTTP_STATUS_CODE_NOT_ALLOWED

The specified status code must not passed to UTM.

KC_HTTP_REASON_PHRASE_TOO_LONG

The specified reason phrase is too long.

KC_HTTP_REASON_PHRASE_NOT_PRINTABLE

The reason phrase contains a non printable character.

8.2 Addressing TAC

An HTTP client can address a service of a UTM application in different ways. On the one hand, the TAC of the called service can be specified directly in the path of the URL. Alternatively, you can use the openUTM generation to map path specifications in a URL to a TAC. The assignment of a path to a TAC of the UTM application is done with the KDCDEF statement HTTP-DESCRIPTOR.

When an HTTP request is received in a UTM application, the TAC is selected in the following sequence: openUTM first searches for the path of an HTTP request in the HTTP descriptors assigned to the BCAMAPPL via which the request was received. If the path is not found there, openUTM searches the HTTP descriptors generated with BCAMAPPL=*ALL. If the path is not found there either, openUTM checks whether the path corresponds to a generated TAC. If this also does not apply, openUTM determines whether a path is generated with "/*", first for the BCAMAPPL via which the request was received, then for BCAMAPPL=*ALL.

8.3 Evaluation of the HTTP Header of an HTTP request

openUTM evaluates the following header fields in an HTTP request. If the HTTP request contains additional HTTP headers, these are not evaluated by openUTM. However, an application program can read and evaluate these headers with the functions `kcHttpGetHeaderByIndex` or `kcHttpGetHeaderByName`.

In the following list of header fields evaluated by openUTM, the header fields that can be included in an HTTP request are marked as "Optional" and the header fields that must be included in an HTTP request are marked as "Mandatory":

- **Accept**

Optional

With this header a client expresses its expectations concerning the representation of the reply message.

openUTM uses this header to format the output message if no HTTP descriptor or an HTTP descriptor with HTTP-EXIT=*SYSTEM specification was found. The header value is searched for these patterns in the following order:

1. *text/html*
2. *text/plain*
3. *text/** (effect like *text/html*)
4. *application/octet-stream*

If none of these values are found, the output message is treated like *text/html*.

- **Accept-Charset**

Optional

With this header a client expresses its expectations regarding the coding of the response message.

BS2000 systems:

The header value is searched for a generated CHAR-SET name. The first CHAR-SET alias found determines the code conversion of the output message. If no CHAR-SET name is found, the default conversion of openUTM is used.

Unix, Linux and Windows systems:

No evaluation done by openUTM. On Unix, Linux and Windows systems there is no code conversion of the output message.

- **Authorization**

Optional

In this header, a client can pass authentication data to openUTM.

If this header is specified, the value must begin with "basic ". <userid>:<password> must be base64 encoded.

Otherwise the request will be rejected with status code "400 invalid http header format".

- **Connection**

Optional

This header allows a client to specify whether or not the server should terminate the connection after sending the response message.

Only the header value "keep-alive" is evaluated. If this value is specified, openUTM does not close the connection to the client after sending the output message. Otherwise the connection will be terminated by openUTM after sending the HTTP response.

- **Content-Length**

Mandatory if the request contains a message body.

The HTTP client must supply this header with the correct length of the message body.

If an HTTP request is received with a message body and no content length header is specified, the message body is ignored.

- **Content-Type**

Optional

This header field describes the MIME type of the message contained in the message body.

BS2000 systems:

If an HTTP descriptor is found for the path that is generated with CONVERT-TEXT=*YES, a generated CHAR-SET name specified after "charset=" determines the code conversion of the input message, unless APPLICATION/OCTET-STREAM is found. If no CHAR-SET name is found, the standard conversion of the input message takes place.

Unix, Linux and Windows systems:

No evaluation by openUTM. On Unix, Linux and Windows systems there is no code conversion of the input message.

- **Expect**

Optional

With this header, a client can request the server to check the correctness of the sent HTTP request before the client sends the message body.

The header value must be "100-continue". In this case, the HTTP client can wait for the openUTM response with status code 100 before sending the message body. If the header value is not "100-continue", the HTTP request is rejected with status code "417 expectation failed".

- **Host**

Mandatory

An HTTP client must supply this header with the name of the HTTP server.

- **Transfer-Encoding**

Optional

If this header is specified, then the value must be "identity". Otherwise, the request is rejected with status code "501 transfer encoding rejected".

8.4 Setting the HTTP Header of an HTTP Response

openUTM sets a number of header fields in an HTTP response. A distinction is made between header fields that must not be set by the user, and header fields that are only set by openUTM if they have not been set by the user.

List of header fields set by openUTM in an HTTP response that must not be set by the user:

- **Connection**
Specifies whether the connection is terminated by the HTTP server after sending the HTTP response.
openUTM always set this header field to the value "close", unless the client has set "keep-alive" in the HTTP request header connection.
- **Content-Length**
Length of the message body.
- **Date**
Date and time at the time of transmission.
Example: Mon, 28 Oct 2019 14:38:45 GMT
- **Server**
Information about the UTM HTTP server in the form: "UTM HTTP SERVER openUTM version application name platform."
Example: UTM HTTP-SERVER V07.0A00 SAMPLE Linux Intel

List of header fields in an HTTP response that are only set by openUTM if they have not been set by the user:

- **Cache-Control**
Specifies whether and for how long the response may be stored by the client or by gateway hosts and reused as a response for subsequent identical requests.
By default, openUTM provides this header field with the value "no-cache, no-store, must-revalidate".

- **Content-Type**

Specifies the MIME type and, if necessary, the character set of the message body.

openUTM set this header field as follows:

- *text/html;charset=*

- if the TAC started by the HTTP request was selected without an HTTP descriptor or using an HTTP descriptor with HTTP EXIT=*SYSTEM and
and
- the request did not contain the HTTP header field Accept or the value of the header contained *text/html* or *text/**, but not *text/plain* or neither *text/...* nor *application/octet-stream*.

- *text/plain;charset=*

if the TAC started by the HTTP request was selected

- using an HTTP descriptor with HTTP-EXIT not equal to *SYSTEM and CONVERT-TEXT = *YES or
- without an HTTP descriptor or an HTTP descriptor with HTTP-EXIT=*SYSTEM and the request contained the HTTP header field Accept with the value *text/plain* but not *text/html*.

- *application/octet-stream*

if the TAC started by the HTTP request was selected

- using an HTTP descriptor with HTTP-EXIT not equal to *SYSTEM and CONVERT-TEXT = *NO or
- without an HTTP descriptor or using an HTTP descriptor with HTTP EXIT=*SYSTEM and the request contained the HTTP header field Accept with the value *application/octet-stream* but not *text/...*

- *charset=*

If the HTTP header field Content-type has the value *text/html* or *text/plain*, then the *charset* parameter is supplied as follows:

Unix, Linux and Windows systems:

charset=ISO-8859-1

BS2000 systems:

charset=<charset-name>

- If the TAC started by the HTTP request was selected without an HTTP descriptor or using an HTTP descriptor with CONVERT-TEXT=*YES and the request contained the HTTP header field Accept-Charset and the value of the header contained a name generated with CHAR-SET *<charset-name>*.
- if the TAC started by the HTTP request was selected using an HTTP descriptor with CONVERT-TEXT=*YES and the request contained the Content-Type header and the value of the header contained a name generated with CHAR-SET *<charset-name>* and the request did not contain the HTTP header field Accept or the value of the header did not contain a name generated with CHAR-SET.

charset=ISO-8859-1

else

- **X-Content-Type-Options**

Prohibits MIME sniffing.

openUTM set this header field to the value "nosniff".

- **X-Frame-Options**

Protection against clickjacking.

openUTM set this header field to the value "deny".

- **X-Xss-Protection**

Filter for cross-site scripting.

openUTM set this header field to the value "1".

8.5 Specifics of communicating with HTTP clients

The specifics listed below must be observed when communicating with HTTP clients:

1. HTTP clients may only call one-step dialog operations.
2. The following restrictions apply to HTTP messages:
 - a. The request line and the status line must not be larger than 2KB.
 - b. The length of all headers must not be greater than 8KB.
 - c. An HTTP message may contain a maximum of 100 headers.
 - d. The length of a message is limited to a maximum of 32,700 bytes.
 - e. The length of a message body is limited to a maximum of 32,000 bytes.
3. No logon procedure may be configured for HTTP clients.
4. When handling K messages, the message target PARTNER is not evaluated for HTTP clients. Instead, K Messages sent to HTTP Clients, independently of the configured message targets are only output if a K message is required as a dialog response to the HTTP client.
Examples are the messages K017, which is sent to a client when a process terminates, and K034, which is sent when a distributed transaction is reset.
5. openUTM does not use cookies.
6. Asynchronous messages cannot be sent to HTTP clients.
7. A screen restart (KDCDISP, KDCLAST) is not possible for HTTP clients.

8.6 Behaviour in error situations

- When an HTTP request is received with methods other than POST, GET, PUT and DELETE, it is rejected by openUTM with HTTP status code "501 Method Not Implemented".
- If no TAC can be assigned to an HTTP request, it is rejected by openUTM with HTTP status code "404 Not Found".
- When an invalid HTTP request is received, the connection to the HTTP client is terminated after a negative HTTP response has been sent.



An overview of the HTTP status codes used by openUTM in error situations can be found in the chapter "HTTP Status Codes" in the openUTM manual "Messages, Debugging and Diagnostics".

9 Event functions

In order to be able to react to certain events in a program, openUTM permits the use of what are known as event functions. Unlike “normal” program units which are called by specifying a transaction code, openUTM starts these program units when certain events occur.

There are two different types of event functions:

- event exits, which **must not contain any KDCS calls** and
- event services, which **must contain KDCS calls**.

Note for BS2000 systems

Since STXIT routines such as those used on BS2000 systems are also event-driven, a description of these routines has also been included in this manual in section “[STXIT routines \(BS2000 systems\)](#)”. The section “[Event handling in ILCS programs \(BS2000 systems\)](#)” deals with event handling in ILCS programs.

Event exits:

INPUT	This event exit is called with input from a data display terminal.
HTTP	This event exit is called when the input message is read from and before the HTTP response is sent to an HTTP client.
START	These event exits (up to 8) are called at each start of the application program.
SHUT	These event exits (up to 8) are called at each termination of an application work process, including at PEND ER.
VORGANG	This program unit is called at the start and the end of a service, and also in the case of incorrect termination or termination caused by loss of connection or in the case of a service restart.
FORMAT	Only on BS2000 systems: This event exit is called if a message is entered or output which you then want to format using a formatting routine of your own (-format).

Event services:

BADTACS	This dialog service is called whenever an invalid transaction code is entered at a terminal or a TS application or data protection is violated.
MSGTAC	This asynchronous service is called whenever openUTM outputs a message with MSGTAC defined as its destination (see the openUTM manual “Messages, Debugging and Diagnostics”, the section describing the modification of output messages).
SIGNON	This dialog service is called whenever a terminal user, a TS application or a UPIC client signs on to the application. The prerequisite for this is that a signon service must be generated for the transport system access point via which the client signs on; in addition, UPIC= YES must be generated in the SIGNON statement for UPIC clients.

For each transport system access point of a UTM application (generated with MAX APPLNAME or BCAMAPPL), a separate sign-on service can be generated (see the SIGNON-TAC parameter of the BCAMAPPL statement in the openUTM manual “Generating Applications”).

Database calls are only allowed in the program units for VORGANG, BADTACS, MSGTAC and SIGNON, and not in the case of program units for INPUT, START and SHUT.

Only on BS2000 systems: Database calls are not permitted in FORMAT program units.

9.1 Event exits

Event exits are created as subroutines without KDCS calls. This section describes the following event exits:

INPUT
HTTP
START
SHUT
VORGANG
FORMAT (only on BS2000 systems)

The event exits INPUT, START, SHUT and FORMAT are defined with the KDCDEF statement EXIT. You can define the event exit VORGANG with the TAC and PROGRAM statement.

Of these five event exits, database calls are permitted only in the VORGANG exit.

Reading the application name

An event exit is able to read the name of the own application by calling the KDCAPLI entry, see the following example:

Assembler Program

```
                EXTRN  KDCAPLI  
AKDCAPLI DC     A(KDCAPLI)
```

C Program

```
extern char KDCAPLI[8];
```

9.1.1 Event exit INPUT

You can use this event exit to determine the effect of terminal input.

openUTM calls the event exit INPUT - with a few exceptions - every time input is made at a terminal. The exceptions are as follows:

- input if no user is as yet signed on
- input in the event service SIGNON
- input using a function key generated with
- input after a program has issued the call SIGN OB/OF.

openUTM passes the address of the parameter area, comprising an input area and an output area, to the program for an INPUT exit.

Programming language-specific data structures are available for declarations in the parameter area: COBOL uses the COPY member KCINPC, whereas C/C++ use the header file *kcinp.h*. For an explanation of the individual fields in the parameter area and the meanings of these fields, see pages from table "[Parameter area KDCINPC/kdcinp.h](#)".

On BS2000 systems, openUTM also passes a second parameter to the input exit containing additional input fields. Once again, a programming language-specific data structure is available for the structure of the second parameter as well: the COBOL structure is the COPY member KCCFC; the C/C++ structure is the header file *kccf.h*. The second parameter area is described on pages from section "[Second parameter area KCCFC/kccf.h \(BS2000 systems\)](#)".

The program analyzes the values entered in the input area and sets the output area accordingly. Depending on the values entered in the output area, openUTM decides which of the following actions is to be executed:

- continue the service or
- start a new service or
- stack a service and start a new service or
- execute a user command, e.g. KDCOFF or
- send a message with error information to the terminal.

Possible applications

The input exit provides the terminal interface with greater freedom regarding the layout of the user interface.

- Position of transaction codes or KDC commands in the message:
transaction codes or KDC commands do not have to appear at the start of a message.
- Visibility of transaction codes on screen:
The Transaction code has not to be visible on screen if you want to start a service. For example, a menu might offer a number of activities. The terminal user enters a text or a number to choose one of them. This input itself does not have to be a transaction code: it is only the INPUT exit which converts it to a transaction code (a service TAC). In this way transaction codes, which are an element of generation information, become independent of the dialog interface.
- Representation of command names:
There is no need to specify "KDC..." in order to issue a KDC command.
If it is felt to be useful, commands can be represented in some other form, e.g. "/" instead of "KDC".

Parameter area KDCINPC/kdcinp.h	
Input area (supplied by openUTM)	
Field name	Contents
KCIFCH	First 8 characters of the input
KCIMF/kcifn	Format identifier
KCICVTAC	Service transaction code
KCICVST	Service status
KCIFKEY	Value of F key: 1,...,20 / binary zero
KCIKKEY	Binary zero / on BS2000 systems: value of K key: 1,...,20
KCICFINF: "NO"/"MO"/"ON"/"UN" ¹	Formatting information
KCILTERM	Current LTERM partner
KCIUSER	Current user ID
Output area (supplied by the INPUT exit)	
Field name	Contents
KCINTAC or KCINCMD	Next service TAC or next user command
KCICCD	Code for the effect of the input: "ER"/"CC"/"SC"/"ST"/"CD"
KCICUT	Truncate TAC: "Y"/"N"
KCIERRCD	Error info for terminal (4 bytes)

¹ "MO" / "ON" / "UN" (only on BS2000 systems)

openUTM enters the following values in the appropriate fields of the input area:

KCIFCH

the first 8 characters of the input, at most, however, up to the first blank.

KCIMF/kcifn

the format identifier:

- Blanks in line mode or
- the format identifier of the format on the screen (only on BS2000 systems).

Only on BS2000 systems: The field **KCIMF/kcifn** can also contain the format identifier #!POPUP. #!POPUP indicates that a box “pops up” on screen. You can use the FHS service function KDCFHS with the USER-CODE INFD to display the names of all formats on the screen.

KCICVTAC

the transaction code used to start the current service (if any).

KCICVST

the service status:

- **ES**(End of dialog **S**tep)
End of the dialog step with PEND KP or PGWT KP
- **ET**(End of **T**ransaction)
End of the transaction with PEND RE
- **RS**(Return from **S**tack)
End of the inserted service; the input is intended for the stacked service.
- **EC**(End of **C**onversation)
The last dialog step was terminated with PEND FI; the input is intended for a new service.

KCIFKEY

the value of the F key (1 - 20, on BS2000 systems: 1 - 24) if pressed, otherwise binary zero.

KCIKKEY

binary zero

or (on BS2000 systems) the value of the K key (1 - 14), if pressed

KCICFINF

Information of the formatting system:

- **NO** (**NO** control field)
 - The input does not contain any control fields; either the input was in line mode
 - or (on BS2000 systems) the format does not contain any control fields or one of the control fields was empty.

Only on BS2000 systems:

- **MO** (**MO**re control fields)
The input contains several control fields.
- **ON** (**ON**e control field)
The input contains exactly one control field.
- **UN** (**UN**successful)
Input could not be formatted.
Therefore no control field specifications were possible; this entry is made, for instance, after input in a format fetched with KDCOUT

KCILTERM

name of the LTERM partner via which the terminal is connected.

KCIUSER

the current user ID.**KCICVST**

You input the following in the fields of the output area:

KCINTAC

if a new service is to be started: the TAC of the program unit which starts the next service.

KCINCMD

if a user command is to be executed: the user command (KDC command).

Blanks have to be entered in the case of an error message (KCICCD = ER) or continuation of the service (KCICCD = CC, follow-up TAC is entered with PEND!).

KCICCD

depending on the required effect of the input:

- **ER (ERror indication)**
for an error message to the data display terminal. You can then enter an insert in the KCIERRCD field for this message.
- **CC (Continue Conversation)**
for continuing the service. This must not be specified after end of service (KCICVST = EC).
- **SC (Start new Conversation)**
if a new service is to be started; only allowed after end of service (KCICVST = EC).
- **ST (STack Conversation)**
if the current service is to be stacked and a new service is to be started; allowed only at end of transaction (KCICVST = ET/RS).
- **CD (process CommanD)**
if openUTM is to execute a user command.

KCICUT

the value Y if the TAC is to be truncated at the start of a service (permissible only where KCICCD = SC/ST), otherwise N.

KCIERRCD

a character string of up to 4 bytes to be sent to the terminal with the UTM message K098 if KCICCD=ER. Otherwise (KCICCD != ER) blank.

Second parameter area KCCFC/kccf.h (BS2000 systems)

openUTM uses the second parameter to pass the contents of the control fields from the screen formats to the program unit - which is why this second parameter area is also referred to as the control field area. openUTM can use the field KCCFS to pass input made in various control fields for a format (and even in different subformats of a format).

The first two fields, KCCFCREM and KCCFCFLD, correspond to the control field area in earlier openUTM versions. They have been kept for compatibility reasons. The fields KCCFNOCF and KCCFS are relevant.

The table below illustrates the structure of the control field area in which openUTM makes the input parameters available:

Second parameter area (supplied by openUTM)

Field name	Contents
KCCFCREM (bytes 1 - 8)	First 8 characters of the input
KCCFCFLD (bytes 9 - 140)	Format identifier
KCCFNOCF (bytes 141 - 144)	Service transaction code
KCCFS (bytes 145 - 7744)	Table (array) of control field information: each array element contains the information for one control field. There can be up to 50 elements. The elements are structured as follows:
	<ul style="list-style-type: none">• KCCFFNAM (8 bytes) Name of the format or subformat containing the control field
	<ul style="list-style-type: none">• KCCFREM (8 bytes) Remark defined as with IFG
	<ul style="list-style-type: none">• KCFLOFL (4 bytes) Length of the control field
<ul style="list-style-type: none">• KCCFFLD (132 bytes) Contents of the control field	

In the second parameter area, openUTM supplies the following values:

KCCFCREM

contains the remark defined for the control field when the format was generated with IFG and whose contents are included in KCCFCFLC. If no remark was created when the format was generated, or if no entry was made in the control field, the 8 bytes in this field are filled with blanks.

KCCFCFLD

contains the entry for a control field in the format, provided that at least one control field is defined in the format and that an entry has been made in it. KCCFCFLD contains this entry with the length permitted by the control field. The remainder of the KCCFCFLD field is padded with blanks.

If no entry has been made in a control field, or if the format does not have any control fields, then both KCCFCREM and KCCFCFLD will contain blanks and KCCFNOCF will have the value null.

If the format has several control fields which, in some cases, will be in different subformats, then both the remark and the contents of the control field will refer to a control field in which an entry has been made. If entries were made in more than one control field, KCCDCFLD will assume the entry made in the first control field in the uppermost subformat on the screen. KDDFCRREM will then contain the corresponding remark.

KCCFNOCF

contains the number of control fields in the format in which entries have been made.

KCCFS

contains an array which covers all the control fields passed by FHS, including the control field whose data is already entered in the fields KCCFCFLD and KCCFCREM. The number of valid array elements is stored in the field KCCFNOCF.

Each array element consists of a structure containing the following fields:

KCCFFNAM

contains (in 8 bytes) the (sub-) format name of the format to which the control field belongs. If the name is less than 8 characters long, the rest of the field is padded with blanks.

KCCFREM

contains the remark defined for this control field when the format was generated with IFG. If no remark was created when the format was generated, or if no entry was made in the control field, the 8 bytes in this field are filled with blanks.

KCCFLOFL

length of the control field.

KCCFFLD

contains the entry for a control field in the format. KCCFFLD contains this entry with the length permitted by the control field. The remainder of the KCCFCFLD field is padded with blanks.

Input in control fields (BS2000 systems)

Input can be made in a control field from a variety of sources:

- Terminal users can make entries in the control field.
- The field may have been defined with the property “automatic input” during format generation with IFG.
- In the case of formats or +formats: The field has the property “unprotected” and the FHS start parameter ISTD=RUNP (read unprotected) is set.

Errors with INPUT exit

If there are errors in the INPUT exit, an open service is not terminated; however, the terminal user is informed of the error with message K098 if

- the entry in KCICCD (effect of the input) is invalid or
- the entry in KCICCD does not match the values of the other output fields.

In both cases, a UTM dump with REASON=INPERR is supplied for error diagnosis. On BS2000 systems, a USERDUMP is also generated in such cases.

Database calls are not permitted in the INPUT exit.

If database calls are nevertheless included, a USERDUMP is generated on BS2000 systems with the error code KDCDB10.

Generation notes

The event exit INPUT must be defined during generation with the EXIT statement and the operand USAGE=(INPUT,...). You can also defined several INPUT exits for a variety of purposes. The following options are available:

- An application contains just one universal INPUT exit which is called with inputs in formatted mode and with inputs in line mode. This universal exit is generated with USAGE=(INPUT,ALL). Other INPUT exits are not allowed in this case.
 - A special INPUT can be generated for each type of format identifier. There are two possible types; no more than one of each type may be defined:
 - With USAGE=(INPUT,LINEMODE), an INPUT exit is defined for input in line mode.
- Only on BS2000 systems:*
- With USAGE=(INPUT,FORMMODE) an INPUT exit is defined for +formats and *formats. An INPUT exit generated in this way will also be called for the #formats.
 - With USAGE=(INPUT,USERFORM), an INPUT exit is defined for the user’s own formatting routines (-formats).

If special INPUT exits are used in an application, then it is not allowed to define a universal type with USAGE=(INPUT,ALL).

9.1.2 Event exit HTTP

The event exit HTTP is used to enhance existing program units for the calls of HTTP clients, without having to change the program units themselves.

Messages from and to HTTP clients are usually built in a different format than expected and processed by existing program units. The task of the HTTP exit is to convert the input messages from HTTP clients into the data structure expected of a program unit and to reformat output messages of a program unit in such a way that they are readable by an HTTP client.

In order to be able to keep the processing logic of an HTTP exit program simple, a separate HTTP exit program can be assigned to each TAC via the generation.

The HTTP event exit is called when the input message is read from and before the HTTP response is sent to an HTTP client.

The HTTP exit is invoked for an input message only once, at the time of the first MGET call, and must process the entire input message and build the message segments for the first and all subsequent MGET calls of the program unit. For this purpose, the exit can use the `kcHttpGet` functions to access all components of an HTTP request, for example, the message body of the HTTP request using the function `kcHttpGetReqMsgBody`. The function `kcHttpPutMgetMsg` can be used to provide the message reformatted for the program unit. The exit also has the option of using the structure `kcHttpExitMsgInfo` to split the input message into message segments. This means that the exit determines the number and length of the message segments that the program unit can read with MGET.

Before sending an HTTP response, the HTTP exit is called to process the output message. The exit then can use the function `kcHttpGetMputMsg` to read the message (parts) passed to UTM by the program unit with MPUT calls and use the function `kcHttpPutRspMsgBody` to specify the message body of the HTTP response. The splitting of the output message created by the program unit with MPUT calls is passed to the exit in the structure `kcHttpExitMsgInfo`, that is, it receives information about the number and length of the message parts.

The HTTP exit can also supply the HTTP status line with the function `kcHttpPutStatus` and HTTP header fields for the HTTP response with the function `kcHttpPutHeader`. The process flow is outlined in the following figure.

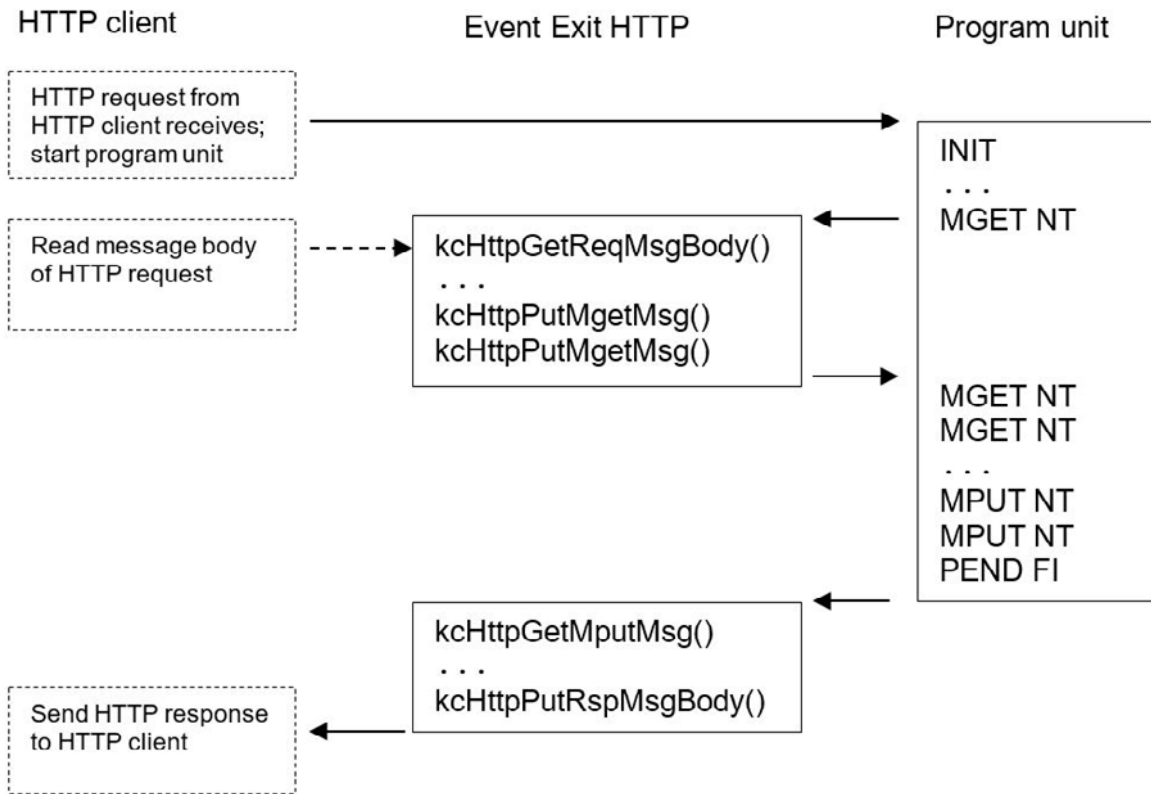


Figure: Message handling flow through an HTTP event exit

Programming notes

- The HTTP event exit must be implemented in the C programming language.
- The event exit HTTP must not use KDCS calls.

Generation notes

- Each event exit HTTP requires a PROGRAM statement.
- The statement HTTP-DESCRIPTOR defines a link from the URL of an HTTP request to an HTTP exit program as well as to a TAC of the application and thus a program unit.

KDCDEF statement HTTP-DESCRIPTOR

```

HTTP-DESCRIPTOR <http-descriptor-name>
    [, BCAMAPPL = <bcamappl> | *ALL]
    [, CONVERT-TEXT = *YES | *NO]
    [, HTTP-EXIT = <program-name> | *NONE | *SYSTEM]
    [, PATH = C'<path>' | C'/*']
    , TAC = <tac>
    [, USER-AUTH = *NONE | *BASIC]
  
```

Prototype of event exit HTTP

```
extern void <program-name>(kcHttpExitPar *);
```

Data structures for event exit HTTP

```
typedef enum
{
    KC_UTM_HTTP_VERSION      = 1          /* current version of UTM HTTP interface */
    , KC_UTM_HTTP_VERSION_1  = 1          /* UTM HTTP interface version of UTM V07.0A */
    , KC_UTM_HTTP_VERSION_MAX = INT_MAX
} kc_http_version;

typedef struct {
    int          nrMsgParts;          /* structure for message */
    short        lthMsgParts[254];   /* number of message parts */
    /* length of message parts */
} kcHttpExitMsgInfo;

typedef struct {
    /* parameter structure for HTTP exit */
    kc_http_version utmHttpVersion; /* version of UTM-HTTP interface */
    char            ioIndicator;    /* 'I' Input; 'O' Output */
    unsigned char   retcode;        /* ok: 0; nok: 1-255 */
    struct kcHttpInfo httpInfo;     /* http info from INIT PU */
    void *          pCa;            /* ptr to communication area */
    kcHttpExitMsgInfo * pStructureInfo; /* ptr to message structure info */
} kcHttpExitPar;
```

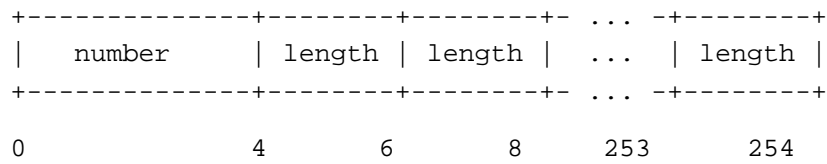
The fields of the data structure `kcHttpExitMsgInfo` have the following meaning:

<code>nrMsgParts</code>	Number of message segments
<code>lthMsgParts[254]</code>	Array with lengths of maximum 254 message segments

The fields of the data structure `kcHttpExitPar` have the following meaning:

<code>utmHttpVersion</code>	Version of the UTM-HTTP interface
<code>ioIndicator</code>	Indicator whether the event exit HTTP was called to handle the input message or the output message: 'I' Input 'O' Output
<code>retcode</code>	In this field, the event exit HTTP returns a return code. If the field has a value other than 0, the service is terminated with PEND ER, whereby the value of the field is converted into the secondary KDCS return code (the value 26 would result, for example, in the secondary KDCS return code HX1A).
<code>httpInfo</code>	In this structure, UTM passes the HTTP information that is returned to a program unit in the KDCS call INIT PU to the event exit HTTP.
<code>pCa</code>	Pointer to KB

pStructureInfo Pointer to the structure information of the message. When calling the event exit HTTP while reading the message with MGET, the exit must supply the data structure. When calling before sending the HTTP response, UTM provides the exit in the data structure with the number and length of message segments passed to UTM by the program unit with MPUT:



9.1.3 Event exit START

START exits are called when the application program is started, when the program is reloaded after a PEND ER or when the entire application program is replaced.

The event exits START are called in the order of the corresponding EXIT statements in the KDCDEF file.

You can use START exits, for example, in order to open files in order to work with them.

Programming notes

- You can access the KB header and SPAB in this event exit, but the KB program area and the SPAB do not contain any relevant data. openUTM enters the transaction code "STARTUP" for this exit program in the KCTACVG/kccv_tac and KCTACAL/kcpr_tac fields of the KB header.
- When the first process of the application is started, openUTM enters the service ID "F" in the KCKNZVG /kccv_status field, otherwise a blank.
- If you use other shared storage areas (AREAs), you can access them in the START exit. For more information refer to the following sections: "Other data areas (AREAs)" and item "Extending the LINKAGE SECTION" in section "COBOL program units as subroutines".
- The event exit START must not use KDCS calls.
- You can exit the event exit START with a return statement.
- The additional processes (if there are any) are only started after the first process of an application is started.
- If an error occurs in the event exit START (e.g. because of an attempt to open a nonexistent file), the event exit START CAN ensure that the current process is terminated. An error message must, however, always be written beforehand.
- Should irrecoverable errors occur during the START exit for the first process in the UTM application and thus prevent the UTM application from running, the START exit routine can only be terminated with *exit(-1)* (with COBOL85: set RETURN-CODE to -1 and afterwards STOP RUN). The event exit START which starts the UTM application is then aborted.

Unix, Linux and Windows systems

- If the START exit for a follow-up process in a UTM application is terminated with *exit(-1)* (COBOL85: RETURN-CODE to -1 and STOP RUN), the UTM application loses a process. For this reason, the START exit for a follow-up process must never be terminated with *exit(-1)*. Instead, this status must be handled by other program units - if necessary by shutting the process down from the administration interface.

BS2000 systems

- If the application program is to be terminated and a USERDUMP is to be written you can, for example, call a short Assembler program in which you first call the CDUMP macro and then call TERM with the operand UNIT=STEP.

Generation notes

- The program unit for the event exit START has to be defined at generation with the EXIT statement and the operand USAGE=START.
- A maximum of 8 event-driven START program units are allowed per application.

This version enables you to use several START exits and thus allows you to work better with preconfigured or purchased application components, which often have their own START and SHUT exits. These can now be processed one after the other. In addition, as an application operator, you can also add your own START exits.

9.1.4 Event exit SHUT

SHUT exits are called when the application program is terminated (e.g. as a result of PENDING). You can use SHUT exits, for example, to close your own files.

The event exits SHUT are called in the order of the corresponding EXIT statements in the KDCDEF file.

Programming notes

- You can access the KB header and SPAB in this event exit, but the KB program area and the SPAB do not contain any relevant data. openUTM enters the transaction code "SHUTDOWN" for this exit program in the KCTACVG/kccv_tac and KCTACAL/kcpr_tac fields of the KB header.
- If you use other shared storage areas (AREAs), you can access them in the SHUT exit. For more information refer to the following sections: ["Other data areas \(AREAs\)"](#) and item "Extending the LINKAGE SECTION" in section ["COBOL program units as subroutines"](#).
- If the application terminates normally, openUTM enters the service indicator "L" in the KCKNZVG/kccv_status field for the final process of the application, otherwise a blank.
- The event exit SHUT must not use KDCS calls.
- You can exit the event exit SHUT with a return statement.

BS2000 systems

- If an error occurs in the event exit SHUT (e.g. because of an attempt to open a non-existent file), the event exit SHUT can be terminated. Before doing so, however, you should first issue a message that you are going to terminate the program. If the application program is to be terminated and a USERDUMP is to be written you can, for example, call a short Assembler program in which you first call the CDUMP macro and then call TERM with the operand UNIT=STEP.

Generation notes

- The programs for the event exits SHUT must be defined at generation with the EXIT statement using the operand USAGE=SHUT.
- A maximum of 8 event exits SHUT are allowed per application.

This version enables you to use several SHUT exits and thus allows you to work better with preconfigured or purchased application components, which often have their own START and SHUT exits. These can now be processed one after the other. In addition, as an application operator, you can also add your own SHUT exits.

For an example of how an event exit SHUT can be used in C or COBOL, see ["Additional information for C/C++: Example of a complete UTM application on BS2000 systems"](#) and ["Additional information for COBOL: Example of a complete UTM application on BS2000 systems"](#).

9.1.5 Event exit VORGANG

openUTM calls the VORGANG event exit when a service is started or terminated, including incorrect termination and restart.

Even if a service consists of two or more transactions processed in different program units, the same event exit VORGANG which was called at the start of the service is called again at the end of the service.

If VORGANG is called at the end of a service, but an error occurs at this time, the last transaction of the service is not rolled back.

Programming notes

- The event exit VORGANG must not use KDCS calls.
- The longest processing time of the event exit VORGANG should be less than the maximum time in seconds for which a resource locked by another process is to be waited (KDCDEF statement MAX, RESWAIT operand, value time2) since UTM locked resources during the event exit VORGANG at the end of the service.
- You can exit the event exit VORGANG with a return statement.
- You can access the KB header and SPAB but the KB program area and the SPAB do not contain any relevant data.

openUTM enters the service indicator for this exit program in the KCKNZVG/kccv_status field of the KB header. The service indicator can assume one of the following values:

- F First program unit run of a dialog service
- C First program unit run of a concatenated service
- A Restart of a service
- R Errored end of service
- Z End of service
- E End of service
- D Termination of the service due to connection cleardown or loss of connection if RESTART=NO is generated for the UTM user id.

The program indicator (field KCPRIND) shows whether a exit program is running in a dialog service or in an asynchronous service:

- A The program unit is running in an asynchronous service.
- D The program unit is running in a dialog service.

Note that in distributed transaction processing, after the end of the service, the VORGANG event exit may be processed by a process other than the one which processed the last program unit in the service.

Generation notes

- There can be more than one event exit VORGANG for a single application.

-
- Which event exit VORGANG is called for which service is defined with the TAC statement, operand EXIT=TAC of the service. In particular, the event-driven services BADTACS, MSGTAC and SIGNON can have an event exit VORGANG.
 - Each event exit VORGANG requires a PROGRAM statement.

9.1.6 Event exit FORMAT (BS2000 systems)

If you use the event exit FORMAT, you are implicitly doing without the output support provided by the system components FHS and VTSU. You will therefore need to write your own formatting and may need to handle screen restarts manually. openUTM recognizes the event exit FORMAT by means of the “-” prefix to the format identifier in KCMF/kcfn.

The event exit FORMAT must be generated in the EXIT statement with the operand USAGE=FORMAT. Only one event exit FORMAT is permitted per application. Subformats must not be used.

i The event exit FORMAT is a program which implements system software functions. The code it contains must therefore be written very carefully: no exits should be left open or paths uncoded etc., as errors can cause the service, and possibly even the application, to crash. If in doubt, terminate the event exit FORMAT with formatting errors.

The event exit FORMAT can be written in any of the programming languages supported by openUTM. The programming languages Assembler and C/C++ are, however, particularly well suited to this purpose. The description of the FORMAT exit provided in the remainder of this section is based on the Assembler language. Nevertheless, here is a brief example of the prototype of a FORMAT exit in C:

Prototype of a FORMAT exit in C (ANSI)

```
void FORMATEX( struct kc_ca * const pKB
               , char      * const pSPAB
               , char      * const pFormatName
               , char      * const pDevice
               , char      * const pFormatArea
               , char      * const pPhysicallyInOutArea
               , char      * const pRestartArea
               , char      * const pFormatControlArea
               , char      * const pInOutIndicator
               , char      * const pSecondaryReturnCode
               );
```

Address list

When the event exit is called, openUTM provides the following address list:

Sequence of word addresses	Contents
1.	Address of the KB
2.	Address of the SPAB
3.	Address of the format name
4.	Address of the terminal type
5.	Address of the formatting user area
6.	Address of the physical input/output area
7.	Address of a restart area
8.	Address of the formatting control area
9.	Address of the input/output indicator

openUTM calls the formatting routine if you use a -format in the KDCS calls MPUT, FPUT, DPUT, MGET or FGET.

A dialog output message (MPUT) is not formatted until after the PEND or PGWT call. The contents of KB and SPAB are identical to those of the PEND or PGWT call. An asynchronous output message is not formatted until it is sent. The contents of KB and SPAB are undefined in this case, i.e. they no longer relate to the program unit which called FPUT or DPUT.

A dialog input message is formatted during MGET handling. KB and SPAB have the contents of the MGET call. This applies only for the event exit FORMAT: normally, openUTM formats messages before the INIT.

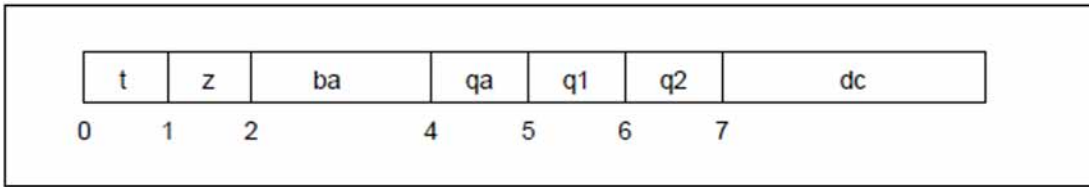
An asynchronous input message is formatted when the message is received, not when the FGET occurs. The contents of KB and SPAB are therefore undefined.

Please ensure that there are no fields that precede the transaction code, since openUTM identifies the TAC without calling the format exit.

Format name (address in word 3)

- In the case of input formatting: The format name used for this terminal during the previous output formatting operation (calls: MPUT, FPUT, DPUT or the command KDCFOR).
- In the case of output formatting: The specification made in KCMF/kcfn in the parameter area for the MPUT or FPUT call.

Terminal type and additional information (address in word 4)



t is the physical device type which can be queried by means of a TSTAT macro with TCHAR. The codes can be looked up in the DCSTA macro (see the BS2000 manual "Executive Macros").

If the specified terminal type is not supported by the event exit FORMAT, a formatting error **must** be forced.

z is an item of additional information:

X'00' = delete screen.

X'01' = do not delete screen.

ba is the screen output function:

X'0001': KCRESTRT

X'0001': KCREPL

X'0002': KCERAS

X'0004': KCALARM

X'0008': KCREPR

X'2000': KCEXTEND

X'4000': KCCARD

qa is an identifier which indicates whether confirmation must be requested - applies to output to printers only.

X'00' = request confirmation

X'01' = do not request confirmation

q1, If qa = X'01', then these two bytes will contain the confirmation numbers in EBCDIC code.

q2 If you are using a message header, both of these bytes must be converted to ASCII and entered in the return bytes RB1 and RB2 (see the manuals for your terminal).

dc device characteristics; contains 8 bytes of information on the device type and configuration, in the format that would be generated in PDN with XSTAT and XOPCH.

Refer to the DCSTA macro for information on the significance of the first 8 bytes (see the BS2000 manual "Executive Macros").

Formatting user area (address in word 5)

Input formatting:

Once the format exit has been called, openUTM expects the logical message here in the input format (see “[Message formats](#)”). The maximum length is determined by the generated value (see MAX statement, operand NB, in the openUTM manual “Generating Applications”). openUTM enters this maximum length in the length field of the formatting user area before the call is made.

If conversion of the logical message to a physical message causes it to exceed the length of this area, a formatting error **must** be forced.

Output formatting:

The area contains the message to be formatted in the form in which it was made available in the message area with MPUT or FPUT. The message is structured in input format. Subformats are not permitted.

Physical input/output area (address in word 6)

Input formatting:

openUTM passes the message as it is received from the terminal in the input format.

Output formatting:

Once the format exit has been called, openUTM expects to find the formatted message here in output format.

The maximum length is determined by the maximum message length allowed on the connection to the client. openUTM enters this maximum length in the length field of the physical input/output area before the call is made.

If conversion of the logical message to a physical message causes it to exceed the length of this area, a formatting error **must** be forced or an alternative message must be generated.

Restart area (address in word 7)

The restart area must be used to reconstruct screen formats where necessary, which can arise in three different situations, for example:

- with the KDCDISP command (display last screen)
- if the terminal user wants to continue an interrupted service with the most recently entered format (e.g. after a connection has been lost or after the command KDCOFF has been issued while a service was still running).
- if the screen is destroyed by an asynchronous output and is to be restored again.

You must ensure that the restart area always contains the current logical message so that this can be output if the need arises.

If you first want to delete the old screen when formatting output, you must refresh the restart area.

If you do not want the old screen to be deleted in this case, you need only modify (overwrite) those fields in the restart area that are also modified at the terminal.

After input has been made at the terminal, the restart area must be updated accordingly.

In the case of a PEND, the restart area is backed up to the length specified for the user area for this format when the output was last formatted (KCLM for MPUT).

In the event of a restart, output formatting takes place. The address of the formatting user area is the same as that of the restart area (i.e. there is only a restart area).

Formatting control area (address in word 8)

As of address + 1 in this area, you must store in the event exit FORMAT a (hexadecimal) return code which indicates whether formatting was successful.

The return code must be one of the following:

X'00' Output formatting was successful.

X'xy' User error messages were passed in the form of UTM return code "FRxy" in the field KCR CDC (formatting errors). The entries X'01', X'02', X'03', X'04', X'08', X'10' and X'99' are not permitted: these return codes are reserved for cooperation between openUTM and FHS.

Input/output indicator (address in word 9)

The first byte of the indicator contains the value:

X'00': for input formatting

X'01': for output formatting

X'02': for a restart

X'03': for KDCFOR

In the case of a restart, the addresses of the formatting and restart areas are identical.

Message formats

Two different message formats are used in the event exit FORMAT (see previous section). These formats do not necessarily adhere to the half-word boundary.

input format	-----
	length b b (partial) message

	0 2 4
output format	-----
	length b b b (partial) message

	0 2 5

length is the length of the entire message (binary), including the prefix, which accounts for 4 bytes in input formatting and 5 bytes in output formatting.

b is a blank (X'40')

For more information on the structure of physical messages, refer to the manuals for your terminal.

Example

```
FEXIT      CSECT
           STM    14,12,12(13)
           BALR   12,0
           USING *,12
           USING KB,2
           USING SPAB,3
           USING DFORMNAM,4
           USING DFORMSDE,5
           USING DADUSERA,6
           USING DAREAFMI,7
           USING DADRSRTA,8
           USING DMDCBUSE,9
           USING DFORMMOD,10
           LM     2,10,0(1)

*
* INPUT OR OUTPUT FORMATTING, RESTART OR KDCFOR ?
*
           CLI    FORM#IND,X'00'           00=INPUT,   01=OUTPUT
           BE     EINFORM                   02=RESTART, 03=KDCFOR
           CLI    FORM#IND,X'01'
           BE     AUSFORM
           CLI    FORM#IND,X'02'
           BE     RESTFORM
           CLI    FORM#IND,X'03'
           BE     FORFORM

*
* SET FORMATTING ERROR: INVALID OPCODE !
*
***** K D C F O R
*
FORFORM DS    0H
*
* A) SET UP PHYSICAL MESSAGE AS PER FORMAT NAME
*   AND PREASSIGN WITH "STD." VALUES
* B) ANALYZE CONFIRMATION REQUEST ('FORMQA')
*   AND SUPPLY MESSAGE HEADER
* C) SET UP RESTART AREA
* D) SET RETURN CODE IN FORMATTING CONTROL AREA
*
END#EXIT LM    14,12,12(13)
           BR    14

*
***** INPUT FORMATTING
*
EINFORM CNOP   0,4
*
* A) ANALYZE PHYSICAL NAME AS PER FORMAT NAME AND
*   SET UP FORMATTING USER AREA ('DADUSERA') AS PER
*   MESSAGE FORMAT FOR INPUT
* B) SUPPLY RESTART AREA
* C) SET RETURN CODE IN FORMATTING CONTROL AREA
*
```

```
*  
DMDCBUSE DSECT  
          DS    0H  
*  
DFORMMOD DSECT  
FORM#IND DS    X  
          END
```

9.2 User-specific error handling (Unix and Linux systems)

On Unix and Linux systems, you can program a user-specific error handling, for example to allow a service to be continued even if there are serious errors or to enable additional diagnostic documents to be created.

The following functions are available:

- **KCX_REG_USER_SIGNAL_HANDLER**

Registration of the user signal routine that is called when a signal occurs. The signal routine must also be created. If you register multiple signal routines, the last registered routine is always called.

Registration of the user signal routine in a utmwork process is effective until the process is terminated, provided it is not explicitly deregistered prior to this.

- **KCX_UN_REG_USER_SIGNAL_HANDLER**

Deregistration of the user signal routine if the user signal routine had previously been registered. This routine should be called immediately before the PEND.

- **KCX_SET_RELOAD_FLAG**

Exchanging the utmwork process after PEND RE.

Calling this function initiates exchange of the utmwork process when the current program unit run is terminated with PEND RE.

We recommend always calling this function for Cobol runtime errors in the UTM application to eliminate the delayed effects of this error, i.e. to ensure the application is capable of running continuously.

i For all other PEND calls (except for PEND ER), the utmwork process is not replaced.

- **KCX_WRITE_DUMP**

Creates a UTM dump.

This function enables an application program to write a UTM dump for a reason defined by the user without the service being aborted. UTM outputs the ROOT area and the stack information (as for the PEND ER dump) and creates a memory dump (core dump).

Information on how to program these functions can be found on "[Programming user-specific error handling \(Unix and Linux systems\)](#)" (C/C++) and "[Programming user-specific error handling \(Unix and Linux systems\)](#)" (COBOL).

User signal routine

The user signal routine is executed by openUTM instead of the default error handling when a signal occurs in the application program. The user signal routine is called under the following conditions:

- When the signals SIGILL, SIGFPE, SIGSEGV, SIGBUS, SIGPWR and SIGABRT occur in the application program.
- With SIGALRM after expiry of the program runtime timer in the application program.

The use of a user signal routine enables:

- Program errors to be handled within the UTM service.
- Specific error messages to be output to the UPIC client.
- The UTM service to be continued despite errors in the application program.

The user signal routine replaces the default error handling in openUTM, i.e. abnormal service termination with PENDER / XT *nn* (*nn* = signal number), output of K017 to terminal clients, for UPIC clients in UPIC log file (+ error code "CM_DEALLOCATED_ABEND"), PENDER dump, and exchange of the utmwork process.

The user signal routine should only initiate "clear-up actions" and then terminate the program with PENDER. Typical "clear-up actions" in a dialog program include the following KDCS calls:

- RSET to reset the transaction data,
- MPUT NE with appropriate error message to the client,
- PENDER to specify the follow-up program that will run after this error situation.

The last registered signal routine is always called.

In addition, UTM replaces the affected utmwork process after the next PENDER KDCS call.

An example can be found on "[Programming user-specific error handling \(Unix and Linux systems\)](#)" (C program) or "[Programming user-specific error handling \(Unix and Linux systems\)](#)" (COBOL program).

i Please note that no timer functions such as the C library function alarm() may be used in the application program, at least not if a timer has been generated for the current TAC (KDCDEF generation TAC RTIME= <rtime>).

9.3 STXIT routines (BS2000 systems)

On BS2000 systems it is possible to define STXIT routines for certain events (e.g. address errors, program end). These routines are activated by the operating system (not by openUTM) if one of the specified events occurs (see the BS2000 manual "Executive Macros").

openUTM provides STXIT routines of its own which are opened before the START exit is called. Exception: TIMER /RTIMER, which are opened immediately after the START exit and are used by openUTM to check the program unit runtime (see the TIME parameter for the TAC statement).

You can define your own parallel STXIT routines which are then activated in addition to the ones defined by openUTM. If you specify the start parameter STXIT=OFF, only those STXIT routines that you have defined are activated (UTM STXIT routines are not activated). The latter is only possible if the application was started in the dialog.

The STXIT routines that you have created are always activated before the UTM STXIT routines (with the exception of RUNOUT).

i If programs are loaded dynamically with associated runtime systems after the start phase, and if these programs initiate their own STXIT routines, the sequence in which the STXIT routines are activated may differ from the one described here.

The STXIT routines that you have created must be terminated with EXIT CONTINU=YES. Otherwise, openUTM cannot guarantee that errors will be handled correctly (e.g. PEND ER in certain situations). The openUTM STXIT routines are terminated with EXIT CONTINU=NO.

i For STXIT processing in ILCS programs, please refer to the description in section "[Event handling in ILCS programs \(BS2000 systems\)](#)".

i Please note that no timer functions such as the C library function alarm() or the macro SETIC (Set interval timer) may be used in the application program, at least not if the respective timer has been generated for the current TAC (KDCDEF generation TAC TIME={time1 | (time1,time2)}).

9.4 Event handling in ILCS programs (BS2000 systems)

In an ILCS application, all interruptions are first rerouted to the ILCS event routines. Whether and how an event is handled depends on:

- the event itself
- the programming language in which the most recent active program is written
- the event handling routines in the programs involved
- the call sequence, if this contains different ILCS programming languages

Event handling variants:

1. The program unit (i.e. a program within the call sequence) or a runtime system incorporated in its call sequence handles the event and continues processing.
2. Within the framework of the program unit as described above, the event is not handled but is passed on to openUTM together with its context and event code.

Two distinctions must be drawn in this case:

- a. It is an event of the class PROCHK or ERROR:

openUTM prepares the message K102 together with the context and IW passed to it. In this case, the IW is additional control element for the following PEND handling.

- b. It is any OTHER EVENT:

If the event 'Other Event' occurs, openUTM can only offer a stereotypical response and has to prevent the task from being terminated abnormally. The event code that is passed is not an IW in the sense used in STXIT - its value is of no significance to openUTM. In particular, it is important to prevent this event code, in its role as a control element in UTM PEND handling, from leading to incorrect interpretations. To enable UTM error handling to run correctly, the event code is therefore set to the value X'FF'. During continued processing, openUTM interprets this value as a (simulated) IW. In other words, if an OTHER EVENT is passed to openUTM, then openUTM behaves as though an STXIT event had occurred with IW=X'FF'.

In such cases, diagnosis has to be based on the message that was output when the OTHER EVENT occurred by the corresponding language, the program unit or ILCS. If no such message is output, the STXIT event X'FF' is displayed together with the UTM message K102...KDCIWFF.

The resulting user-dump contains the code KDCIWFF.

3. Within the framework of the program unit as described above, the event is interpreted, a message is output (if necessary) and the ILCS entry IT0TERM is called. This entry activates openUTM and simulates the event handling of a TERM UNIT=PROG. In this case, the event data for the primary interruption could only be derived from the UTM message issued by the program unit or from the corresponding language. openUTM issues the message K102... KDCIW90 (TERM), together with all register states up to the time of the IT0TERM call. The resulting user-dump contains the code KDCIW90.

4. An ILCS-internal error occurs:

ILCS branches to a defined UTM entry; openUTM sets an internal event code, IW=X'00', which can have one of two meanings:

- an ILCS-internal error occurred
- the ILCS stacking chain has been interrupted.

openUTM outputs this IW=X'00' in the message K102. In its function as a control element, this IW=X'00' is interpreted by openUTM during further execution of the program as an IW=X'88', i.e. the task is terminated with TERM UNIT=STEP.

STXIT events - how ILCS behaves if an error occurs

After STXIT events which ILCS or the EHL routines that were called are unable to process, ILCS closes its own STXIT and terminates the routine with EXIT CONTINUE=NO. In most cases, the same error will occur again immediately, whereupon other STXIT routines (e.g. those controlled by UTM) can handle the error. In isolated cases, such as an exponential overflow, the program environment (register states etc.) at the start of the ILCS STXIT routine will already have been modified in such a way that it is now no longer possible to reconstruct the error environment. Before the STXIT is terminated, ILCS uses the IW to check whether it is possible for the error to recur. If not, ILCS calls its program termination routine IT0TERM.

User-specific STXIT routines in an ILCS environment:

To ensure that STXIT routines are executed in the correct sequence in an ILCS program environment, you should register user-specific STXITs directly with ILCS by means of special assembler macros or C functions. For details, see the relevant user manual for CRTE, ASSEMH and C.

9.5 Event services

Event services are dialog or asynchronous services which are started as a result of a certain event, i.e. they are event-driven services. The program units in these services must contain KDCS calls and adhere to the rules described in chapter “[Structure and use of UTM programs](#)”.

Event services are generated with a privileged transaction code which openUTM uses internally. The following event-driven services are possible:

BADTACS with the TAC **KDCBADTC**

MSGTAC with the TAC **KDCMSGTC**

SIGNON with the TAC **KDCSGNTC** or specified as **SIGNON-TAC** in the BCAMAPPL statement

The transaction codes for these event-driven services are defined with the KDCDEF statement TAC.

Database calls are permitted, but (in the case of SIGNON event service) only if this was permitted explicitly during generation (SIGNON ...,RESTRICTED=NO).

9.5.1 Dialog service BADTACS

If it has been generated, the dialog service BADTACS is started whenever a terminal or a transport system application has entered an invalid transaction code. This can have any of the following reasons:

- The transaction code has not been generated.
- The transaction code is not assigned to any program unit.
- The user does not have the authorization to call the transaction code. There can be various reasons for this, e.g.:
 - The transaction code is an administrator TAC but the user did not sign on with administrator privileges.
 - A lock code is assigned to the transaction code but the user or LTERM partner does not have the corresponding keycode.

Programming notes

- The dialog service BADTACS must issue an MPUT call in accordance with the rules described in the chapter "Structure and use of UTM programs". This MPUT call then replaces error message K009, which openUTM would generate in the absence of a BADTACS service.
- At the start of a service, after the INIT call, the invalid TAC is located in the KB header, in both the KCTACAL/kcpr_tac and KCTACVG/kccv_tac fields.
- If the BADTACS service is called in line mode, it will receive the full message including the first 8 bytes. If it is called in format mode, the first 8 bytes (for *formats) or 10 bytes (for +formats) are removed from the message.
- Outside of a service, BADTACS can also be started with a function key if one has been generated with a return code (20Z-39Z) but no TAC (SFUNC statement, operand RET=), or if the function key has not been generated (return code 19Z). The return code is then passed with the first MGET; a message (including the first 8 bytes) can be read with the second MGET. No entry is made in the KCTACAL/kcpr_tac and KCTACVG/kccv_tac fields.

Generation notes

- There must be no more than one BADTACS service per application.
- The first program unit in the dialog service BADTACS must be defined during generation with the TAC statement
TAC KDCBADTC, PROGRAM=...

Examples of BADTACS event services in C and COBOL are given on ["Example of a complete UTM application on BS2000 systems"](#) and ["Example of a complete UTM application on BS2000 systems"](#) respectively.

9.5.2 Asynchronous service MSGTAC

The asynchronous program unit MSGTAC is called:

- if openUTM outputs a *Knnn* or *Pnnn* message
- if MSGTAC is entered as the destination for this message.

How you enter MSGTAC as the message destination and how the messages that are passed are structured is described in the openUTM manual "Messages, Debugging and Diagnostics".

The MSGTAC service is given administration authorization and all keys of the application by openUTM , i.e. with the maximum authorization allowed.

If the MSGTAC program unit aborts with *KCRCCC >= 70Z*, openUTM locks it for the remainder of the application run (*STATUS=OFF*). It then needs to be released explicitly by the administrator (*STATUS=ON*). This rule does not apply if a program is aborted by a programmed *PEND ER/FR*.

openUTM writes messages for the message destination MSGTAC to the page pool. As long as warning level 2 for this page pool is not exceeded, you can be sure that none of these UTM messages will be lost.

Exception: The messages indicating that the warning level has been exceeded or not reached cannot always be sent to the MSGTAC program unit.

Programming notes

- The asynchronous program MSGTAC reads the message to the message area for the program unit with an FGET call. In this context, FGET calls should be repeated as often as necessary until the return code 10Z is set, to ensure that all pending UTM messages are read in a single program unit run.
- For each UTM message, there is a data structure available which can be used in the program unit to interpret the message contents. For C/C++, these structures are contained in the header file *kcmsg.h*, for COBOL they are contained in the COPY member KCMMSGC.
- The MSGTAC program unit runs as an asynchronous service under the internal UTM user ID KDCMSGUS with *KSET=MASTER* and *PERMIT=ADMIN*.
- The MSGTAC service can only consist of one program unit run.
- In a program unit run, at least one message must be read with FGET as otherwise the program unit will be terminated abnormally.
- The service is started internally with the administrator TAC KDCMSGTC.

openUTM supplies the KB header as follows:

Fields in the KB header		Entries for MSGTAC
COBOL	C/C++	
KCBENID	kcuserid	KDCMSGUS
KCTACVG	kccv_tac	KDCMSGTC
KCTACAL	kcpr_tac	KDCMSGTC
KCLOGTER	kclogter	KDCMSGLT
KCTERMN	kctermn	MT

-
- The MSGTAC program unit can use the administration program interface and it can issue administration commands. In particular, the MSGTAC program unit can issue the KDCS calls DADM and PADM to administer DPUT messages and printers; see the openUTM manual "Administering Applications".

Generation notes

- There can be only one MSGTAC program unit per application.
- The MSGTAC program unit must be defined in the TAC statement with

```
TAC KDCMSGTC,PROGRAM= . . . .
```

Example of a MSGTAC program unit

The MSGTAC program unit NOHACK is designed to prevent unauthorized users from gaining access to a UTM application. If more than three invalid attempts are made to sign on via an LTERM partner (with an invalid user ID, an incorrect password or the wrong ID card), the connection to the terminal is to be aborted. This will require additional preparatory measures (see also the openUTM manual "Messages, Debugging and Diagnostics").

- Preparations:
 1. Call the UTM tool KDCMMOD.
 2. Issue the GEN command, specifying the name of the message module.
 3. Use MODMSG commands to define MSGTAC as an additional destination for the messages K008, K033 and K094.
 4. Compile the source program written so far and link it to the application.
 5. Define the KDCDEF statement MESSAGE in the message module.
 6. Define KDCPTRMA in the TAC statement.

A more elegant solution would be to write the specifications for points 2 and 3 to a file and then to use this as an input file for point 1.

- Implementing the MSGTAC program unit:

The MSGTAC program unit NOHACK counts the number of incorrect attempts in a TLS. If openUTM accepts a sign-on attempt to the application (message K008 or K033), this TLS is deleted again.

If three consecutive incorrect attempts are followed by a fourth incorrect attempt, the corresponding terminal is to be released by means of "asynchronous administration". This happens with an FPUT call with KCRN = "KDCPTRMA" and a message area with the contents PTERM=pterm, ACT=DIS (see also the openUTM manual "Administering Applications").

The administration command is then written with LPUT to the user log file and the TLS is deleted. Examples in C are given in section "[Example: MSGTAC event service](#)" and in and COBOL in section "[Example of an asynchronous MSGTAC program unit](#)" respectively.

Each K message is read with FGET by the MSGTAC program unit. After one K message has been "processed", FGET immediately reads the next K message within the same program unit run. A list of all the K messages is provided in the openUTM manual "Messages, Debugging and Diagnostics".

9.5.3 The SIGNON service

The SIGNON sign-on service is a dialog service that is started

- after the connection to a terminal or a transport system client has been established by means of a transport system application, provided a sign-on service has been generated for this access point, or
- before the start of every conversation initiated by a UPIC client, provided a sign-on service has been generated for this access point and
 - sign-on services were released for UPIC clients at generation,
 - the application is generated with OMIT-UPIC-SIGNOFF=NO,
 - and the user is not yet signed on.

A separate sign-on service can be generated for each transport system access point of a UTM application, see the SIGNON-TAC operand of the BCAMAPPL statement and the TAC statement with the KDCSGNTC transaction code in the openUTM manual “Generating Applications”.

Generation notes

- The sign-on service for a transport system access point defined with MAX APPLINAME is generated with TAC KDCSGNTC , PROGRAM= . . . This sign-on service thus becomes the default for all the transport system access points of the application.
- The SIGNON-TAC parameter of the BCAMAPPL statement can be used to generate another sign-on service for a transport system access point. If a sign-on service is not to be used for a transport system access point, the value *NONE must be specified for the SIGNON-TAC parameter.
- Sign-on services are enabled for UPIC clients as follows:
SIGNON . . . , UPIC=YES .
- In the SIGNON statement in the generation you can specify that a user can still temporarily sign on to the UTM application if the validity period of his or her password has run out (operand GRACE = YES). In this case, the password of the user must be changed if the sign-on service is to end successfully.
- The maximum number of failed sign-on attempts from a client can be monitored as follows:
SIGNON , SILENT-ALARM= *number*
When this value is reached, message K094 is output to SYSLOG. This message can also be processed by an MSGTAC program (see "[Asynchronous service MSGTAC](#)").

You will find a detailed description in the openUTM manual “Generating Applications”.

9.5.3.1 Programming notes

The SIGNON service controls the sign-on procedure by means of a program. The sign-on service is controlled, above all, by the following KDCS calls (see "PENDING Terminate program unit" and "SIGN Control sign-on and sign-off, check authorization data, change passwords"):

SIGN ST	Queries the status of the sign-on service. The call also returns the result of the previous SIGN ON.
SIGN ON	Transfers authorization data to openUTM for checking. The call returns only whether the call was syntactically correct, not whether the sign-on was successful.
PENDING PS	Terminate program unit so that openUTM can verify the authorization data and insert the intermediate dialog if necessary. The sign-on service then continues in the follow-up program unit. Not until this call does a provisional sign-on take place provided the data transferred with SIGN ON were correct.

openUTM on BS2000 systems is shipped with an appropriate sample program. The openUTM manual "Using UTM Applications on BS2000 systems" contains a description of this sample program and additional information on the concept behind the sign-on service and typical applications.

Notes

- In the first part of the sign-on procedure the KCBENID/kcuserid field in the KB header only contains blanks.
- If the sign-on is not completed successfully before PENDING FI is executed, then openUTM clears the connection to the terminal or the TS application, or it ends the UPIC conversation. In this manner, you can handle several unsuccessful attempts to sign on, e.g. because the user is not authorized, in a simple manner using PENDING FI after KCRSIGN1 = U.
- If the sign-on service violates the rules applicable to it, then openUTM aborts the service with PENDING ER. The connection to the terminal or to the TS application is cleared, and the connection to the UPIC client remains.
- If the UTM application is generated without user IDs (i.e. without USERS), the sign-on service can terminate immediately because the sign-on has been successful. The sign-on service receives the corresponding information at the SIGN ST call. However, an application-specific authorization check can also be carried out in the sign-on service (using a database with authorization data, for example).
- Restrictions in the sign-on service
 - The KDCS calls PENDING RE/RS/SP are prohibited.
 - FPUT/DPUT calls and accesses to a ULS are not allowed before the sign-on is successful. Database calls and accesses to GSSBs and TLSs are only allowed before the sign-on is successful if the SIGNON statement explicitly allow this. You should therefore query the sign-on status (returned in KCRSIGN1) with SIGN ST to see if it contains the value A or R before you execute the accesses stated above.
 - You are not allowed to initiate calls for distributed processing.

9.5.3.2 Sign-on service for terminals

The sign-on service for terminals consists of two parts:

- 1st part: Read authorization from terminal and transfer to openUTM.
- 2nd part: Send confirmation (message and USER-specific start format for the terminal, for example) in the event of a correct sign-on.

Between the first and the second part, openUTM may conduct an intermediate dialog with the terminal in order to query further authorization data such as identification information or the password.

openUTM returns the status of the sign-on procedure in the KCRSIGN1 field for SIGN ST. The program unit decides on how to proceed after this point based on this status indicator. The following values are possible:

- KCRSIGN1 = C (connected)
The terminal is connected to the application, but there is no user signed on yet. The user on the terminal is requested to enter his or her authorization data via an MPUT call. The program unit terminates itself with PEND KP. The follow-up program unit reads the authorization data with MGET, passes the data with SIGN ON to openUTM and terminates itself with PEND PS.
- KCRSIGN1 = I (incomplete)
openUTM already knows the user ID, but still requires additional information (password, ID card). This information is queried in an intermediate dialog. The program unit must terminate itself with PEND PS (specify the follow-up TAC!), and then openUTM executes the intermediate dialog.
- KCRSIGN1 = A (accepted)
The sign-on is correct. The user ID is entered in the KB header. If so desired, additional dialog steps can be inserted before the end of the service. The sign-on service is terminated with PEND FI or PEND FC. The final message is created by the service itself and is output using MPUT. If the message is directed to a terminal, then it can be created from the user-specific start format. The name of the start format is returned by openUTM when SIGN ST is called in the KCRMF/kcrfn field.
When MPUT PM is called, and then PEND FI, the last dialog message of the last service is output, if such a message is available.
- KCRSIGN1 = R (restart)
The sign-on is correct and a service restart is pending. The user ID is entered in the KB header.
If desired, additional dialog steps can be inserted before the end of the service. The sign-on service must terminate itself with PEND FI. The service restart is initiated by calling MPUT PM, KCLM=0, KCMF/kcfn=blanks. In this case, openUTM outputs the last saved message of the interrupted service (screen restart on the terminal), or it starts the follow-up program unit or follow-up service when there is a local synchronization point after PEND SP/FC. The service that is open can be terminated abnormally by terminating it without using an MPUT call. A K017 message is sent to a TS or terminal partner.
- KCRSIGN1 = U (unsuccessful)
openUTM did not accept the authorization data. A terminal sign-on service is still in the 1st part and must request the user to re-enter the authorization data. If the sign-on service terminates in this state, the connection to the terminal is cleared.

LTERM partner with automatic KDCSIGN

At the SIGN ST call, the sign-on service receives the information that the user ID is already known. Depending on the generation, an intermediate dialog can be conducted to request a magnetic strip card or a password.

Sign-on via multiplex connection (BS2000 systems)

Depending on the configuration of the multiplex connection in OMNIS, OMNIS forwards the authorization data to openUTM by means of the PUTMMUX protocol for checking. If the data is correct, openUTM starts the sign-on service, which receives corresponding information with the SIGN ST call. If the data is not correct, the sign-on service is not started and the router must inform the terminal at the terminal.

The following diagram shows the sequence of execution of a sign-on service at the terminal:

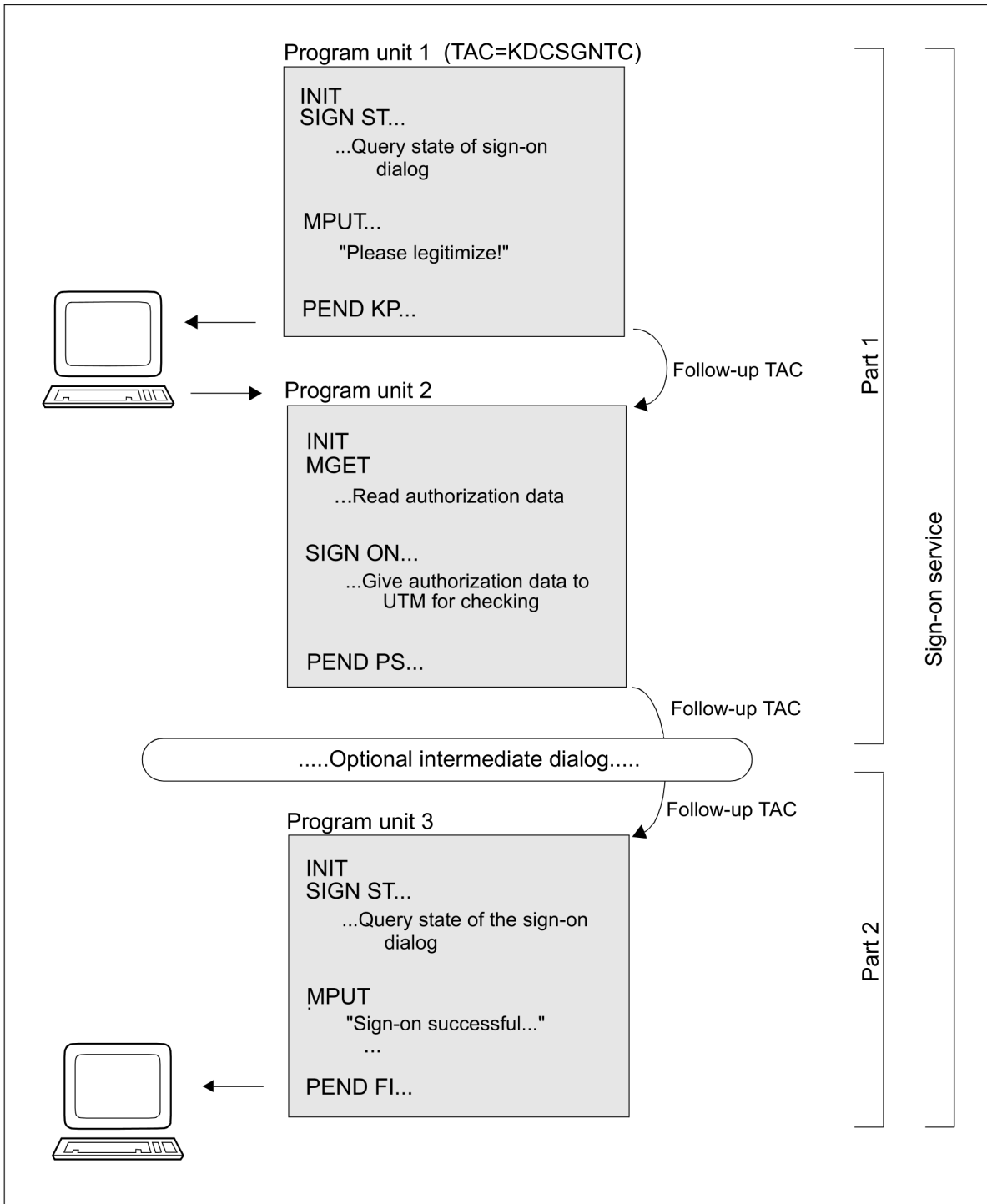


Figure: Processing of a sign-on service for terminals

9.5.3.3 Sign-on service for UPIC clients or transport system applications

If the sign-on service is running for a UPIC client or a transport system application, then the sign-on service will **never** be located in the **first part** because, at a minimum, the connection user ID is assigned as the user ID. The following applies:

- In the case of TS applications, the user is signed on under the connection user ID or a user ID passed by means of a SIGN ON call. If the user is signed on under the connection user ID, the sign-on service can still sign the user on under a real user ID by means of the SIGN ON call when there is no service open for the connection user ID (KCRSIGN1=R).
- In the case of UPIC clients, the user is signed on under the connection user ID, the user ID passed in the UPIC protocol or the user ID passed by means of a SIGN ON call. If the user is signed on under the connection user ID, the sign-on service can still pass a real user ID in the SIGN ON call.

The second part of the sign-on service

You can use the SIGN ST call to query the status.

1. KCRSIGN1= A or R

The sign-on was successful. The service is now assigned a user ID.

When a sign-on service starts for a transport system application, the connection user ID is signed on.

When a sign-on service starts for a UPIC client, either the connection user ID or a real user ID passed by the client in the UPIC protocol is signed on.

If the client is signed on under the connection user ID, the sign-on service can now pass a real user ID by means of the SIGN ON call.

For KCRSIGN1 = A

The sign-on service can terminate with PEND FI or PEND FC. The final message is created by the service itself and is output with MPUT.

If the sign-on service terminates with MPUT PM, KCLM=0, KCMF=SPACE and PEND FI, then openUTM outputs the last dialog message and terminates the conversation. If no message is available, then a "NULL message" is output and the conversation is terminated abnormally.

For KCRSIGN1 = R

The sign-on is correct, and there is no service restart. If desired, other dialog steps can be inserted before the end of the service. The sign-on service must terminate with PEND FI. The service restart is initiated by the call MPUT PM, KCLM=0, KCMF/kcfn=blanks. In this case, openUTM outputs the last saved message of the interrupted service (screen restart) or, in the case of a local synchronization point, starts the follow-up program unit or the follow-up service after PEND SP/FC.

If terminated without an MPUT call, the open service can be terminated abnormally. A UPIC client receives a CM_DEALLOCATED_ABEND, and message K017 is sent to a transport system application.

2. KCRSIGN1= U

The sign-on attempt was not successful, i.e. openUTM has not accepted the authorization data. If a sign-on service for a UPIC client terminates in this state, then the conversation is terminated. If a sign-on service for a transport system application terminates itself in this state, then the connection is cleared.

Particularities of the sign-on service for UPIC clients

The sign-on service is started before the beginning of every conversation but in the case of applications with OMIT-UPIC-SIGNOFF=NO only if the user is not yet signed on.

A PEND FI in the sign-on service after a successful sign-on terminates the sign-on service but not the conversation.

If a program unit of the sign-on service terminates after receiving a message from the UPIC client with PENDING PA /PR, PS or FC without a preceding MPUT, the follow-up program unit specified in the KCRN field can read messages or message segments that have not yet been read. If the sign-on service is terminated with PENDING FC without a preceding MPUT, the first program unit of the concatenated service receives the value F (first) rather than C (chained) as the service identifier in KBKOPF because it receives a message from the client.

The following diagram shows an example of the processing of a successful sign-on service via a UPIC client that passes the authorization data of a real user idea in the protocol field.

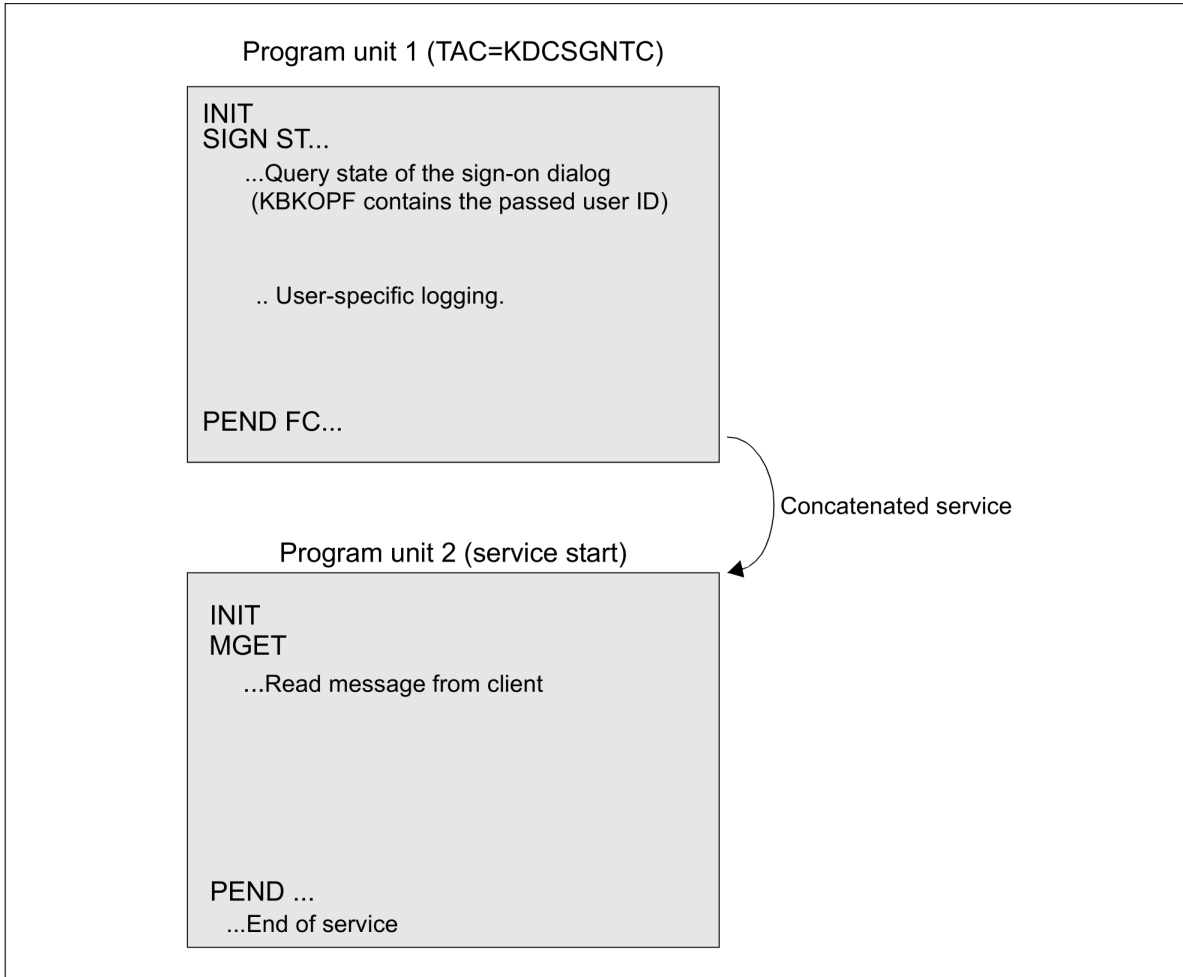


Figure: Processing of a sign-on service for UPIC clients

The sign-on service is terminated with PENDING FC in program unit 1. The transaction code passed with SIGN ST is taken from the UPIC protocol as a follow-up TAC.

The concatenated service can then read the message from the client in program unit 2. In this way, UPIC clients can use the sign-on service without any need for reprogramming.

Example of a sign-on service for TS applications

The following diagram shows the processing of a sign-on service via a TS application when the sign-on is successful under a real user ID:

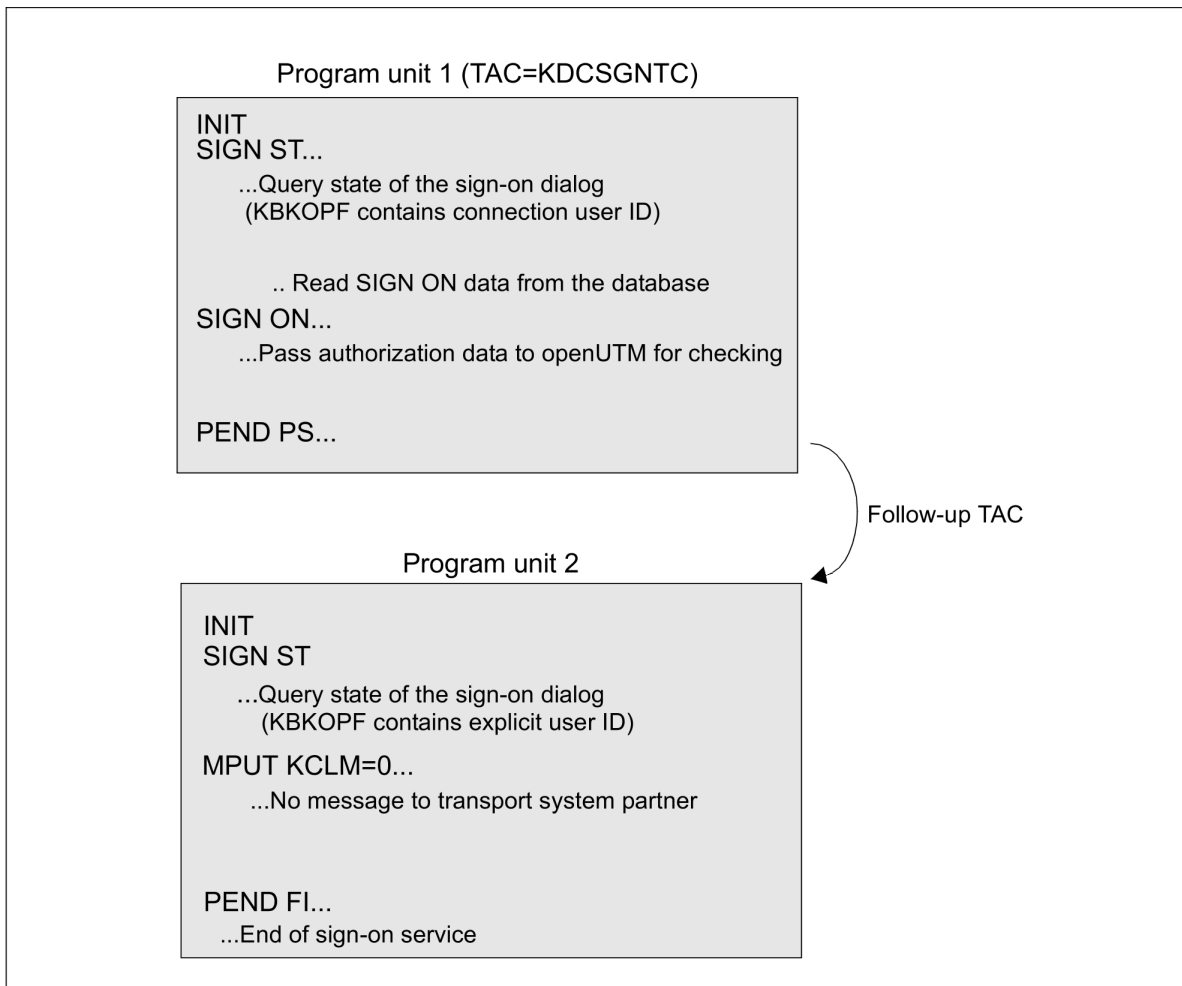


Figure: Processing of a sign-on service for TS applications

Sample programs for sign-on service

openUTM is shipped with program units as source programs that implement a complete sign-on service with a formatted interface to the terminal. This sign-on service is suitable for all generation variants. The format used contains English text.

The user can adapt this template to suit his or her requirements. A sign-on procedure with a formatted interface to the user is thus easily obtained. It is thus not necessary to start programming from scratch.

10 Additional information for C/C++

This chapter contains programming language-specific information as a supplement to the general information in chapters "[Structure and use of UTM programs](#)" to "[Event functions](#)". You will need the information provided here when writing C or C++ program units:

In the first section you will learn about the structure of C/C++ program units. The second section contains sample programs. The third section contains a list of the data structures in *kcca.h*, *kcmac.h* and *kcpa.h*.

10.1 Program structure for C/C++ program units

In this section you will learn:

- how to create a UTM program unit as a subroutine
- how you must declare the data
- what the command should look like and how a KDCS call is programmed
- what kind of special platform-specific characteristics exist (for example, format system or compiler-specific dependencies).

10.1.1 C/C++ program units as subroutines

UTM program units and event exits are subroutines of the UTM main routine. This has the following consequences:

- The program name defines the start address.
- A C/C++ program unit is defined as a function of type *void*.
- All formal parameters must be declared explicitly.
- The program unit is terminated dynamically with a PEND call; the event exits are an exception to this rule. They can be exited using the *return* statement. The *exit* statement must never be used.

A set of header files is provided for compatibility and to ensure that you are working with correct data structures. You use the same header files for C and C++ program units. The use of these header files is described in chapter "[Data structures for C/C++ program units](#)".

The include files *kcca.h*, *kcmac.h* and *kcpa.h* are located:

- on BS2000 systems in the library *SYSLIB.UTM.070.C*
- on Unix, Linux and Windows systems, in the *include* subdirectory of the UTM *utmpath* directory

i If you cannot compile C programs because the first KDCS call parameter has the type *struct kc_pa ** instead of the type *union kc_paa ** then you should set the UTM_OLDANSI option for the C precompiler in order to prevent checking.

Program unit names

The name of a C program unit is also its start address.

This name is freely definable. It must be unique within an application program. Some names have already been reserved and for that reason may not be used.

You should observe the following points when choosing a name:

- For BS2000 systems:
 - All names beginning with KDC, KC and I are reserved and should be avoided.
- For Unix, Linux and Windows systems:
 - All names beginning with KDC, KC, x or ITS are reserved.
 - Names beginning with t_ are reserved for PCMX.
 - Names beginning with a_, o_ and s_ are reserved for OSS.
- The name must conform to the C/C++ conventions.

You must also specify the program names (start address names) when generating the UTM application in the PROGRAM KDCDEF application for each name (see the openUTM manual "Generating Applications").

10.1.2 Parameters of a C/C++ program unit

A C/C++ program unit contains at least one (but usually several) parameters that are passed in the form of addresses as follows.

```
[extern "C"] void cprog (kb [,spab] [,param_1] ...[,param_n])
```

extern "C" is only necessary for C++ program units: You must identify C++ program units as external "C" links in your source code for openUTM, otherwise errors will occur during linking.

void A C/C++ program unit is defined as a function of type *void*.

cprog The name of the program unit. The name must be specified during the generation in the PROGRAM statement; see the openUTM manual "Generating Applications".

kb The name of the communication area (KB). You may choose any name, but the communication area must then be declared under this name. The header file *kcca.h* is provided for use with the communication area.

spab The name of the standard primary working area. You may choose any name, but the standard primary working area must then be declared under this name. The header file *kcpa.h* is provided for use with the KDCS parameter area.

param_1 These are the names of additional objects (AREAs) that must also be declared. In particular, these
... objects could be storage areas that serve to expand the standard primary working area.

param_n

If these objects are not used, then this data does not have to be specified.

The *kcca.h*, *kcpa.h*, *kcapro.h* and *kcdf.h* header files are included implicitly when the *kcmac.h* header file is used. This means that you no longer have to explicitly specify these files as header files in the actual program. The definitions contained in these files are available at all times to the programmer.

The value `KDCS_SPACES` is defined in the include file *kcmac.h* for the transfer of blanks to Char arrays. The value `KDCS_NULL` is available for the transfer of the value "binary zero" to Char parameters.

10.1.3 Declaring data

You must explicitly declare all formal parameters. Please note the points described below when doing so.

10.1.3.1 Communication area

Each program unit, including the event exits (exception: INPUT exit), must contain a data structure that describes the KDCS communication area. Use the *kcca.h* header file for this purpose.

10.1.3.2 Standard primary working area

A C/C++ program unit generally also contains a data structure for the standard primary working area. If the standard primary working area is used by the program unit, then it should include the KDCS parameter area (*кспа.н* header file). You should also store the KDCS message areas and other variable data in the standard primary working area.

If you do not store variable data in the standard primary working area, then you must make sure that the program unit is reentrant by storing it in the automatic area of the function, for example.

You must define the KDCS message areas yourself. For calls that request information from openUTM (KDCS_INFOSI, KDCS_INITPU, for example) there are specific data structures provided in the header files. If you are working with a formatting system, you can use automatically generated address assistants to format the KDCS message area (see the formatting system manual).

In the following example, the communication area also contains a KB program area for transferring data to follow-up program units. The message area is located in the SPAB.

Example

```
#include <kcmac.h> /* UTM data structures */
#include <forma3a.h> /* Structure of the addressing */
/* assistant for +format forma3 */

struct ca_area
{ struct ca_hdr ca_head; /* KB header */
  struct ca_rti ca_return; /* KB return area */
  struct ca_prog_area
  { char ca_info[22]; /* Application-specific */
    char ca_start[2]; /* declaration of the KB */
    char ca_dest[2]; /* program area */
    char ca_fl_day[5];
    char ca_fl_nrl[5];
    char ca_fl_nr2[5];
  } ca_prg;
};

struct work
{ union kc_paa param; /* KDCS parameter area */
  struct msg_area
  { forma3a std_mask; /* Declaration +format forma3 */
    ...
  } msg_a; /* KDCS message area */
};

void cprog (struct ca_area *ca, struct work *spab)
{.../* Start of the function area of the program unit */ ...
```

10.1.3.3 Other data areas (AREAs)

In addition to the communication area and SPAB, you can also pass other areas as parameters (see [Other areas](#)). You create such an area in C/C++ as a source code file that only contains data definitions but no executable statements.

The following examples will demonstrate how you define such areas in C/C++ and how to use them in your C/C++ programs.

Example with AREAs (Unix, Linux and Windows systems)

In the following, two areas are generated, defined in a C source and passed to a program unit. The following are defined:

- the area *area* for direct access (i.e. the data area is passed directly to the program unit)
- the area *areaind* for indirect access

KDCDEF generation

```
AREA area,ACCESS=DIRECT
AREA areaind,ACCESS=INDIRECT
```

Creating a C/C++ source to supply the additional data areas

You define the data structures belonging to the areas in a C/C++ source as follows. In this example, the address of the area is set for *areaind* (i.e. for the area with indirect access) at compilation time.

Definition of areas

```
char area[20] = "Area direct ";
static char area_ind[30] = "Area indirect ";
char *areaind = &area_ind[0];
```

You have to compile the C/C++ source with the C/C++ compiler and link the created object module to the program units.

If you want to set the address of the area *areaind* during the application run, you have to define *areaind* in the C/C++ source as follows:

```
char *areaind:
```

During the application run (typically in the START event exit) you then have to supply *areaind* with the address of the area that you want to pass to the program units as a parameter – by means of the following statement, for example:

```
static char area_ind[30] = "Area indirect ";
areaind = &area_ind[0];
```

This makes it possible, for example, to open a shared memory in the START event exit and store the address of the shared memory in the pointer variable *areaind*. The program units are thus able to access the shared memory.

A program unit in which you use the areas or one of the areas must be as below. Note that the order of the areas in the parameter list has to be the same as the order of the AREA statements at KDCDEF generation.

Program unit in C

```
void areaprg (  
struct spab *spab ,  
struct kc_ca *kb ,  
char area1 [20] ,  
char area2 [30] )  
{  
printf ( BUFFER  
, "Hello world from UTM (Lterm = %.8s)\n"  
"Area is '%s' \n"  
"Area (indirect) is '%s' \n"  
, kb -> kopf.kclogter  
, area1  
, area2  
);  
...  
}
```

Alternatives to AREAs

If program units that use AREAs are to be transferred from one application to another application, then the use of AREAs can lead to problems due to possible differences in the parameter lists.

The following alternatives are available for C/C++ programs. You must determine whether the data area is stored in memory local to the process or in shared memory on Unix and Linux systems or in the memory mapped file on Windows systems.

BS2000 systems

Data areas in local process memory

To use this option, it is necessary to provide a global C/C++ structure which other modules can then access with the same definition and with the 'external' storage class attribute.

Unix, Linux and Windows systems

For Unix and Linux systems in shared memory and for Windows systems in the memory mapped file:

In the start exit you must provide a data structure (see example 3):

```
static DataAreas struct {  
    struct table *TABLE1;  
    struct table *TABLE2;  
    struct table *TABLE3;  
};  
...  
struct DataAreas ExternDataAreas;
```

The shared memory area will then be requested in the start exit and the addresses will be set in the ExternDataAreas data structure.

Other program units will access the data structure with:

```
extern struct DataAreas ExternDataAreas;
```

Example with AREASs (BS2000 systems)

You must provide a data area (see the example) which has been written in Assembler, for example:

```
TABLE1    CSECT PUBLIC
          DS      CL64
          END
```

This CSECT is compiled and may be linked with other modules. The module (without an additional module that has code linked to it) should be named MTABLE1; you should then generate it as a load module:

```
LOAD-MODULE MTABLE1
           , LOAD-MODE = (POOL , poolname , NO-PRIVATE-SLICE ) -
           , ...
```

You then make it possible for a program unit or event exit to access the data area with:

```
extern struct table TABLE1;
```

This program unit or event exit must then be linked dynamically afterwards.

Example with AREAs (all systems)

The areas TABLE1, TABLE2 and TABLE3 have been defined in this order with the AREA statement. TABLE3 is required in a program unit. TABLE1, TABLE2 and TABLE3 have the same structure and are defined as follows:

```
struct TABLE
{
  int   no;
  int   tag;
  char  name[20];
  char  company[20];
  int   order_no;
  int   quantity;
  float price;
  int   discount;
};
```

The addresses of these areas are passed as follows:

```
...
#include <kcmac.h>                                /* UTM data structures */
...
struct ca_area
  {...};
struct work
  {...};
struct TABLE
  {...};
...
void cprog (struct ca_area *ca, struct work *spab, struct TABLE *TABLE1,
            struct TABLE *TABLE2, struct TABLE *TABLE3)
{ ...
```

10.1.4 Data structures for C/C++ program units

In order to structure the data areas, the following header files containing predefined data structures are supplied with openUTM.

On BS2000 systems, the data structures are present in the library SYSLIB.UTM.070.C.

On Unix, Linux and Windows systems, the data structures are present in the *include* directory in the UTM directory *utmpath*.

Name	Contents and meaning
kcapro.h	Optional second parameter area for the APRO call: This area is used to select special combinations of OSI TP functions and the type of security. <i>kcapro.h</i> is included by <i>kcmac.h</i> .
kcat.h	KDCS attribute functions (only on BS2000 systems): When using +formats, you can change the attribute field formats with the symbolic names for attribute functions.
kcca.h	The data structure for the KDCS communication area; this area contains: <ul style="list-style-type: none">• current service and program data,• return data from a UTM call and• if desired, the communication area program area for passing data between programs in a service. You must also define the fields of the communication area program area. <i>kcca.h</i> is included by <i>kcmac.h</i> .
kccf.h	Only on BS2000 systems: Defines the second parameter passed by openUTM during the INPUT event exit. In this parameter openUTM passes the contents of the control fields of screen formats to the program unit. This second parameter is also called the control field area for this reason.
kcdad.h	Data structure for the DADM call: You should place this data structure in the KDCS message area during a DADM RQ KDCS call.
kcdf.h	KDCS screen functions: Using these symbolic names, you can influence the screen output by placing the name of the desired function in the KCDF field of the KDCS parameter area. <i>kcdf.h</i> is included by <i>kcmac.h</i> .
kcinf.h	Data structure for the INFO call: You should place this data structure in the KDCS message area during a INFO DT/SI/PC KDCS call.
kcini.h	Defines a second parameter area for the INIT call (only required for INIT PU): openUTM returns the information queried with the INIT PU call in this parameter area.
kcinp.h	Data structure for the INPUT exit: This data structure contains the input and output parameters of the INPUT exit.

Name	Contents and meaning
kcmac.h	KDCS macro interface for C/C++: This file contains all macros in the C/C++ macro interface as well as the include statements for the <i>kcpro.h</i> , <i>kcca.h</i> , <i>kcdf.h</i> and <i>kcpa.h</i> header files.
kcmsg.h	Data structure for the UTM messages: You will need this data structure if you handle UTM messages in an MSGTAC routine or when you want to evaluate the SYSLOG file using your own program.
kcpa.h	Data structure for the KDCS parameter area: This area contains the parameters of a KDCS call. <i>kcpa.h</i> is included by <i>kcmac.h</i> .
kcpad.h	Data structure for the PADM call: You should place this data structure in the KDCS message area during a PADM AI/PI KDCS call.
kcsgst.h	Data structure for the SIGN call: You should place this data structure over the message area when issuing the KDCS call SIGN ST with KCLA > 0.

Insert the data structures you will use with *#include* before the call to the program unit. You must explicitly declare the corresponding areas (communication area, KDCS parameter area,...) in the program unit.

Example 3

```

/* insert constants and data structures */
#include <kcmac.h>                /* UTM data structures      */
#include <kcinf.h>
    struct ca_area {...};
    struct work
    { union kc_paa param;
      struct msg_area
      { struct kc_dttm  info_time;    /* area for INFO DT      */
        struct kc_sysinf info_sys;   /* area for INFO SI      */
        char text[200];
      } msg_a;
    };
void cprog (struct ca_area *ca, struct work *spab)

```

10.1.5 Command section of a C/C++ program unit

You can design the command section of a C/C++ program unit any way you want. You merely need to abide by a few rules pertaining to transaction processing as described in detail in chapter "[Structure and use of UTM programs](#)":

- the program units are subroutines of the UTM main routine KDCROOT
- the program units must be reentrant
- dialog program units must observe the strict rules of the dialog.

KDCROOT is used to designate the UTM main routine. The source program for KDCROOT is created with the KDCDEF generation tool; see the openUTM manual "Generating Applications".

There are special rules for event exits that will be described in section "[Event exits](#)".

Local classes in C++ program units

If a local class is declared in a C++ program, then the destructor for this class may only be executed if the class is in a block whose block terminator "}" is reached before the PEND call. This restriction does not apply under LINUX.

Recommendation: Local classes should be used within their own "inner" block.

Example

```
//extract of cpphello.C in sample Application
extern "C" void cpphello (struct kc_ca *kb, struct work *spab)
{
    {
        Demo Autoclass('A');
        // further code using Autoclass
    }
    // reached after destructure call for Autoclass
:
:
    /* PEND-FI - Call */
    KDCS_PENDFI();
}
```

KDCS calls in C/C++ program units

KDCS allows you to use the using the C/C++ macro interface, which makes it easy to supply the parameters with data (see "[C/C++ macro interface](#)") when calling UTM functions.

10.1.6 C/C++ macro interface

To make the passing of parameters through the KDCS interface easier, macros are provided in the *kcmac.h* header file for each of the KDCS calls. These macros contain all the data specifications required for a KDCS call as macro parameters. These macros execute the desired call and then provide a return code (see also "[Programming the KDCS error handling routines](#)").

The names and characteristics of the various macros and how the macro names were created will be explained in the following section. The preparations you must make in order to utilize the *kcmac.h* header file are discussed. You will find an example of a macro call and a program listing of an executable KDCS program that will clarify the use of the *kcmac.h* header file at the end of the section.

Using KDCS_SET to prepare for a call

In each compilation unit in which you want to call a KDCS macro, you must execute the following two actions before the first macro call:

- Copy the include file *kcmac.h* into the compilation unit
- Copy the *kcmac.h* header file into the program unit

The four header files *kcca.h*, *kcpa.h*, *kcpro.h* and *kcdf.h* are used implicitly when *kcmac.h* is used, i.e. the definitions therein are available to the programmer at all times.

- Call the KDCS_SET(pb,hdr,rti) macro for initialize the areas

pb: pointer to the KDCS parameter area.

hdr: pointer to the header area of the communication area (ca_hdr data structure).

rti: pointer to the return area of the communication area (ca_rti data structure).

The KDCS_SET call establishes the connection between the KDCS macros and the programmer's definitions for the parameter area and the communication area. You can call this macro more than once. It is therefore possible to use several different parameter areas, for example.

Macro names

The names of the macros are created according to the following rules:

A KDCS macro name always begins with the prefix "KDCS_". The operation code of the desired KDCS call follows in upper case letters. If necessary, the operation modifier is appended to the operation code (also in uppercase letters).

Examples:

KDCS_INIT, KDCS_LPUT, KDCS_MGET

KDCS_MPUTNT, KDCS_PENDFI, KDCS_SPUTMS

The DPUT calls using a "+T", "-T", "+I" or "-I" as the kcom parameter represent an exception to these rules. These macros are named: KDCS_DPUTPT, KDCS_DPUTMT, KDCS_DPUTPI and KDCS_DPUTMI.

Other exceptions are the APRO calls used to address OSI TP partners:

KDCS_APRODM_OSI, KDCS_APROAM_OSI, KDCS_APRODM_OSI_O, KDCS_APROAM_OSI_O

Macro parameters

The macro parameters are each named after the KDCS parameters for which they will contain values (*kcrn*, *kclt*, *kchour*, *kcpi*,...). The KDCS message area is named *nb* and, if it is needed, is always specified as the first parameter.

There are three different types of KDCS parameters: character arrays, letters and numbers:

- Character arrays

In the KDCS interface these parameters are either two, three or eight characters long. In the C/C++ macro interface these parameters are specified as pointers to a C string of any length.

Internally, these parameters are converted to arrays of characters of the required length by either appending any eventually missing spaces to the end of the C string or by ignoring all superfluous characters at the end of the C string. In this manner, for example, for an array of length 8, three spaces " " or no space "" are converted to the same string, namely eight spaces: " ".

A string such as "xyz" is filled up with five spaces to "xyz ". The conversion is performed without adding an end of string character ("\0").

Parameters of this type are: *kcrn*, *kcfn*, *kclt*, *kcpa*, *kcus*, *kcadrft*, *kcact*, *kcpi*, *kcpos*, *kcneg*, *kccomid*, *kclangid*, *kcterrid*, *kccsname*.

- Letters

In the KDCS interface these parameters are of type character.

In the C/C++ macro interface these parameters are also specified as characters (per value). The parameters are specified in the form: ' ', 'A', 'C', etc.

Parameters of this type are: *kcmmod*, *kcof*.

- Numbers

There are different types of numbers in the KDCS interface: short, unsigned short and numbers that are expected to be in the form of printable text.

In the C/C++ macro interface these parameters are always specified as numbers (per value). These numbers are converted internally to the desired format. Short and unsigned short numbers are passed directly. Numbers that must be provided as text are converted.

Parameters of this type are: *kcla*, *kclm*, *kcdf*, *kclcapa*, *kclspa*, *kcday*, *kchour*, *kcmmin*, *kcsec*, *kcli*.

Simplified parameter passing

The macros know the required length of every parameter and ensure that they are passed correctly (short strings are padded with spaces up to the required length). A parameter only needs to be specified in the macro parameter list and does not have to be passed anymore using *memcpy*. The macros also process all data that was previously processed with *memcpy*. The assignments of the parameters to the appropriate KDCS parameter fields is done implicitly by the C/C++ macros. The parameter types are determined by the C/C++ macro definitions.

For comparison, here is an example of supplying the *kcrn* parameter with data:

- In a direct call:

```
memcpy(pb.kcrn,"rnam",8) /* only kcrn is supplied with data*/
```

- When using a macro:

```
macroname(...,"rnam",...) /* complete KDCS call*/
```

Any parameter fields not used are implicitly set to binary zero. You specify the constant `KDCS_SPACES` for the fields that are to be set to spaces in a call.

Some of the KDCS parameters that were previously passed as an array of characters are usually stored as integers in C.

Such parameters are, for example, the parameters used to specify the time and date: *kcday*, *kchour*, *kcmin*, *kcsec*. Such parameters are expected to be passed as numbers (integers) in the new macro calls. The macros ensure that the data is passed correctly to the interface.

Here is an example of supplying the KDCS call with a time specification for comparison:

- In a direct call:

```
memcpy(pb.kcext.kcdput.kcday, "003", 3);
memcpy(pb.kcext.kcdput.kchour, "11", 2);
memcpy(pb.kcext.kcdput.kcmin, "55", 2);
memcpy(pb.kcext.kcdput.kcsec, "00", 2);
```

- When using a macros:

```
macroname(..., 3, 11, 55, 0)
```

Format of the KDCS call through the C/C++ macro interface

KDCS calls using the C/C++ macro interface have the following format:

```
KDCS_ operation_code [ operation_modifier ] ( parameter_list )
```

If a KDCS message area is required, then its address is always specified as the first parameter. The parameter list can also be empty.

There are a few exceptions to the macro name format (see "[C/C++ macro interface](#)").

Example

```
KDCS_INIT(length_communication_area_program_area, length_standard_primary_working_area);
KDCS_SGETRL(pointer_to_message_area, message_length, name_of_local_secondary_storage_area)
KDCS_PGWTKP()
```

Example: `KDCS_MPUTNT` macro call

In the following the use of a KDCS macro is demonstrated with an example of an MPUT NT call. First, a description of the macros:

```
KDCS_MPUT NT(nb, kclm, kcrn, kcfn, kcfd)
```

char *nb	pointer to the KDCS message area
short kclm	length
char kcrn[8]	space/TAC/service ID
char kcfn[8]	format/space/edit profile

unsigned short kcdf screen fill character / binary zero / ---

The KDCS_MPUTNT macro requires five parameters, one of which is a pointer to the KDCS message area *nb*. This parameter is always passed as the first parameter. The other parameters of the macro originate in the KDCS parameter area. The required type and meaning of each parameter is specified (for example, *kclm* is of type *short* and specifies the length of the area in which the message is to be passed). In the following example, NB is a pointer to the KDCS message area used and *kc_pa* is the KDCS parameter area.

A typical macro call looks like the following call, for example:

```
KDCS_MPUTNT(NB, 10, KDCS_SPACES, KDCS_SPACES, KCNODF);
```

The same call without using a macro looks like (direct KDCS interface call):

```
memcpy(PB.kcop, MPUT, 4);
memcpy(PB.kcom, NT, 2);
kc_pa.kclm=10;
memcpy(kc_pa.kcrn, "      ", 8);
memcpy(kc_pa.kcfn, "      ", 8);
kc_pa.kcdf=0;
KDCS(&kc_pa, NB);
```

DEBUG function

You can enable a logging function during run time for the KDCS calls triggered by the macros. The calling module, the source code line and the KCOP, KCOM, KCRCCC and KDCDCDC KDCS fields are recorded.

The logging function is switched on as follows:

- *Unix, Linux and Windows systems*:
By setting and exporting the KDCS_C_DEBUG environment variable.
The information logged is written to *stdout*.
- *BS2000 systems*:
By setting the *KDCSCDB JOB VARIABLE LINK.
The information logged is written to SYSOUT.
Please note that the job variable link must point to a non-empty job variable.

Example

```
/CREATE-JV    JV-NAME = KDCSCDB
/MODIFY-JV    JV-CONTENTS = KDCSCDB, SET-VALUE = 'YES'
/SET-JV-LINK  LINK-NAME = *KDCSCDB, JV-NAME = KDCSCDB
```

You will find additional information on this subject in the openUTM manual "Messages, Debugging and Diagnostics".

Note: Macros as statement follow-ups

The KDCS macros are not simply individual C/C++ functions, rather they are a series of several statements. This means that a single macro must be handled exactly as would be required for a series of several statements. This peculiarity is normally not relevant, and the macros can be used like normal C/C++ functions. There are, however, program structures that require single statements, for example within an if statement:

```
if (condition) STATEMENT else STATEMENT;
```

Because the macros consist of several individual statements, it is not possible simply to use a macro as if it were one (single) STATEMENT. You must therefore first designate the macro as a unified block. This is done by using curly brackets: {macro;}. Instead of incorrectly writing

```
if (condition) macro; else macro;      /* W R O N G ! ! ! ! ! */
```

you should write:

```
/* C O R R E C T ! */
```

```
if (condition) {macro;} else {macro;}
```

10.1.7 Event exits

The INPUT, START, SHUT and VORGANG event exits may not contain any KDCS calls. They should be written as subroutines and must end with the *return* statement.

For START, SHUT and VORGANG the addresses of the communication area (KB) and standard primary working area (SPAB) are passed as parameters; these areas must be declared accordingly (just like for program units containing KDCS calls). In "[Example of a complete UTM application on BS2000 systems](#)" you will find an example of a combined START/SHUT exit.

openUTM passes an address for the INPUT exit. This address specifies the INPUT parameter area. The header file *kcinp.h* contains the structure of the INPUT parameter area; the name of the data structure is *kc_inp*. In "[Example: INPUT exit \(BS2000 systems\)](#)" you will find an example of a INPUT exit.

On BS2000 systems, it is also possible to pass the address of a control field area. The include file *kccf.h* is available for the control field area.

There can be a maximum of eight START and eight SHUT event exits per application. There can only be one INPUT and one VORGANG. For further information on event exits, please refer to [chapter "Event functions"](#)

10.1.8 Programming the KDCS error handling routines

The *kcrccc* return code in the return area of the communication area is returned as a threecharacter field in the C/C++ KDCS interface. If the C/C++ macros are not used, then the values must be compared using the *strncmp* function.

The request for the return code is simpler when the macro interface is used:

The *kcmac.h* header file defines a return code in the static variable *long* KCRCC that contains the integer value of the *kcrccc* field after each macro call. Determining if an error occurred during the call is then limited to checking KCRCC.

For comparison, here are two examples of determining if an error has occurred after a KDCS call:

- for a direct call:

```
if(strncmp(kb->rti.kcrccc,"000",3) != 0) ...
```

- when using a macro:

```
if (KCRCC != 0) ...
```

To ensure a better diagnosis of a problem, all unused parameters are automatically set to binary zero before a KDCS call when the macros are used.

In this manner, the entire parameter area contains a precisely defined set of data. If an error occurs, the parameter area can be specifically checked and any deviation from the expected contents can be detected.

10.1.9 Programming user-specific error handling (Unix and Linux systems)

Additional functions are available on Unix and Linux systems, which go beyond the normal KDCS error handling:

- User signal routines

The two functions `KCX_REG_USER_SIGNAL_HANDLER()` and `KCX_UN_REG_USER_SIGNAL_HANDLER ()` are available to you for registration and deregistration of the user signal routine. The user signal routine is called when a signal occurs and must be created by the user.

- Exchange of the utmwork process after PENDING with `KCX_SET_RELOAD_FLAG()`
- Creation of a UTM dump with `KCX_WRITE_DUMP()`

The prototypes for all functions are located in the C header file `kcerrh.h` supplied at `utmpath/include`.

10.1.9.1 User signal routines (Unix and Linux systems)

A user signal routine is registered in the program unit or in the Start-Exit with the function `KCX_REG_USER_SIGNAL_HANDLER()`, i.e. user-specific signal handling is only activated once this is done.

`KCX_UN_REG_USER_SIGNAL_HANDLER()` is used to deregister it and thus deactivate it.

Function `KCX_REG_USER_SIGNAL_HANDLER()`

The function `KCX_REG_USER_SIGNAL_HANDLER()` requires a function pointer that points to a user signal routine as an argument.

C prototype

```
typedef void utm_user_signal_function_t(int *, char *, char *);
void KCX_REG_USER_SIGNAL_HANDLER(utm_user_signal_function_t
                                **p2p_user_signal_func_param);
```

Example

```
void my_user_signal_handler(int * p_signal_number,
                           char * signal_text,
                           char * stack_info);
typedef void utm_user_signal_function_t(int *, char *, char *);
static utm_user_signal_function_t * p_user_signal_func;
p_user_signal_func = my_user_signal_handler;
KCX_REG_USER_SIGNAL_HANDLER(&p_user_signal_func);
```

Function `KCX_UN_REG_USER_SIGNAL_HANDLER()`

Calling `KCX_UN_REG_USER_SIGNAL_HANDLER()` from the application program deregisters, i.e. deactivates, the current user signal routine in openUTM. From this point onwards, the default openUTM error handling is activated.

C prototype

```
void KCX_UN_REG_USER_SIGNAL_HANDLER(void);
```

Programming the signal routine

The user signal routine is always assigned three arguments:

Param-1

The system signal number as a binary variable 4 bytes in length, i.e. data type "int".

Param-2

"Printable" explanation of the system signal number, e.g. "Segmentation fault" for signal 11, maximum 255 bytes long and ending with a null byte.

Param-3

Stack information, multi-line and maximum 4096 bytes long, ending with a null byte.

The user signal routine should only initiate “clear-up actions” and terminate the program with PEND RE:

- KDCS call RSET,
- KDCS call MPUT NE with error info from the user signal routine parameters,
- KDCS call PEND RE with KCRN="Follow-up TAC".

Note

The function may not be exited with *exit()*.

Example

```
static void my_user_signal_handler( int* p_signal_number
    , char * utm_signal_string
    , char * utm_stack_string )
{
struct kc_ca *pntrCa ;
struct spab *pntrSpab;
fprintf(stderr, "Error Handler \"my_user_signal_handler\"
    called:\n" "signal_number %d\n"
    "utm_signal_string \"%s\"\n" "utm_stack_string \"%s\"\n",
    *p_signal_number, utm_signal_string, utm_stack_string);
fflush(stderr);
```

This is followed by e.g. KDCS("RSET"), KDCS("MPUT") and KDCS("PENDRE").

Example of parameters transferred to a user signal routine

```
utm-signal-number: 8
utm-signal-string: " Arithmetic Exception"
utm-stack-string:
[5] KCSSIGNAL(signal_nbr = 8) (optimized), at 0xfebb39a8 (line ~2458) in "kcxrtst.c"
[6] __sighndlr(0x8, 0x0, 0xffbfbff8, 0x2f1a4, 0x0, 0x0), at 0xfelca79c
[7] fb(), line 115 in "regsignal.c"
[8] fa(), line 104 in "regsignal.c"
[9] regsig(kb = 0xfed3a788, spab = 0xfed42808), line 82 in "regsignal.c"
[10] KDCCC(iutmhlpar = 0xfed4cdd8), line 855 in "root.c"

[11] KDCHLLC(iutmhlpar = 0xfed4cdd8, lgcon = 0x30400) (optimized), at 0xfebb26ac (line
~1922) in "kcxrtst.c"
[12] START_TEILPROGRAM(adfptr01 = 0xffbfc940 "F^A") (optimized), at 0xfec0223c (line
~14697) in "kdcrmm.c"
[13] KDCRTMM(RTMM_CALL = 0xffbfd0e4 "KDCRTSI \xfe\xdl\xec`) (optimized), at 0xfebf9af4
(line ~9766) in "kdcrmm.c"
[14] KDCRTSI() (optimized), at 0xfec04dc0 (line ~818) in "kdcrtsi.c"
[15] KDCRTST(argc = 80, argv = <value unavailable>, pKDCMDATA = 0x20) (optimized), at
0xfebblf74 (line ~1786) in "kcxrtst.c"
[16] kcxmnt(argc = 9, argv = 0xffbfda74), line 568 in "xirtend.h"
[17] main(argc = 9, argv = 0xffbfda74, envp = 0xffbfda9c) (optimized), at 0x13b1c (line
~64) in "mainutm.c"
```

10.1.9.2 Exchanging the utmwork process (Unix and Linux systems)

The function `KCX_SET_RELOAD_FLAG()` initiates exchange of a utmwork process after the KDCS call `PEND RE`.

C prototype

```
void KCX_SET_RELOAD_FLAG(void);
```

Call

```
KCX_SET_RELOAD_FLAG();
```

10.1.9.3 Creating a UTM dump (Unix and Linux systems)

The function `KCX_WRITE_DUMP()` initiates creation of a UTM dump.

C prototype

```
void KCX_WRITE_DUMP(char * reason);
```

The function requires a pointer to a 6 byte long field containing the reason for the dump.

Example for the call

```
KCX_WRITE_DUMP("MYDMP1");
```

10.1.10 Modifying KDCS attributes (BS2000 systems)

If you use `+formats` or `#formats`, you can change the attributes of format fields in the program.

The KDCS attribute combinations are contained in the header file `kcat.h` and are copied into the program unit via include statements.

The `kcat.h` header file also contains the `KDCATTR` macro with which you can set the KDCS attribute combinations. `KDCATTR` is called as follows:

```
KDCATTR (attribute_field, attribute_value);
```

The names and characteristics of the possible KDCS attribute combinations are listed in your formatting system manual.

Example

The "name" field is to be output to the screen as a protected field; `a_name` is the attribute field corresponding to this.

```
KDCATTR (spab->std_mask.a_name, KCPROT);
```

The `+format "FORMAT5"` contains the "FELD1" to "FELD5" fields. FELD4 should be sent to the screen blinking, all other fields maintain the attributes from the format description.

```
#include <kcat.h>
unsigned short mput_features;
...
{... a_format5 mask_out; ...} *spab; 1)
...
/*MPUT call */
...
KDCATTR (mask_out.a_field4, KCSIGN);
KDCATTR (mask_out.a_field1, KCNOATTR);
KDCATTR (mask_out.a_field2, KCNOATTR);
KDCATTR (mask_out.a_field3, KCNOATTR);
KDCATTR (mask_out.a_field5, KCNOATTR);
...
KDCS_MPUTNT (&mask_out, sizeof(a_format5),
             KDCS_SPACES, KDCS_SPACES, mput_features);
```

¹⁾ Declares the addressing assistants for the `+format "format5"`.

10.1.11 Platform-specific characteristics on BS2000 systems

Compiling C/C++ program units

If a link and load module (LLM) is to be created that consists of a code CSECT and a data CSECT section at compilation of C/C++ program units, you must set `MODULE-GENERATION(MODULE-FORMAT=LLM)` for the `COMPILER-ACTION` option when calling the compiler. The LLM must be made available in a PLAM library for linking with the `BINDER`. Object modules can also be created for your C program units (type=R in LMS).

Using shareable code

If you plan on loading C/C++ program segments as shareable code, then you must set the following option when compiling:

```
COMPILER-ACTION=MODULE-GENERATION( SHAREABLE-CODE=YES , . . . )
```

The shareable code does not have to be stored in its own object module, rather it can be placed together with the non-shareable segment in an LLM that is divided into a public and a private slice.

The shareable program segments only need to be loaded together once for all processes (tasks) of the application (s). Then only the non-shareable segments need to be loaded into the local task memory.

openUTM offers several ways of loading shareable objects:

- as a non-privileged subsystem
- with the `ADD-SHARED-PROGRAM` command into system memory
- into a common memory pool in user memory (class 6 memory).

You can find additional information on compiling shareable code in the User's Manual for your compiler. The openUTM manual "Generating Applications" as well as the openUTM manual "Using UTM Applications on BS2000 Systems" contains detailed information on linking and loading shareable code.

Creating formats with the IFG

A detailed explanation of how to create formats using the IFG can be found in the IFG manual. Please follow the guidelines below when creating these formats for use with openUTM:

- The format name may be at most 7 characters long.
- Select "Structure of the data transfer area" in the user profile:
 - for #formats: separated attribute blocks and field contents
 - for *formats: unformatted, without attribute fields
 - for +formats: unformatted, with attribute fields
- For the C/C++ programming languages the IFG always creates **one** address assistant. Fields with the "arithmetic field data type" are represented as character strings (char [..]).

- Please note when defining the addressing assistants for *formats and +formats that openUTM deletes the transaction code from the UTM message for MGET and FGET (as long as this is not explicitly prevented in an INPUT exit). If the first field in the format contains the transaction code, then you can take this into account by reading the UTM message into the second field.

Example

```

struct work
{ union kc_paa param;
  FORM1 std_mask;           /* declare addressing aid for */
  ..                        /* the *format FORM1      */
} *spab;
  ...
  ...
/* MGET call */
KDCS_MGET ( spab->std_mask.FUNCTION      1)
           ,sizeof( FORM1 )
           ,"*FORM1 "                   );
  ...
/* MPUT call */
KDCS_MPUTNT (&spab->std_mask,sizeof(FORM1)
            ,KDCS_SPACES,"*FORM1 " ,KCNODF);
/* PEND FI call */
  ...

```

1) FUNCTION is the second input field of the format.

- When preparing for the application, you bring the formats into the format application field (format library). You specify these names together with the FHS start parameters.

Extended line mode

You must define the control characters yourself when working in extended line mode if they are not available in C/C++. You will find a list of which control characters correspond to which hexadecimal values in the "TIAM User Guide", for example in the description of the VTCSET macro.

10.1.12 Platform-specific characteristics on Unix and Linux systems

Signal handling

Program units in C have limited usage of signals on Unix and Linux systems. The SIGUSR1 and SIGUSR2 signals can be trapped by the C program unit in the start exit of a work process. All other signals are handled by the openUTM system code itself by default.

As an alternative to the default handling of signals in openUTM, you can program a separate user signal routine for certain signals and register it in openUTM, see section [“Programming user-specific error handling \(Unix and Linux systems\)”](#).

CMX interface in utmwork

You must note the following when using CMX calls in C/C++ program units:

For technical reasons, a CMX simulation is used in the UTM library libwork.a and libwork.so in UTM applications with OSI TP. It is therefore not possible in this case to use CMX calls in a C/C++ program unit.

Calling the fork() function in a C/C++ program unit

You must note the following when calling the `fork()` function in C/C++ program units: No openUTM program interfaces may be used in a child process created using `fork()`. Otherwise, the UTM application will terminate abnormally.



For details on creating and linking shared objects, compiling program units and linking applications, see the manual openUTM manual “Using UTM Applications on Unix, Linux and Windows Systems”, section “Creating the application program”.

10.1.13 Platform-specific characteristics on Windows systems

On Windows systems, the projects must be created with Visual Studio as of Version 2010.

Signals are not supported on Windows systems.



For details on creating DLLs, compiling program units and linking applications with Visual Studio, see the manual openUTM manual "Using UTM Applications on Unix, Linux and Windows Systems", chapter "Creating the application program".

10.2 Programming examples in C/C++

In this section you will find examples of code for individual KDCS calls executed through the C/C++ macro interface, examples of complete C programs, an INPUT exit, an MSGTAC event service and an example of a complete UTM application.

10.2.1 Examples of individual KDCS calls

In this section you will find examples of code for the following KDCS calls:

- MGET
- MPUT
- DPUT
- MCOM with DPUT in a job complex
- APRO with MPUT for distributed processing

Because the rest of the KDCS calls are programmed analogously, we will not explicitly present all of the calls.

In a KDCS call *&pa* designates the address of the KDCS parameter area and *&ma* the address of the KDCS message area.

MGET call

- An unformatted, 80 byte long dialog message is to be received. If the message received is too short due to an error, then a request for new input is sent.

```
KDCS_MGET (&ma, 80, KDCS_SPACES);
if (KCRCC != 0)
    mget_error();
if ( pa.kcla > ca->ca_return.kcrlm)
    r_mput ();
```

In the *r_mput ()* routine a request to repeat the input is sent to the terminal with MPUT.

- In a running service an input which consists of a short message, created with the F2 function key, as well as 10 characters of data can be entered. The input should trigger a special function. The F2 key was assigned the 21Z return code during generation.

```
KDCS_MGET (&ma, input_lth, dev.features);
if (KCRCC == 21 ) {
    KDCS_MGET (&ma, 10, KDCS_SPACES);
    if (KCRCC != 0 )
        mget_error();
}
/* return code for F2 */
```

BS2000 systems

- The "FORM15" format was requested by a terminal. The length of the unprotected data is 500 characters in various format fields. This format should be received in the program. FORM15 was declared as a std_mask in the program.

```
KDCS_MGET (&ma.std_mask,500,"*FORM15 ");
if (KCRCC == 5) /* invalid format ID */
    format_error();
if (KCRCC != 0)
    mget_error();
```

In the format_error routine the format must be output again in order to continue working with the correct format.

MPUT call

- An unformatted, 80 byte long UTM message is to be sent to the terminal.

```
KDCS_MPUTNE (&ma,80,KDCS_SPACES,KDCS_SPACES,KCNODF);
if (KCRCC != 0 )
    mput_error();
```

BS2000 systems

- The last UTM message in a service is to be sent to a terminal in the format mode. The name of the *format is "FORM15". The screen should be cleared beforehand.

```
KDCS_MPUTNE (&ma,500,KDCS_SPACES,"*FORM15 ",KCREPL);
if (KCRCC != 0 )
    mput_error();
```

REPLACE is executed by default during a format change. The output is performed in order to rule out the possibility of an error due to the undefined contents of a field.

- In a "FORM10" *format that is still on the terminal according to the last input, all unprotected fields are to be erased as a result.

```
.
KDCS_MPUTNE (&ma,0,KDCS_SPACES,"*FORM10 ",KCERAS);
if (KCRCC != 0 )
    mput_error();
```

DPUT call

- A queued job with an 11 character long UTM message is to be sent on Nov.11 (= 315th day of the year) at 11:11 AM to a program unit (absolute time). The TAC name is "ALAAF".

```
KDCS_DPUTNE (&ma,11,"ALAAF",KDCS_SPACES,0,'A',315,11,11,0);
if (KCRCC != 0) /* A = absolute time */
    dput_error();
```

BS2000 systems

- An 80 character long queued message is to be output on terminal 'DSS1' in 1 hour (relative time). The 'acoustic alarm' (BEL) screen function should be triggered when the message is output.

```
KDCS_DPUTNE (&ma,80,"DSS1",KDCS_SPACES,KCALARM,'R',0,1,0,0);
if (KCRCC != 0) /* R = relative time */
    dput_error();
```

Job complex: MCOM and DPUT call

A formatted queued message (200 bytes) is to be sent to the printer PRINTER2 on the same day at 18:00. The printer confirmation is handled in the program.

For a positive confirmation an asynchronous program receives a confirmation job using the PRINTPOS TAC with a 20 byte long message, for a negative confirmation an asynchronous program is started with the TAC PRINTNEG (without a message). For a negative confirmation an 80-byte piece of user information is logged; it can be read using DADM UI.

The job complex is framed by two MCOM calls; the target of the print job (=base job) and confirmation jobs are set in the call MCOM BC; the complex identification is "**PRICOMP".

```

/* Begin of the complex */
KDCS_MCOMBC ("PRINTER2", "PRINTPOS", "PRINTNEG", "*PRICOMP");
if (KCRCC != 0 )
    mcom_error();
/* DPUT-message for printer */
KDCS_DPUTNE (&ma1,200,"*PRICOMP","*FORM1 ",KCNODF,'A',
             ca->ca_head->kccv_doy,18,0,0);
if (KCRCC != 0 )
    dput_error();
/* acknowledgment job in positive case */
KDCS_DPUTPT (&ma2,20,"*PRICOMP");
if (KCRCC != 0 )
    dput_error();
/* User information in negative case */
KDCS_DPUTMI (&ma3,80,"*PRICOMP");
if (KCRCC != 0 )
    dput_error();
/* acknowledgment job in negative case */
KDCS_DPUTMT (&ma2,0,"*PRICOMP");
if (KCRCC != 0 )
    dput_error();
/* End of complex */
KDCS_MCOMECC ("*PRICOMP");
if (KCRCC != 0 )
    mcom_error();

```

Distributed processing: APRO call followed by MPUT

The dialog service is to be addressed by the job-submitting service with the 'LTAC1' transaction code of the application 'PARTNER1' (two stage addressing). The job-receiving service will be assigned the service identification '>VGID1'. Finally, a 100 byte long MPUT message is sent to the partner application in line mode.

```

KDCS_APRODM ("LTAC1 ", "PARTNER1", ">VGID1 ");
if (KCRCC != 0 )
    apro_error();
...
KDCS_MPUTNE (&ma,100,">VGID1 ",KDCS_SPACES,KCNODF);
if (KCRCC != 0 )
    mput_error();

```

10.2.2 Example of a complete C program unit

The following is an example of an executable KDCS program unit in the C programming language. The program outputs the text "hello world !" and the names of the logical terminals.

Program mhello

```
#include <kcmac.h>
struct work {
    union kc_paa call_pb;
    char  buffer[400];
};
struct kc_ca {
    struct ca_hdr kopf;
    struct ca_rti rfld;
    char  kcprg[500];
};
#define NB      spab->buffer
#define KBKOPF kb->kopf
#define KBRFLD kb->rfld
#define PB      spab->call_pb
void mhello ( struct kc_ca *kb, struct work *spab )
{
    /* KDCS interface initialization */
    KDCS_SET( &PB, &KBKOPF, &KBRFLD );
    /* INIT - Call */
    KDCS_INIT( sizeof(struct kb->kcprg), sizeof(struct work) );
    /* MPUT-NT - Call */
    strcpy ( NB, "hello world !\n\n" );
    KDCS_MPUTNT( NB, (short)strlen(NB), KDCS_SPACES,
                KDCS_SPACES, KCNODF );
    /* MPUT-NT - Call */
    sprintf ( NB, "lterm = %.8s \n", KBKOPF.kclogter );
    KDCS_MPUTNT( NB, (short)strlen(NB), KDCS_SPACES,
                KDCS_SPACES, KCNODF );
    /* PEND-FI - Call */
    KDCS_PENDFI();
}
```

10.2.3 Example: INPUT exit (BS2000 systems)

The *forinput* INPUT exit is called when data is input in the format mode, and it reacts to the input as follows:

User commands are initiated:

- KDCOUT: Press the F1 key
- KDCDISP: Press the F2 key
- KDCOFF: the first character of the input is "/"; this is only accepted outside of a service.

If the user is also allowed to input KDCLAST and KDCFOR, then the program must be expanded accordingly.

This INPUT exit is generated with the KDCDEF statement EXIT:

KDCDEF statement

```
EXIT PROGRAM=FORINPUT,USAGE=( INPUT,FORMMODE)
```

Event exit INPUT

```
#include <string.h>
#include <kcinp.h>
#define KDCDISP 2
#define KDCOUT 1
#define NOKEY 0
#define FKEY 1
#define KDCOFF "KDCOFF "
#define NOTAC (strncmp (param->kcicfinf, "ON", 2) != 0)
#define CV_END (strncmp (param->kcicvst, "EC", 2) == 0)
#define TAC      param->kcicvtac[0]
#define fkey     param->kcifkey
#define cmd      param->kcintac
#define nexttac  param->kcintac
#define errcode  param->kcierred
#define contcode param->kciccd
#define firstchar param->kcifch[0]
#define cut      param->kcicut
static int  key( struct kc_inp * );
static void func_control( struct kc_inp * );
static void cv_continue( struct kc_inp * );
void forinput ( struct kc_inp *param )
{
    if ( key ( param ) == NOKEY)                /* No F-key */
        { if ( CV_END)
            func_control ( param );
          else
            cv_continue ( param );
        }
}

/*****
/*          function key for checking F-key          */
*****/
int key ( struct kc_inp *param )
{
    int key_value = NOKEY;
```



```

if (fkey > 0)
{
    switch (fkey)
    {
        case KDCOUT:
            memcpy (cmd, "KDCOUT ", 8);
            memcpy (contcode, "CD", 2);
            cut = N ;
            memset (errcode,      , 4);
            key_value = FKEY;
            break;
        default: break;
    }
}
return key_value;
}
/*****
/*  function func_control: checking the next FUNCTION out of conversation*/
*****/
void func_control ( struct kc_inp * param )
{
    if (firstchar == / )          /* check the first character*/
    {
        memcpy (cmd, KDCOFF, 8);          /* of input: / = KDCOFF */
        memcpy (contcode, "CD", 2);
        cut = N ;
        memset (errcode,      , 4);
    }
    else                          /* check control field */
    {
        if (NOTAC)                /* no input in control field*/
        {
            memset (nexttac,      , 8);
            memcpy (contcode, "ER", 2);
            cut = N ;
            memcpy (errcode, "ER01", 4);
        }
        else
        {
            switch (TAC)          /* TAC for the next */
            {                    /* conversation */
                case 1 :
                    memcpy (nexttac, "DTAC1 ", 8);
                    memcpy (contcode, "SC", 2);
                    cut = Y ;
                    memset (errcode,      , 4);
                    break;
                case 2 :
                    memcpy (nexttac, "DTAC3 ", 8);
                    memcpy (contcode, "SC", 2);
                    cut = Y ;
                    memset (errcode,      , 4);
                    break;
                case 3 :
                    memcpy (nexttac, "DTAC6 ", 8);
                    memcpy (contcode, "SC", 2);
                    cut = Y ;
                    memset (errcode,      , 4);
                    break;
                default:          /* TAC is invalid */
                    memset (nexttac,      , 8);
                    memcpy (contcode, "ER", 2);
                    cut = N ;
            }
        }
    }
}

```

```
        memcpy (errcode, "ER02", 4);
        break;
    }
}
}
}
}
/*****
/*      function cv_continue: continue the conversation      */
/*****
void cv_continue ( struct kc_inp * param )
{
    memset (nexttac,      , 8);
    memcpy (contcode, "CC", 2);
    cut = N ;
    memset (errcode,      , 4);
}
```

10.2.4 Example: MSGTAC event service

The MSGTAC event service NOHACK counts the number of failed attempts in a TLS. If openUTM accepts a KDCSIGN (i.e. UTM message K008 or K033), then this TLS is deleted.

If after three invalid KDCSIGN attempts the 4th KDCSIGN attempt also fails, then the corresponding terminal should be automatically disconnected using an FPUT call with KCRN="KDCPTRMA". The KDCS message area contains the following administration command, see also the openUTM manual "Generating Applications":

```
PTERM=pterm,PRO=proname,ACT=DIS
```

The K-messages are each read from the MSGTAC program unit using FGET. After "processing" a K-message, the next K-message is read immediately within the same program run using FGET.

Event service MSGTAC

```
#include <stdio.h>
#include <kcmac.h>
#include <kcmsg.h>
#define _K008 (memcmp (NR, "K008", 4) == 0)
#define _K033 (memcmp (NR, "K033", 4) == 0)
/* K008: KDCSIGN accepted */
/* K033: Start-Format */
#define MESSAGE_OK (_K008 || _K033)
#define _K004 (memcmp (NR, "K004", 4) == 0)
#define _K006 (memcmp (NR, "K006", 4) == 0)
#define _K031 (memcmp (NR, "K031", 4) == 0)
/* K004: Invalid Identification */
/* K006: Invalid password */
/* K031: Card not ok */
#define OTHER_MESSAGE !(_K004 || _K006 || _K008 || _K031 || _K033)
#define HACK_MAX 3
#define PTERM " PTERM="
#define PRONAM ",PRONAM="
#define DIS ",ACTION=DIS"
#define OFF ",STATUS=OFF"
#define kcrc_ca->ca return.kcrccc
#define pa spab->param
#define NR spab->ma.kcmsgs.msghdr.MSGNR
#define MSG spab->ma.kcmsgs.msg
#define LTERM spab->ma.lterm
#define hacknr spab->hack_nr
#define admin spab->ma.adm

struct adm_line
{
    char pterm_t[6];
    char pterm[8];
    char pronam_t[8];
    char pronam[8];
    char dis_t[11];
    char off_t[11];
};

struct ca_area
{
    struct ca_hdr ca_head;
    struct ca_rti ca_return;
};

struct work
```

```

{ struct kc_pa param;
  short hack_nr;
  struct msg_area
    { char lterm[8];
      struct adm_line adm;
      struct KCMSGS kcmsgsgs;
    } ma;
  char buffer[100];
};
static void set_lterm( struct work * );
static void set_pterm( struct work * );
void NOHACK (struct ca_area *ca, struct work *spab )
{
  int other_message = 0;
  /* INIT-Operation */
  KDCS_SET (&spab->param, &ca->ca_head, &ca->ca_return);
  KDCS_INIT (0,512);
  /* ***** */
  /* while-loop: reading and processing all messages */
  /* ***** */
  while (KCRCC == 0 )
  {
  /* FGET-Operation: reading the message */
  KDCS_FGET (&spab->ma.kcmsgsgs,132,KDCS_SPACES);
  if (KCRCC != 0 )
    break;
    if (OTHER_MESSAGE)
      { other_message = 1;
        break;
      }
    set_lterm ( spab );
  /* read TLSB */
  KDCS_GTDA (&hacknr,2,"TLSB",LTERM);
  if (KCRCC != 0 )
    break;
    if ((hacknr < 0) || (hacknr > HACK_MAX))
      hacknr = 0; /* Initialize TLS */
  /* If KDCSIGN is correct, initialize the TLS, if not, count the number */
  /* of failed attempts. After the fourth invalid KDCSIGN disconnect the */
  /* correspondending terminal. */
  if ((hacknr < HACK_MAX) && MESSAGE_OK)
    hacknr = 0; /* Initialize TLS */
  else /* invalid KDCSIGN */
    {
      if (hacknr < HACK_MAX)
        ++hacknr;
      else
        { memcpy (admin.pterm_t, PTERM, 7);
          memcpy (admin.pronam_t, PRONAM, 8);
          set_pterm ( spab );
        }
  /* Disconnect the terminal by asynchronous administration */
  memcpy (admin.dis_t, DIS, 11);
  memcpy (admin.off_t, OFF, 11);
  KDCS_FPUTNE (&admin,sizeof(struct adm_line),"KDCPTRMA",KDCS_SPACES,KCNODF)
;
  if (KCRCC != 0 )
    break;
      hacknr = 0;
  /* log on User logging */
}

```

```

KDCS_LPUT (&admin,sizeof(struct adm_line));
if (KCRCC != 0 )
    break;
    }
}
/* set up TLSB */
KDCS_PTDA (&hacknr,2,"TLSB",LTERM);
}
/* *****
/*                               End of while loop                               */
/******
if ( KCRCC != 10 || other_message)
/* other message or error in the while loop */
{
/* error line */
sprintf(spab->buffer, "Error in program unit - conversation %8.8s"\
    ", TAC: %8.8s because %4.4s. RC= %3.3s " ,
    ca->ca_head.kccv_tac , ca->ca_head.kcpr_tac ,
    pa.kcop , KDCS_ERR );
/* RSET-Operation */
KDCS_RSET();
/* LPUT-Operation: log on user logging */
KDCS_LPUT( spab->buffer , strlen( spab->buffer ) );
}
/* PEND FI-Operation */
KDCS_PENDFI();
}
/******
/*                               function set_lterm ()                               */
/******
void set_lterm ( struct work * spab )
{ if _K004
    { memcpy (LTERM,MSG.K004.LTRM, 8);
      return;
    }
if _K006
    { memcpy (LTERM, MSG.K006.LTRM, 8);
      return;
    }
if _K008
    { memcpy (LTERM, MSG.K008.LTRM, 8);
      return;
    }
if _K031
    { memcpy (LTERM, MSG.K031.LTRM, 8);
      return;
    }
if _K033
    { memcpy (LTERM, MSG.K033.LTRM, 8);
      return;
    }
}
/******
/*                               function set_pterm ()                               */
/******
void set_pterm ( struct work *spab )
{ if _K004
    { memcpy (admin.pterm, MSG.K004.PTRM, 8);
      memcpy (admin.pronam, MSG.K004.PRNM, 8);

```

```
        return;
    }
    if _K006
    { memcpy (admin.pterm, MSG.K006.PTRM, 8);
      memcpy (admin.pronam, MSG.K006.PRNM, 8);
      return;
    }
    if _K031
    { memcpy (admin.pterm, MSG.K031.PTRM, 8);
      memcpy (admin.pronam, MSG.K031.PRNM, 8);
      return;
    }
}
```

The above example for the MSGTAC event service simply indicates appropriate ways of evaluating messages and administering the application.

However, the K094 message (SIGNON SILENT-ALARM) should be used to monitor security infringements since this also includes UPIC and OSI TP clients. Furthermore, wider-ranging administration of the UTM application is possible using the programmed administration capability (ADMI interface).

10.2.5 Example of a complete UTM application on BS2000 systems

This application example for a UTM application on a BS2000 system administers address data that has been placed in a file. The application provides the following functions which are called by entering the corresponding TAC in the field used for this purpose. The input and output is performed in one format.

i On Unix, Linux and Windows systems, you can find an example for a UTM application in the sample application (Unix and Linux systems) and the QuickStartKit (Windows systems) which are provided with openUTM.

TAC	Function	Explanation
1	Read	outputs an address that is in the file. The search term used is the last name and the first two letters of the first name, both of which are to be specified in the appropriate fields.
2	Write	adds a new address to the file. There may not already be an address with the same search key (see above) in the file.
3	Update	modifies an address entry. The address must already exist in the file.
4	Delete	deletes an existing address from the file.

An error message appears in the lowest line of the format if used incorrectly.

The numbers listed above are the transaction codes (TACs) that control the application. Transaction code 1 calls the "TPREAD" program unit, and transaction codes 2, 3 and 4 call the "TPUPDATE" program unit. These program units then each branch to the "TPFILE" program unit. This program unit is utilized as the START and SHUT exits and contains the subroutines that perform the input/output operations on the address file.

The "BADTACS" program unit is automatically called by openUTM if an invalid TAC is specified.

The "ERRCHECK" function handles errors that arise in the program units.

After the connection to the application has been established and a successful KDCSIGN, the format is immediately output by openUTM (start format). The interaction with the user is then done in a strictly controlled dialog, i.e. the application reacts to the input of the TAC and of the key by outputting the format containing the address searched for or by outputting a success or error message in the bottom line.

i This program is only meant to demonstrate how you program using openUTM. The file accesses are not secured by the UTM transaction concept.

The following structure diagram presents the structure of the program units:

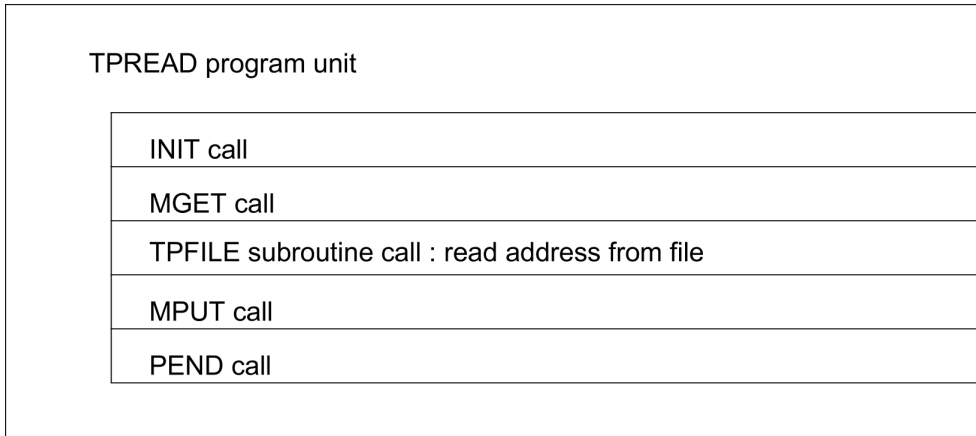


Figure: Structure diagram of the TPREAD program unit

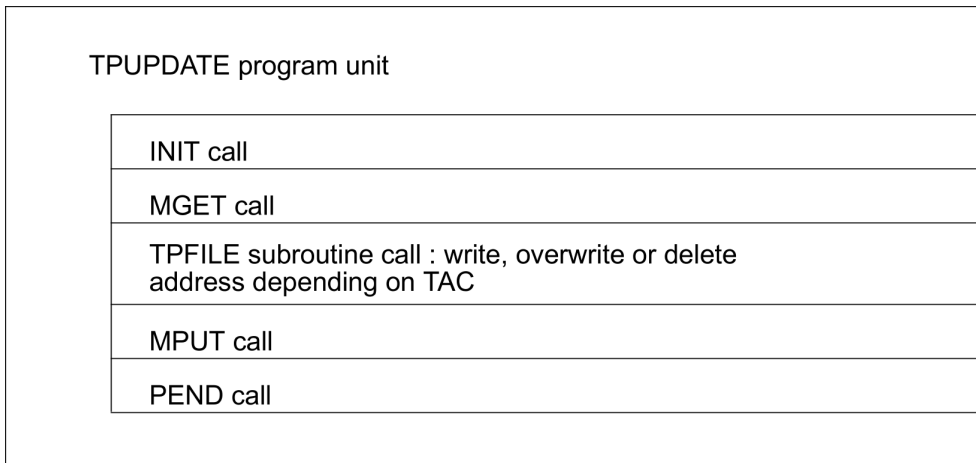


Figure: Structure diagram of the TPUPDATE program unit

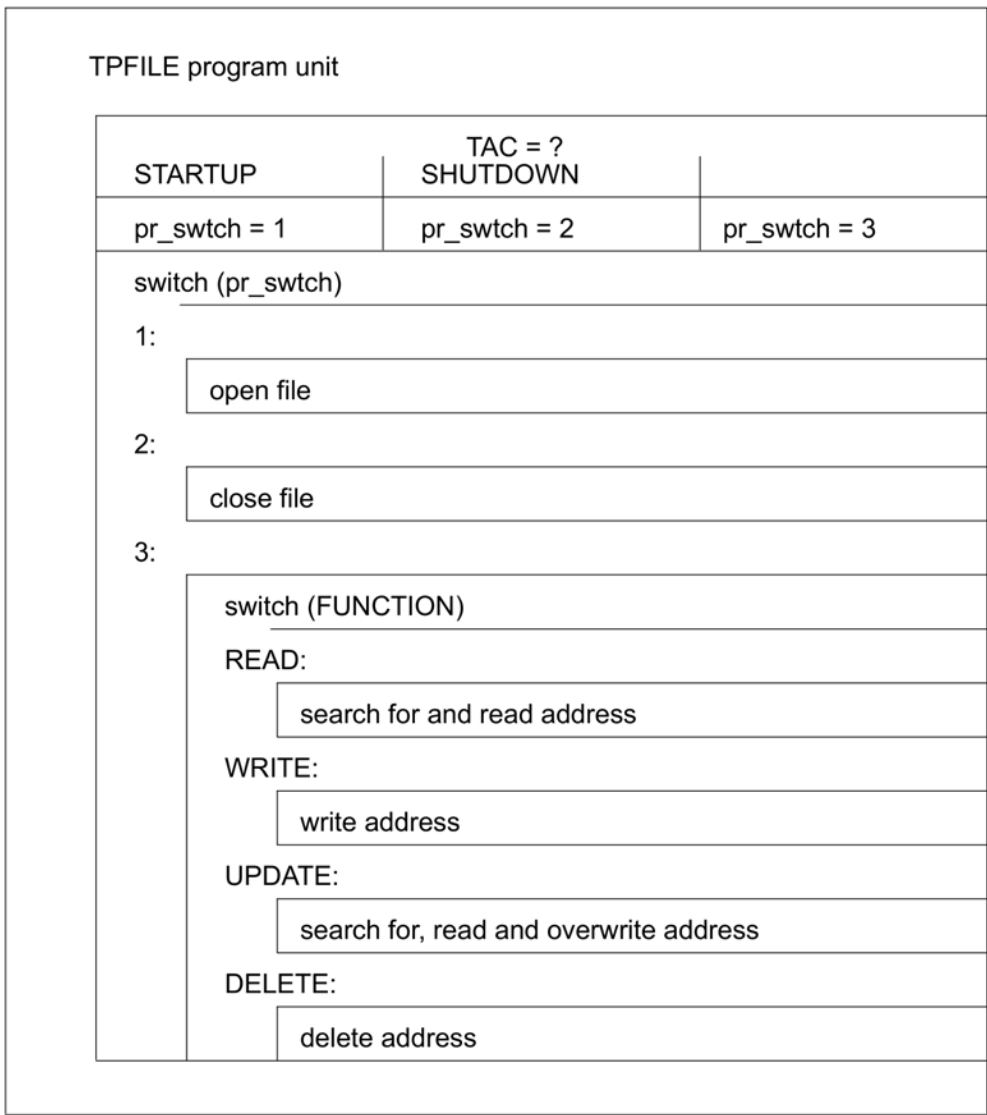


Figure: Structure diagram of the TPFILE program unit.

For the sake of completeness the generation of this application is listed at the end of the C program. Please consult the openUTM manual “Generating Applications” for the exact meaning of the individual operands and statements.

The following diagram shows the FORM1 format used for this application:

Format FORM1

```
*****
      A d d r e s s   A d m i n i s t r a t i o n
*****
      Select function:
-----
Actual function:
Name:                First Name:
Street:              No.:
Postal Code:         Residence:
Phone:
-----
                        Function selection
1 = Show address      |   4 = Delete address
2 = Enter address    |
3 = Update address   |           Finish with kdcoff
-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

The data structure for the address assistant for this format is printed in the following.

The FUNCTION field is a protected output field with the "automatic input" attribute. Numerical data is allowed to be entered in the POSTAL_CODE field and MSGTEXT is a protected output field. You can print out the entire list of attributes. You will find more information on this subject in your formatting system manual.

Header file FORM1.h

```
/* FORMAT NAME      : FORM1      */
/* USER AREA LENGTH :   235      */
typedef struct {
    char NAME          [ 14 ] ;
    char FIRST_NAME    [ 20 ] ;
    char STREET        [ 26 ] ;
    char NUMBER        [ 10 ] ;
    char POSTAL_CODE   [ 5 ] ;
    char RESIDENCE     [ 24 ] ;
    char PHONE        [ 21 ] ;
} ADDRESS;
typedef struct {
    char TAC           [ 8 ] ;
    char FUNCTION      [ 27 ] ;
    ADDRESS addr;
    char MSGTEXT       [ 80 ] ;
} FORM1 ;
```

Header file tp.h

```
#ifndef TP_H
#define TP_H
#include "FORM1.h"
#define kcrc ca->ca_return.kcrccc
#define pa spab->param
    struct ca_area
    { struct ca_hdr ca_head;
      struct ca_rti ca_return;
    };
    struct work
    { union kc_paa param;
      FORM1 std_mask; /* addressing assistant area */
      char progname[8];
    };
void BADTACS ( struct ca_area * , struct work * );
void errcheck ( struct ca_area * , struct work * );
void TPFILE ( struct ca_area * , struct work * );
void TPREAD ( struct ca_area * , struct work * );
void TPUPDATE ( struct ca_area * , struct work * );
#endif
```

Program unit TPREAD

```
#include <kcmac.h>
#include "tp.h"
void TPREAD (struct ca_area *ca , struct work *spab )
{
/* INIT-Operation */
  KDCS_SET (&spab->param, &ca->ca_head, &ca->ca_return);
  KDCS_INIT (0,sizeof(struct work));
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPREAD ", 8);
      errcheck (ca, spab);
    }
  else
    memcpy (spab->std_mask.TAC, ca->ca_head.kcpr_tac, 8);
/* MGET-Operation */
  KDCS_MGET ( spab->std_mask.FUNCTION
             ,sizeof( FORM1 )
             ,"*FORM1 "
             );
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPREAD", 8);
      errcheck (ca, spab);
    }
/* call function "tpfile" for reading address */
  TPFILE (ca, spab);
/* MPUT-Operation */
  KDCS_MPUTNT (&spab->std_mask,sizeof(FORM1)
              ,KDCS_SPACES,"*FORM1 ",KCNODF);
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPREAD", 8);
      errcheck (ca, spab);
    }
/* PEND FI-Operation */
  KDCS_PENDFI();
}
```

Program unit TPUPDATE

```
#include <kcmac.h>
#include "tp.h"
void TPUPDATE ( struct ca_area *ca , struct work *spab )
{
/* INIT-Operation */
  KDCS_SET (&spab->param, &ca->ca_head, &ca->ca_return);
  KDCS_INIT (0,sizeof(struct work));
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPUPDATE", 8);
      errcheck (ca, spab);
    }
  else
    memcpy (spab->std_mask.TAC, ca->ca_head.kcpr_tac, 8);
/* MGET-Operation */
  KDCS_MGET ( spab->std_mask.FUNCTION
             ,sizeof( FORM1 )
             ,"*FORM1 "
             );
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPUPDATE", 8);
      errcheck (ca, spab);
    }
/* call function "tpfile" for updating address */
  TPFILE (ca, spab);
/* MPUT-Operation */
  KDCS_MPUTNT (&spab->std_mask,
              sizeof(FORM1),KDCS_SPACES,"*FORM1 ",KCNODF);
  if (KCRCC != 0 )
    { memcpy (spab->progname, "TPUPDATE", 8);
      errcheck (ca, spab);
    }
/* PEND FI-Operation */
  KDCS_PENDFI();
}
```

Program unit BADTACS

```
#include <kcmac.h>
#include "tp.h"
#define ERRLINE "***** Wrong TAC - Please repeat \
Input *****"
void BADTACS (struct ca_area *ca, struct work *spab )
{
/* INIT-Operation */
KDCS_SET (&spab->param, &ca->ca_head, &ca->ca_return);
memset (&spab->std_mask.TAC,      , 8);
KDCS_INIT (0, sizeof(struct work));
if (KCRCC != 0 )
    { memcpy (spab->progname, "BADTACS", 8);
      errcheck (ca, spab);
    }
/* MGET-Operation */
KDCS_MGET ( spab->std_mask.FUNCTION
            , sizeof( FORM1 )
            , ca->ca_return.kcrfn
            );
if (KCRCC != 0 )
    { memcpy (spab->progname, "BADTACS", 8);
      errcheck (ca, spab);
    }
/* MPUT-Operation: Replace the standard error message */
memcpy (spab->std_mask.MSGTEXT, ERRLINE, 80);
memset (spab->std_mask.TAC,      , 8);
KDCS_MPUTNT ( &spab->std_mask
              , sizeof( FORM1 )
              , KDCS_SPACES
              , "FORM1 "
              , KCNODF
              );
if (KCRCC != 0 )
    { memcpy (spab->progname, "BADTACS", 8);
      errcheck (ca, spab);
    }
/* PEND FI call */
KDCS_PENDFI();
}
```

Function ERRCHECK

```
#include <kcmac.h>
#include "tp.h"
void errcheck ( struct ca_area * ca , struct work * spab )
{
    struct err_line
    {
        char ftext[35];
        char progname[8];
        char optext[10];
        char op_code[4];
        char cctext[8];
        char cc[3];
        char cdtext[8];
        char cd[4];
    } err_msg;
/* ----- Making connections for the KDCS... macros ----- */
    KDCS_SET (&spab->param, &ca->ca_head, &ca->ca_return);
/* making entries in the errorline */
    memcpy (err_msg.ftext, "***** E R R O R in program unit ",35);
    memcpy (err_msg.progname, spab->progname, 8);
    memcpy (err_msg.optext, " Op-Code: ",10);
    memcpy (err_msg.op_code, pa.kcop, 4);
    memcpy (err_msg.cctext, " kcrccc=", 8);
    memcpy (err_msg.cc, KDCS_ERR , 3);
    memcpy (err_msg.cdtext, " kcrcdc=", 8);
    memcpy (err_msg.cd, KDCS_RTI->kcrcdc, 4);
    memset (&spab->std_mask, , sizeof (FORM1));
    memcpy (spab->std_mask.MSGTEXT, &err_msg, 80);
/* MPUT-Operation */
    KDCS_MPUTNE (&spab->std_mask,sizeof(FORM1),KDCS_SPACES,"*FORM1 ",KCNODF);
/* PEND ER-Operation */
    KDCS_PENDER();
}
```

Program unit TPFILE with START/SHUT exits and file accesses

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <kcpa.h>
#include <kcca.h>
#include "tp.h"
#define M spab->std_mask
#define TAC ca->ca_head.kccv_tac
#define JOB TAC[0]
#define ADR_LENGTH ( (long) sizeof( ADDRESS ) )
#define READ 1
#define WRITE 2
#define UPDATE 3
#define DELETE 4
#ifdef __SNI_HOST_BS2000
    #define FILE_NAME "link=CAPPLI"
    #define FILE_MODE "r+b,type=record,forg=key"
    #define FILE_MODE_FIRST "w+b,type=record,forg=key"
#else
```

```

#define FILE_NAME "cappli.address"
#define FILE_MODE "r+b"
#define FILE_MODE_FIRST "w+b"
#endif
#define PREVIOUS_POSITION -ADR_LENGTH
#define SAG_NAME "FUJITSU TECHNOLOGY SOLUTIONS"
#define SAG_STREET "Musterstrasse"
#define SAG_NUMBER "6"
#define SAG_PCODE "12345"
#define SAG_RES "Musterstadt"
#define SAG_PHONE "+12 34 567-89"
typedef enum {
    FOUND = 1
    ,NOT_FOUND = 2
} address_status;
static address_status addr_fetch(struct work * );
static ADDRESS address;
static FILE * filepointer;
static fpos_t FilePosition;
void TPFFILE ( struct ca_area * ca , struct work *spab )
{
    int pr_swch;
#ifdef __SNI_HOST_BS2000
    char BS2Cmd[500];
#endif
    if (strncmp (TAC,"STARTUP ", 8) == 0)
        pr_swch = 1;
    else
        { if (strncmp (TAC,"SHUTDOWN", 8) == 0)
            pr_swch = 2;
            else
                { pr_swch = 3;
                    memset (M.MSGTEXT, * , 80);
                }
        }
    switch (pr_swch)
    { case 1:
#ifdef __SNI_HOST_BS2000
        sprintf( BS2Cmd ,
            "SET-FILE-LINK LINK-NAME = CAPPLI ,FILE-NAME = CAPPLI.ADDRESS"\
            " ,SUPPORT = *DISK( SHARED-UPDATE = *YES) " ,
            ADR_LENGTH );
        system( BS2Cmd );
#endif
    }
    if ((filepointer = fopen (FILE_NAME, FILE_MODE)) == NULL) {
        if((filepointer = fopen( FILE_NAME , FILE_MODE_FIRST )) == NULL ) {
            perror("fopen:");
            exit(-1);
        }
        memcpy( address.NAME , SAG_NAME , sizeof( SAG_NAME )-1);
        memcpy( address.STREET, SAG_STREET , sizeof( SAG_STREET )-1);
        memcpy( address.NUMBER, SAG_NUMBER , sizeof( SAG_NUMBER )-1);
        memcpy( address.POSTAL_CODE , SAG_PCODE , sizeof( SAG_PCODE )-1);
        memcpy( address.RESIDENCE , SAG_RES , sizeof( SAG_RES )-1);
        memcpy( address.PHONE , SAG_PHONE , sizeof( SAG_PHONE )-1);
        fwrite(&address, ADR_LENGTH, 1, filepointer);
        fclose( filepointer );
        if ((filepointer = fopen (FILE_NAME, FILE_MODE)) == NULL) {

```



```

        perror("fopen:");
        exit(-1);
    }
}
break;
case 2:
    fclose (filepointer);
    break;
case 3:
    switch (JOB)
    { case READ:
        memcpy (M.FUNCTION, "Show address          *****", 26);
        if (addr_fetch( spab ) == NOT_FOUND)
            { memcpy (M.MSGTEXT, "Address not found          ", 22);
              break;
            }
        else
            { memcpy (M.addr.NAME, address.NAME, ADR_LENGTH );
              break;
            }
        case WRITE:
            memcpy (M.FUNCTION, "Enter address          ***", 26);
            if (addr_fetch( spab ) == FOUND)
                { memcpy (M.MSGTEXT, "Address already exists ", 23);
                  break;
                }
            else
                { memcpy (address.NAME, M.addr.NAME, ADR_LENGTH );
                  fseek (filepointer, 0, 2);
                  fwrite (&address, ADR_LENGTH, 1, filepointer);
                  memcpy (M.MSGTEXT, "Address entered          ", 24);
                  break;
                }
        case UPDATE:
            memcpy (M.FUNCTION, "Update address          *****", 26);
            if (addr_fetch( spab ) == NOT_FOUND)
                { memcpy (M.MSGTEXT, "Address not found          ", 22);
                  break;
                }
            else
                { memcpy (address.NAME, M.addr.NAME, ADR_LENGTH );
                  fsetpos(filepointer,&FilePosition );
                  fwrite (&address, ADR_LENGTH, 1, filepointer);
                  memcpy (M.MSGTEXT, "Address changed ", 16);
                  break;
                }
        case DELETE:
            memcpy (M.FUNCTION, "Delete address          *****", 26);
            if (addr_fetch( spab ) == NOT_FOUND)
                { memcpy (M.MSGTEXT, "Address not found          ", 22);
                  break;
                }
            else
                {
#endif __SNI_HOST_BS2000
                memset (&address, * , ADR_LENGTH);
                fsetpos(filepointer,&FilePosition );
                fwrite (&address, ADR_LENGTH, 1, filepointer);
#ifdef __SNI_HOST_BS2000
            }
        }
    }
}
#endif

```

```

#else

```

```

        fdelrec(filepointer , NULL );
        memcpy (M.MSGTEXT, "Address deleted      ", 22);
        break;
#endif
    }
}
return;
}
/*****
/*          Function addr_fetch          */
*****/
static address_status addr_fetch( struct work *spab )
{
    address_status filestatus = NOT_FOUND;
    memset (&address, 0X00, ADR_LENGTH);
    fseek (filepointer, 0, 0);
    while ( fgetpos( filepointer , &FilePosition ) ,
            (fread (&address, ADR_LENGTH, 1, filepointer)) != NULL)
    {
        if (address.NAME[0] != * )          /* Address not deleted      */
        {
            if (strncmp (address.NAME, M.addr.NAME, sizeof M.addr.NAME) == 0)
                if (strncmp (address.FIRST_NAME
                            , M.addr.FIRST_NAME
                            , sizeof M.addr.FIRST_NAME) == 0)
                    { filestatus = FOUND;
                      break;
                    }
        }
        memset (&address, 0X00, ADR_LENGTH);
    }
    return filestatus;
}

```

KDCDEF statements

```

REM *****
REM ***          D E F  -  S T A T E M E N T S          ***
REM ***
REM ***          KDCFILE = CAPPLI          ***
REM *****
*
OPTION GEN=ALL
*
ROOT CAPPLI
*
*+-----+
* | MAX statements          |
*+-----+
*
MAX KDCFILE      = kdcfile
MAX APPLINAME    = CAPPLI
MAX APPLIMODE    = S
MAX TASKS        = 3
MAX ASYNTASKS    = 1
MAX PGPOOL       = (25)

```

```

MAX CACHESIZE      = (100,30)
MAX TRACEREC      = 10000
MAX RECBUF        = (5,4096)
MAX LPUTBUF       = 10
MAX LPUTLTH       = 4096
MAX TERMWAIT      = 60
MAX KB            = 1024
MAX NB            = 2048
MAX SPAB          = 4096
MAX CLRCH         = X FF
*
*+-----+
* | FORMSYS statement |
*+-----+
*
FORMSYS ...
*
*+-----+
* | MESSAGE statement |
*+-----+
*
MESSAGE MODULE=MSGS
*
*+-----+
* | PROGRAM statements |
*+-----+
*
*
*
OPTION DATA={ PROGRAM-STATIC | PROGRAM-SHARED-OBJ | PROGRAM-BLS | PROGRAM-OLD-DLL }
*
*
*+-----+
* | EXIT statements |
*+-----+
*
EXIT PROGRAM=TPFILE ,USAGE=START
EXIT PROGRAM=TPFILE ,USAGE=SHUT
*
*+-----+
* | TAC statements |
*+-----+
*
REM ***          ADMINISTRATION DIALOG          ***
TAC KDCTAC      ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCLTERM   ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCPTERM   ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCSWTCH   ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCSEND    ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCAPPL    ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCUSER    ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCDIAG    ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCLOG     ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCINF     ,PROGRAM=KDCADM , ADMIN=READ
TAC KDCHELP    ,PROGRAM=KDCADM , ADMIN=READ
TAC KDCSHUT    ,PROGRAM=KDCADM , ADMIN=Y
TAC KDCTCL     ,PROGRAM=KDCADM , ADMIN=Y

```

```

*
REM ***      ADMINISTRATION  ASYNCHRON      ***
TAC KDCTACA  ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCLTRMA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCPTRMA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCSWCHA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCUSERA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCSEDA  ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCAPPLA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCDIAGA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCLOGA  ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCINF A ,PROGRAM=KDCADM ,TYPE=A , ADMIN=READ
TAC KDCHELPA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=READ
TAC KDCSHUTA ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
TAC KDCTCLA  ,PROGRAM=KDCADM ,TYPE=A , ADMIN=Y
*
REM ***      Application specific TACs      ***
*
TAC KDCMSGTC , PROGRAM=NOHACK
TAC KDCBADTC , PROGRAM=BADTACS
TAC 1        , PROGRAM=TPREAD           , LOCK = 1
TAC 2        , PROGRAM=TPUPDATE , TACCLASS=1 , LOCK = 2
TAC 3        , PROGRAM=TPUPDATE , TACCLASS=1 , LOCK = 2
TAC 4        , PROGRAM=TPUPDATE , TACCLASS=1 , LOCK = 2
*
*+-----+
* | TACCLASS statements |
*+-----+
*
TACCLASS 1,TASKS=1
*
*+-----+
* | USER statements |
*+-----+
*
USER NINA ,PASS=C SOLO ,FORMAT=*FORM1 ,KSET=BUNDLE1 (1)
USER URSUS ,FORMAT=*FORM1 ,KSET=BUNDLE2 (1)
USER ADMIN ,PASS=C ADM ,KSET=MASTER,PERMIT=ADMIN
*
*+-----+
* | TLS statements |
*+-----+
*
TLS      TL5B
*
*+-----+
* | TPOOL statements |
*+-----+
*
TPOOL LTERM=... , NUMBER=2 , PRONAM=*ANY, PTYPE=... , KSET = MASTER
TPOOL LTERM=... , NUMBER=2 , PRONAM=*ANY, PTYPE=... , KSET = MASTER
*
*+-----+
* | PTERM / LTERM statements |
*+-----+
*
OPTION DATA=TERM
*
*+-----+

```

```

*| KSET statements |
*+-----+
*
KSET BUNDLE1 , KEYS=(1,2)
KSET BUNDLE2 , KEYS=(1)
KSET MASTER , KEYS=MASTER

```

(1) BS2000 format

Input files for the generation procedure

PROGRAM statements:

PROGRAM-STATIC (for static linking)

```

PROGRAM KDCADM , COMP=C
PROGRAM TPREAD , COMP=C
PROGRAM TPUPDATE , COMP=C
PROGRAM TPFILE , COMP=C
PROGRAM NOHACK , COMP=C
PROGRAM BADTACS , COMP=C

```

PROGRAM-BLS (for dynamic loading with BLS)

```

* -----+
DEFAULT PROGRAM COMP = C
PROGRAM KDCADM
* -----+
MPOOL LCPOOL , SIZE = 10 -
, SCOPE = GROUP -
, ACCESS = READ
* -----+
LOAD-MODULE LLMTPS , VERSION = 001 -
, LIB = DYNAMIC-LOADED-LIB -
, LOAD-MODE = ( POOL , LCPOOL , STARTUP )
* -----+
DEFAULT PROGRAM COMP = C , LOAD-MODULE = LLMTPS
PROGRAM BADTACS
PROGRAM TPUPDATE
PROGRAM TPREAD
PROGRAM TPFILE
PROGRAM NOHACK

```

PTERM/LTERM statement:

```
PTERM TERM05 ,PTYPE=T9750 ,LTERM=DST01 ,PRONAM=HOST0001
LTERM DST01
PTERM TERM10 ,PTYPE=T9750 ,LTERM=DST02 ,PRONAM=HOST0001
LTERM DST02
PTERM TERM11 ,PTYPE=T9763 ,LTERM=DST03 ,PRONAM=HOST0001
LTERM DST03
PTERM TERM12 ,PTYPE=T9763 ,LTERM=DSTADMIN ,PRONAM=HOST0001
LTERM DSTADMIN
PTERM D17 ,PTYPE=T9001 ,LTERM=PRINTER1 ,PRONAM=HOST0001
LTERM PRINTER1 , USAGE = 0
```

11 Additional information for COBOL

In addition to the general information in chapters chapters "Structure and use of UTM programs" to "Event functions" , this chapter provides you with programming language-specific information which you will need in order to write COBOL program units:

The first section deals with how COBOL program units are structured. The second contains sample programs. The third lists the data structures KCBC and KCPAC.

11.1 Structure of COBOL program units

This section tells you:

- how to write a UTM COBOL program unit as a subroutine
- what you need to know when developing a LINKAGE SECTION and the WORKING-STORAGE SECTION
- how the PROCEDURE DIVISION has to look and how a KDCS call needs to be programmed in COBOL
- which platform-specific features you need to be aware of (dependencies on specific compilers, formatting systems etc.).

11.1.1 COBOL program units as subroutines

UTM program units and event exits are subroutines of the UTM main routine. This fact leads to the following consequences:

- The program name defines the start address.
- At least one data structure must be defined in the LINKAGE SECTION.
- The program unit is terminated dynamically with the PEND call. Event exits that are exited with the statement EXIT PROGRAM are the exception. The statement STOP RUN is not permitted (exceptions: the START and SHUT event exits).

A series of COPY members are available to ensure compatibility and to enable you to work with error-free data structures. The section “Data structures for COBOL program units” on ["Data structures for COBOL program units"](#) describes how to use these COPY elements.

PROGRAM-ID as a start name

You define the start name for the program unit in the PROGRAM-ID paragraph. This name is freely definable, but must be unique within a given application program. There must be no naming conflicts between the program name and the runtime systems, the database systems, the formatting system, the communication components and openUTM.

When choosing names, it is therefore important to bear in mind the following points:

- For BS2000 systems:
 - All names that begin with KDC, KC or I are reserved.
- For Unix, Linux and Windows systems:
 - All names that begin with KDC, KC, x or ITS are reserved.
 - Names that begin with t_ are reserved for CMX and PCMX.
 - Names that begin with a_, o_ or s_ are reserved for OSS.
- The names you define must comply with COBOL conventions.

You must also specify the program names (start names) when generating the UTM application - each of them must be named in the KDCDEF application PROGRAM (see the openUTM manual “Generating Applications”).

i Please note what the COBOL compiler manual has to say about how program names are to be handled in the IDENTIFICATION DIVISION and in the CALL call.

WORKING-STORAGE SECTION

The WORKING-STORAGE SECTION is used primarily for constant data.

To ensure that program units remain compatibility and to make them easier to read, a series of constants with predefined KDCS names is provided in the form of COPY members.

It is a good idea only to store fields with fixed values in the WORKING-STORAGE SECTION. If you also want to store areas which contain variable data in the WORKING-STORAGE SECTION, you can also define the KDCS parameter area and the message area. However, since it is useful to accommodate them in the SPAB in the interests of saving storage space, these areas are described in the following section.

LINKAGE SECTION

You can use the LINKAGE SECTION for passing parameters and as a working area.

In the LINKAGE SECTION, each program unit must have a data structure with the level number 01 which describes the KDCS communication area.

This can be followed by a further data structure with the level number 01. This data structure describes the standard primary working area (SPAB). You can accommodate the KDCS parameter area and the message areas in the SPAB.

The data structures in the KB and in the KDCS parameter area are available as COPY members (KCKBC and KCPAC).

You will need to define the message areas yourself. However, specific data structures are provided in COPY members for calls which request information from openUTM (e.g. INFO, INIT PU). If you are working with a formatting system, you will be able to use automatically generated addressing aids to structure the message area (see the formatting system manual).

Example

```
LINKAGE SECTION.  
  COPY KCKBC.                1)  
  05 KB-ANY                   PIC X(22).  2)  
  05 KB-STARTLOC              PIC X(2).   2)  
  05 KB-DESTLOC               PIC X(2).   2)  
  05 KB-FLGTAG                PIC X(5).   2)  
  05 KB-FLGNO1                PIC X(5).   2)  
  05 KB-FLGNO2                PIC X(5).   2)  
  COPY KCPAC.                3)  
  03 NB.                      4)  
  COPY IFORMA3.              4)
```

- 1) KDCS communication area
- 2) User-specific declaration of the KB program area
- 3) SPAB with KDCS parameter area
- 4) Message area: the COPY statement fetches the input addressing aid for the format "FORMA3".

Extending the LINKAGE SECTION

In addition to the communication area and the SPAB, you can also accommodate still other areas in the LINKAGE SECTION which can then be used as common data areas within a UTM application.

You can declare these areas with the KDCDEF statement AREA. For more information, refer to the openUTM manual "Generating Applications".

In COBOL program units you can use AREAs as follows:

- In the LINKAGE SECTION you define these areas with the level number 01.
- In the PROCEDURE DIVISION you specify these areas under USING.

The order in which these areas are defined with the AREA statement is also important. If the area defined in *n*th position is required, you will need to specify all areas up until this one both in the LINKAGE SECTION and in the PROCEDURE DIVISION in the case of USING.

This function is not reflected in DIN standard 66 265.

Example 1

The areas AREA1, AREA2 and AREA3 were defined in this order using the AREA statement. AREA3 is required in a program unit. All areas are defined with the length 2000.

```
.  
.   
LINKAGE SECTION.  
  COPY KCKBC.  
.  
.  
  COPY KCPAC.  
.  
.  
.  
01 AREA1  PIC X(2000).  
01 AREA2  PIC X(2000).  
01 AREA3  PIC X(2000).  
.  
.  
PROCEDURE DIVISION USING KCKBC, KCSPAB, AREA1, AREA2, AREA3.  
.  
.
```

Example 2. Program unit in COBOL (on Unix, Linux and Windows systems)

In the following, two areas are generated, defined in a C source (see ["Other data areas \(AREAs\)"](#)) and passed to a program unit. The following are defined:

- the area *area* for direct access (i.e. the data area is passed to the program unit directly)
- the area *areaind* for indirect access

```
IDENTIFICATION DIVISION.  
PROGRAM-ID. COBAREA.  
ENVIRONMENT DIVISION.  
DATA DIVISION.  
WORKING-STORAGE SECTION.  
LINKAGE SECTION.  
  COPY KCKBC.  
  05 PROG PIC X.  
  COPY KCPAC.  
  03 NB PIC X(4000).  
01 AREA1 PIC X(20).  
01 AREA2 PIC X(30).  
PROCEDURE DIVISION USING KCKBC KCSPAB AREA1 AREA2.  
  MOVE AREA1 TO BUFFER.  
  MOVE AREA2 TO BUFFER1.  
  PERFORM INIT-OP.  
.  
.  
.
```

Alternatives to AREAs

If program units which use AREAs are to be copied from one application to another, problems may arise when using AREAs owing to possible differences in the parameter lists. For this reason, AREAs in the local part of an application program should be replaced by data declarations with the EXTERNAL clause. In this case, you do not have to program the AREA declaration in KDCDEF or the AREA data declaration in the LINKAGE SECTION and in the PROCEDURE DIVISION; a data declaration is required in the WORKING-STORAGESECTION with an EXTERNAL clause.

Example

Rather than define:

```
LINKAGE SECTION.  
.  
.  
01 AREA1.  
    02 DATA-ID PIC X(8).  
    02 DATA-EX PIC X(4000).
```

it would be better to define:

```
WORKING-STORAGE SECTION.  
01 COMMON1 IS EXTERNAL.  
    02 DATA-ID PIC X(8).  
    02 DATA-EX PIC X(4000).
```

In this example, the COMMON area COMMON1 is defined in such a way that can be loaded as shareable. It can be defined as follows:

For BS2000 systems, for example, in assembly language

```
COMMON1 CSECT PUBLIC  
COMMON1 RMODE ANY  
COMMON1 AMODE ANY  
*  
DATA_ID DC C'DATA-ID1'  
DATA_EX DS CL4000  
        END
```

If the COMMON area is to be loaded locally in the process, then you do not need to specify the PUBLIC attribute.

For Unix, Linux and Windows systems in C

```
struct COMMON1 {  
char DATA_ID [8] = "DATA-ID1";  
char DATA_EX [4000];  
}
```

11.1.2 Data structures for COBOL program units

To help you structure your data areas, openUTM is supplied with the following COPY members containing predefined data structures:

On BS2000 systems the data structures are present in the library SYSLIB.UTM.070.COB.

On Unix, Linux and Windows systems the data structures are present in the directory *copy-cobol85* or *netcobol* in the UTM directory *utmpath*.

Name	Contents and meaning
KCAPROC	Optional second parameter area for the APRO call: This area allows you to select OSI TP function combinations and the security type.
KCATC	KDCS attribute functions (only on BS2000 systems): Where +formats are used, you can use the symbolic names for attribute functions to modify the attribute fields for formats.
KCCFC	Only on BS2000 systems: Defines the second parameter passed by openUTM for the event exit INPUT. In this parameter openUTM passes the contents of the control fields in screen formats to the program unit. For this reason, this second parameter is also referred to as the control fields area.
KCDADC	Data structure for the DADM call: You should place this data structure over the message area for the KDCS call DADM RQ.
KCDFC	KDCS screen functions: You can use this symbolic name to influence the screen output by entering the name of the function you want in the KCDF field in the KDCS parameter area.
KCINFC	Data structure for the INFO call: You should place this data structure over the message area for the KDCS call INFO DT/SI/PC.
KCINIC	Defines a second parameter area for the INIT call (only necessary for INIT PU) and optional for the PGWT call (if KCLI > 0). UTM returns the requested information in this parameter area.
KCINPC	Data structure for the INPUT exit: This data structure contains the input and output parameters for the INPUT exit.
KCKBC	Data structure for the KDCS communication area. It contains: <ul style="list-style-type: none">• current service and program data• data returned to UTM after a call• (if required) the KB program area for passing data between programs within a service. You will also need to define the fields in the KB program area.
KCMMSGC	Data structure for the UTM messages: You will need this data structure if you have to handle UTM messages in a MSGTAC routine or if you want to use a program you have written to analyze the SYSLOG file.

Name	Contents and meaning
KCOPC	KDCS operation codes: This data structure contains symbolic names for the KDCS operations. For your KDCS calls you can enter a name in the KCOP field in the KDCS parameter area. Please note that the symbolic name for the SIGN call is SGN.
KCPAC	Data structure for the KDCS parameter area: This area accepts the parameters for a KDCS call.
KCPADC	Data structure for the PADM call: You should place this data structure over the message area for the KDCS call PADM AI/PI.
KCSGSTC	Data structure for the SIGN call: You should place this data structure over the message area for the KDCS call SIGN ST with KCLA > 0.

The data structures KCOPC, KCATC and KCDFC define constants. You should therefore copy these area to the WORKING-STORAGE SECTION.

Copy the remaining data structures to the LINKAGE SECTION.

The data structures will be copied to the program unit as illustrated in the example below.

```

Example
DATA DIVISION.
*****
WORKING-STORAGE SECTION.
    COPY KCOPC.
    COPY KCATC.    *** (only on BS2000 systems)
    COPY KCDFC.
*****
LINKAGE SECTION.
    COPY KCKBC.
        05  KBPRG          PIC X(80).
    COPY KCPAC.
    COPY KCINFC.
        05  FILLER          PIC X(50).
        03  NB REDEFINES KCINFC.
*****
PROCEDURE DIVISION USING KCKBC, KCSPAB.
.
.
.

```

Command section in a COBOL program unit

The command section of a COBOL program unit is freely definable. There are merely a few transaction processing rules, as described in chapter "[Structure and use of UTM programs](#)", which you need to note:

- program units are subroutines of the UTM main routine KDCROOT
- program units have to be reentrant

-
- dialog program units must strictly adhere to the rules governing dialogs.

Event exits are subject to special rules which are described in chapter "[KDCS calls in COBOL program units](#)".

Passing addresses

The PROCEDURE DIVISION in a COBOL program unit begins with the following statement:

```
PROCEDURE DIVISION USING kckbc[, spab[, param1 [, ... paramn ]]]
```

kckbc	is the name of the KDCS communication area which must be defined with the level number 01 in the LINKAGE SECTION. Where the COPY member KCKBC is used, the name is KCKBC.
spab	is the name of the standard primary working area defined with the level number 01 in the LINKAGE SECTION. Where the COPY member KCPAC is used, the name is KCSPAB. If an area from the WORKING-STORAGE SECTION was used in place of the SPAB, this specification is omitted.
param ₁ ... param _n	are the names of further objects defined in the LINKAGE SECTION; see heading "Extending the LINKAGE SECTION" in section " COBOL program units as subroutines ". These objects can, for example, be AREAs which serve as an extension of the SPAB. If no such objects are used, this specification is omitted.

11.1.3 KDCS calls in COBOL program units

Before you call a UTM function in a program, the KDCS parameter area must already have been supplied with all the necessary parameters.

These parameters include:

- the operation code for the call
- additional parameters determined by the operation code (see chapter “KDCS calls”).

In some KDCS calls, unused parameter fields must be supplied with `LOW-VALUE`. To avoid errors, you should always issue the command `MOVE LOW-VALUE TO KCPAC` before supplying values to the parameter fields.

Format of the KDCS call

Once all the necessary data areas have been supplied, the KDCS call can be issued. The start address for all operations is "KDCS".

The format of the CALL is as follows:

```
CALL "KDCS" USING parm1[, parm2].
```

parm1	is the data name of the KDCS parameter area. If the corresponding COPY member is used, the name is "KCPAC". This name must always be specified.
parm2	is the data name for the storage area in the program to which messages or data may need to be written or in which messages or data have been made available. In the present description, this area is generally referred to as "NB" (from the German acronym for message area). You can, however, choose any name you wish.

The data names can be labeled if necessary.

The extended format would then be:

```
parm1 [{IN|OF} dataname1}...], [parm2 [{IN|OF} dataname2}...]].
```

For more details, refer to the description of the COBOL compiler.

Example

A data structure which exists more than once as a substructure is to be used as a message area.

```
.  
. .  
  03 BOOK5 .  
    05 DATX          PIC X(50) .  
. .  
. .  
  03 BOOK8 .  
    05 DATX          PIC X(50) .  
. .  
..  
CALL "KDCS" USING KCPAC, DATX IN BOOK5.
```


Event exits

The event exits INPUT, START, SHUT and VORGANG must not contain KDCS calls. They must be written as subroutines and must be terminated with the statement EXIT PROGRAM.

In the case of START, SHUT and VORGANG, the addresses for the communication area (KB) and the standard primary working area (SPAB) are passed in the PROCEDURE DIVISION. Accordingly, the structures of these areas are defined in the LINKAGE

SECTION (as for the program units with KDCS calls). In chapter "[Programming examples in COBOL](#)" is given an example of a combined START/SHUT exit.

In the case of the INPUT exit, openUTM passes the address of the INPUT parameter area. The COPY member KCINPC is available to help you structure the INPUT parameter area; the name of the data structure is KCINPUTC.

On BS2000 systems, you can also pass the address of a control field area. The COPY member KCCFC is available for the control field area; the name of the structure is KCCFILDC.

For further information on event exits see chapter "[Event functions](#)".

Example: INPUT exit

```
DATA DIVISION.  
*****  
WORKING-STORAGE SECTION.  
.  
.  
*****  
LINKAGE SECTION.  
  COPY KCINPC.  
*****  
PROCEDURE DIVISION USING KCINPUTC [ ,KCCFILDC].  
.  
.
```

11.1.4 Programming user-specific error handling (Unix and Linux systems)

Additional functions are available on Unix and Linux systems, which go beyond the normal KDCS error handling:

- User signal routines

The two functions `KCX_REG_USER_SIGNAL_HANDLER` and `KCX_UN_REG_USER_SIGNAL_HANDLER` are available to you for registration and deregistration of the user signal routine. The user signal routine is called when a signal occurs and must be created by the user.

- Exchange of the utmwork process after PEND RE with `KCX_SET_RELOAD_FLAG`
- Creation of a UTM dump with `KCX_WRITE_DUMP`

11.1.4.1 User signal routines (Unix and Linux systems)

A user signal routine is registered in the program unit or in the Start-Exit with the function KCX_REG_USER_SIGNAL_HANDLER, i.e. user-specific signal handling is only activated once this is done.

KCX_UN_REG_USER_SIGNAL_HANDLER is used to deregister it and thus deactivate it.

Function KCX_REG_USER_SIGNAL_HANDLER

The function KCX_REG_USER_SIGNAL_HANDLER requires a function pointer that points to a user signal routine as an argument. In other words, the argument must be of the "PROCEDURE-POINTER" type and is automatically transferred using a reference, i.e. as the address of this pointer.

Note

For using these functions, your COBOL Compiler version must support the COBOL data type "PROCEDURE-POINTER".

Micro Focus Visual Cobol 2.2 or higher supports this data type, for example.

Example

```
WORKING-STORAGE section.  
01 install-address-4-sig usage procedure-pointer.  
PROCEDURE DIVISION USING KCKBC KCSPAB.  
    set install-address-4-sig to entry "MFCBLOOP-SIGNAL".  
    CALL "KCX_REG_USER_SIGNAL_HANDLER" USING install-address-4-sig.
```

Function KCX_UN_REG_USER_SIGNAL_HANDLER

Calling KCX_UN_REG_USER_SIGNAL_HANDLER from the application program deregisters, i.e. deactivates, the current user signal routine in openUTM. From this point onwards, the default openUTM error handling is activated.

The function is called without parameters.

Programming the signal routine

The user signal routine is always assigned three arguments:

Param-1

The system signal number as a binary variable 4 bytes in length, i.e. data type "PIC 9(9) COMP-5" .

Param-2

"Printable" explanation of the system signal number, e.g. "Segmentation fault" for signal 11, maximum 255 bytes long and ending with a null byte.

Param-3

Stack information, multi-line and maximum 4096 bytes long, ending with a null byte.

The user signal routine should only initiate "clear-up actions" and terminate the program with PEND RE:

- KDCS call RSET
- KDCS call MPUT NE with error info from the user signal routine parameters

- KDCS call PEND RE with KCRN="Follow-up TAC"

Notes

- The function may not be exited using "GOBACK" or "EXIT PROGRAM".
- When calling the user signal routine in COBOL, it is possible that the MICRO Focus COBOL runtime system will detect a recursion and reject the call.

If this happens, the suffix "IS RECURSIVE" must be added to the definition of the PROGRAM-ID in the user program unit, e.g.: PROGRAM-ID. MFCBLOOP IS RECURSIVE.

Example

```
WORKING-STORAGE section.
  01 signal-number-print pic 9(9).
LINKAGE SECTION.
  01 utm-stack-string pic x(4096).

  01 utm-signal-string pic x(255).
  01 utm-signal-number pic 9(9) COMP-5.
PROCEDURE DIVISION USING KCKBC KCSPAB.
  ENTRY 'MFCBLOOP-SIGNAL' USING utm-signal-number
  utm-signal-string
  utm-stack-string.
  MOVE utm-signal-number to signal-number-print.
  DISPLAY "UTM-SIGNAL-NUMBER IS "signal-number-print.
```

This is followed by the KDCS calls RSET, MPUT and PEND RE.

Example of parameters transferred to a user signal routine

```
utm-signal-number: 11
utm-signal-string: "Segmentation fault"
utm-stack-string:
#6 0x00007f712cf3103f in KCSSIGNAL () from /opt/lib/utm70a00/sys/libwork.so
#7 <signal handler called>
#8 0x00007f712e6aff30 in MFCBNULL () at MFCBNULL.c:17
#9 0x00007f712e27b418 in MFCBCALL_INIT-OP () at MFCBCALL.cbl:81
#10 0x00007f712e27b267 in MFCBCALL_INIT-OP () at MFCBCALL.cbl:59
#11 0x00007f712e27ae6a in MFCBCALL () from /home/user/filebase/utmcob.so
#12 0x00007f712e904b97 in KDCCOB2 () from /home/user/filebase/proot.so
#13 0x00007f712cf2f7e3 in KDCHLLC () from /opt/lib/utm70a00/libwork.so
#14 0x00007f712cf8e37c in START_TEILPROGRAM () from /opt/lib/utm70a00/sys/libwork.so
#15 0x00007f712cf83658 in KDCRTMM () from /opt/lib/utm70a00/sys/libwork.so
#16 0x00007f712cf91cc3 in KDCRTSI () from /opt/lib/utm70a00/libwork.so
#17 0x00007f712cf2f36c in KDCRTST () from /opt/lib/utm70a00/libwork.so
#18 0x00007f712e90487d in kcxmnt () from /home/user/filebase/proot.so
#19 0x000000000040207c in main ()
```

11.1.4.2 Exchanging the utmwork process (Unix and Linux systems)

The function `KCX_SET_RELOAD_FLAG` initiates exchange of a utmwork process after the KDCS call `PEND RE`.

We recommend always calling this function for Cobol runtime errors in the UTM application to eliminate the delayed effects of this error, i.e. to ensure the application is capable of running continuously.

Call

```
CALL KCX_SET_RELOAD_FLAG.
```

11.1.4.3 Creating a UTM dump (Unix and Linux systems)

The function `KCX_WRITE_DUMP` initiates creation of a UTM dump.

The function requires a pointer to a 6 byte long field containing the reason for the dump.

Example for the call

```
CALL KCX_WRITE_DUMP( "MYDMP1" ).
```

11.1.5 Platform-specific features on BS2000 systems

Notes on the DYNAMIC clause (COBOL85)

The DYNAMIC clause should not be used in load modules that are to be exchanged, because the working storage space allocated dynamically by this clause would not be released again when exchange takes place.

When exchanging load modules which make use of the dynamic allocation of working storage, memory overflow errors can occur.

Programming program units with COBOL2000

The lifetime of the objects is limited to one program unit run. At the PEND call, all objects created in a program unit run are therefore released by the runtime system. This also applies in the case of PEND variants without a change of process.

Object references therefore cannot be preserved after the end of a program unit run in order to be passed on to follow-up program units. In other words, they cannot be preserved in UTM storage areas either.

All LLMs that contain, use or inherit COBOL2000 modules with class definitions must always be replaced together with the modified class definition. In other words, if a class definition changes, all users of this class and the classes derived from it and their users must be replaced together with the modified class definition.

Compiling COBOL program units

COBOL program units can be compiled with COBOL85 or COBOL2000 (see the "COBOL85 User Guide" or "COBOL2000 User Guide").

You must specify the following COMOPT parameter TRUNCATE-LITERAL=NO when compiling a UTM program unit. The COMOPT parameter TRUNCATE-LITERAL=NO is no longer described for COBOL85 as of V1.2. In the interests of compatibility, COBOL85 nevertheless still supports it. When compiling a UTM program unit with COBOL85, it continues to be mandatory to specify TRUNCATE-LITERAL=NO.

COBOL85 then issues a message informing you that the parameter does not conform to the ANS85 standard; this does not, however, affect the compiler run.

When compiling with COBOL2000 you must specify the COMOPT parameter MARK-LAST-PARAMETER=YES.

Using shareable code

If you are intending to load COBOL program units and make them shareable, you must specify the following option when compiling them:

```
*COMOPT GENERATE-SHARED-CODE=YES
```

The shareable code does not necessarily have to be stored in a separate object module: it can also be stored together with the non-shareable part in a link and load module (LLM), which is subdivided into a public slice and a private slice. To do this you must specify the compiler option

```
COMOPTGEN-LLM=YES.
```

The shareable program units only need to be loaded once for all tasks in the application(s). In the memory used locally by the task, all you then have to do is load the non-shareable parts.

openUTM offers a variety of ways of loading shareable objects:

- as a non-privileged subsystem,

-
- in a common memory pool in the user storage area (class 6 memory).

For further information on how to compile shareable code, refer to the manual for your compiler. The openUTM manual "Using UTM Applications on BS2000 Systems" provides a detailed explanation of how to link and load shareable code.

Generating formats with IFG

The manual "IFG for FHS" offers in-depth information on how to generate formats using the IFG. If these formats are to be generated for use in conjunction with openUTM, please note the following points:

- The format name must not be more than 7 characters long.
- In the user profile you must select "Structure of the data transfer area"
 - for #formats: separate attribute blocks and field contents
 - for *formats: non-aligned, without attribute fields
 - for +formats: non-aligned, with attribute fields
- For * and + formats you declare two addressing aids, one each for input and output. You must also define a prefix for each addressing aid. The following example shows how addressing aids can be used:

```
LINKAGE SECTION.  
  COPY KCKBC.  
  05 KBPROGAREA PIC X(100).  
  COPY KCPAC.  
  03  NB-EINGABE.  
  COPY IFORMA-LIB.  
  03  NB-AUSGABE.  
  COPY OFORMA-LIB.
```

where FORMA is the format name defined with IFG, I is the prefix for input and O the prefix for output. When using this format, you specify the format name for MPUT, FPUT or DPUT calls in the field KCMF as "**FORMA" (for addressing aids without attribute fields) and as "+FORMA" (for addressing aids with attribute fields).

- When defining addressing aids, please note that, in the case of + and * formats, openUTM removes the transaction code from the message at the start of the service for MGETs and FGETs (unless an INPUT exit explicitly prevents it from doing so). If the first field in the format contains the transaction code, provision must be made for this in addressing aids for input formatting. The example below suggests one way of doing this for a *format or a +format:

```

LINKAGE SECTION.
.
COPY KCPAC.
03  NB.
   05  TACA                PIC X(002).          1)
   05  TAC                 PIC X(008).
   05  DATEN               PIC X(220).
03  FILLER REDEFINES NB.
COPY FORMA-LIB.
.
MOVE MGET TO KCOP.
.
IF KCKNZVG = "F"
THEN CALL "KDCS" USING KCPAC, DATEN          (Service start)
ELSE CALL "KDCS" USING KCPAC, NB            (During service)
END-IF.

```

1) This field is mandatory for +formats but must be omitted for *formats.

- When preparing to implement these addressing aids, the formats are to be stored in the formats library. This name should be specified in the FHS start parameters.

Extended line mode

The COPY element TIAMCTRC is available for work in extended line mode, but is not supplied with openUTM. This COPY member contains the data structure LINE-MODE-CONTROL-CHARACTERS with the symbolic names of the control characters. TIAMCTRC can be copied to the WORKING-STORAGE SECTION.

11.1.6 Platform-specific features on Unix and Linux systems

You can create COBOL programs either with the compilers from Micro Focus or with the Fujitsu NetCOBOL compiler.

This subsection describes the following compiler-specific characteristics:

- Generation
- Keywords
- Environment variables
- Compilation of COBOL program units

For details on linking applications and generating shared objects, see the manual openUTM manual “Using UTM Applications on Unix, Linux and Windows Systems”, subsection “Linking a UTM process on Unix and Linux systems”.

i All the programs in the **openUTM sample application** are suitable for use with the various COBOL compilers. The appropriate environment is set depending on the selected COBOL compiler.

Generation

At generation, you must specify the following KDCDEF statement for these programs:

- Micro Focus COBOL:

```
PROGRAM objectname, COMP=MFCOBOL [ ,SHARED-OBJECT=shared_object_name ]
```

- NetCOBOL:

```
PROGRAM objectname, COMP=NETCOBOL [ ,SHARED-OBJECT=shared_object_name ]
```

Keywords

Micro Focus COBOL and NetCOBOL

COBOL compilers include the keywords OBJECT-ID, RESTRICTED and USER. These keywords clash with names in the COPY elements of the UTM interfaces. There are two ways of preventing such conflicts.

- If the COBOL program units are not object-oriented, some compilers offer the possibility to specify the compiler options REMOVE(OBJECT-ID), REMOVE(RESTRICTED) and REMOVE(USER) at compilation.
- If the compiler does not provide the REMOVE functionality or if you want to preserve object-oriented functionality, you must modify the COPY statements as follows, for example:

```
COPY COPY-element REPLACING OBJECT-ID BY NEW-OBJECT-ID.  
COPY COPY-element REPLACING RESTRICTED BY NEW-RESTRICTED.  
COPY COPY-Element REPLACING USER BY NEW-USER.
```

The new names must be used when data access is performed.

NetCOBOL

Both the COBOL copies supplied by openUTM (KCAUSERC and KCAUSD2C) contain a structure field named PASSWORD.

Because PASSWORD is a reserved word in the NetCOBOL compiler, a REPLACING statement must be added when including these files in the COBOL source, e.g.

```
COPY KCAUSERC REPLACING PASSWORD BY PASSWORD-NC.
```

Reserved keywords when CPIC is used

In MicroFocus COBOL, TIMEOUT is a reserved word. However, since this word is contained in the COBOL copy CMCOBOL on account of the CPIC specification, this name must be replaced in the source. For example:

```
COPY CMCOBOL REPLACING TIMEOUT BY CPIC-TIMEOUT.
```

Environment variable

Micro Focus COBOL

Perform the following steps if you use COBOL program units with Micro Focus COBOL:

- > Call the script `<coboldir>/bin/cobsetenv`.
This script sets the required environment variables for the compiler.
- > Extend the COBCPY environment variable by adding `$UTMPATH/copy-cobol85`.
- > If you create programs based on CPIC, TX or XATMI under openUTM, extend the COBCPY environment variable as follows:
`$UTMPATH/<interface>/copy-cobol85`, where `<interface>` stands for `cpic`, `tx` or `xatmi`.
- > If you create client programs based on UPIC-L, extend the COBCPY environment variable by adding `$UTMPATH/upicl/copy-cobol85`.
- > Set the COBMODE environment variable:
 - To generate 32-bit objects, set it to 32.
 - To generate 64-bit objects, set it to 64.

NetCOBOL

Perform the following steps if you use NetCOBOL program units:

- > Call the script `<COBOLDIR>/config/cobol.sh`.
This script sets the required environment variables.
- > Extend the COBCOPY environment variable by adding `$UTMPATH/netcobol`.
- > Set the COB_LIBSUFFIX environment variable to `None,CPY,copy`.
- > If you create programs based on CPIC, TX or XATMI under openUTM, extend the COB_COBCOPY environment variable as follows:
`$UTMPATH/<interface>/netcobol`, where `<interface>` stands for `cpic`, `tx` or `xatmi`.
- > If you create client programs based on UPIC-L, extend the COB_COBCOPY environment variable by adding `$UTMPATH/upicl/netcobol`.

Compiling a COBOL program unit

Micro Focus COBOL

Micro Focus COBOL source programs are compiled with *cob*. You will need to set the following switches:

-c to create an .o file

-x for static linking

-g to retain the symbol table during linkage

NetCOBOL

NetCOBOL source programs are created with *cobol*. To do this, specify the following switches:

```
cobol -c WC'LIST,SOURCE,XREF,MESSAGE,COPY(FULL),SRF(VAR,FIX)' P'cobolprogramm.lst '  
cobolprogramm.cbl (to create a .o file)
```



For more details of creating UTM applications with COBOL programs, please refer to the openUTM manual “Using UTM Applications on Unix, Linux and Windows Systems”.

11.1.7 Platform-specific features on Windows systems

You can create COBOL programs with the compiler from Micro Focus.

This subsection describes the following compiler-specific characteristics:

- Generation
- Keywords
- Environment variables
- Compilation of COBOL program units
- Using the CPIC and XATMI COBOL interfaces

For details on linking applications, see the manual openUTM manual “Using UTM Applications on Unix, Linux and Windows Systems”, subsection “Linking a UTM process on Unix and Linux systems”.

i All the programs in the **openUTM Quickstart Kit** are suitable for use with the COBOL compiler.

Generation

At generation you must specify the following `kdcdef` statement for these programs:

```
PROGRAM objectname, COMP=MFCOBOL [ ,SHARED-OBJECT=shared_object_name]
```

Keywords

Micro Focus COBOL compiler include the keywords OBJECT-ID, RESTRICTED and USER. These keywords clash with names in the COPY elements of the UTM interfaces. There are two ways of preventing such conflicts.

- If the COBOL program units are not object-oriented, some compilers offer the possibility to specify the compiler options REMOVE(OBJECT-ID), REMOVE(RESTRICTED) and REMOVE(USER) at compilation.
- If the compiler does not provide the REMOVE functionality or if you want to preserve object-oriented functionality, you must modify the COPY statements as follows, for example:

```
COPY COPY-Element REPLACING OBJECT-ID BY NEW-OBJECT-ID.  
COPY COPY-Element REPLACING RESTRICTED BY NEW-RESTRICTED.  
COPY COPY-Element REPLACING USER BY NEW-USER.
```

The new names must be used when data access is performed.

Reserved keywords when CPIC is used

In Micro Focus COBOL, TIMEOUT is a reserved word. However, since this word is contained in the COBOL copy CMCOBOL on account of the CPIC specification, this name must be replaced in the source. For example:

```
COPY CMCOBOL REPLACING TIMEOUT BY CPIC-TIMEOUT.
```

Environment variable

Perform the following steps if you use Micro Focus COBOL program units:

- > For Visual Cobol: Call the command script `<visualcoboldir>\base\bin\CreateEnv.bat`.
- > Extend the COBCPY environment variable by adding the directory `%UTMPATH%\copy-cobol85`.

-
- > Extend the INCLUDE environment variable by adding `<path>\include`, where `<path>` is the installation directory of the COBOL compiler (required for the compilation of the root sources).
 - > If you create programs based on CPIC, TX or XATMI under openUTM, extend the COBCPY environment variable as follows:
`%UTMPATH%\<interface>\copy-cobol85`, where `<interface>` stands for `cpic`, `tx` or `xatmi`.
 - > If you create client programs based on UPIC-L, extend the COBCPY environment variable by adding `%UTMPATH%\upicl\copy-cobol85`.

Compiling a COBOL program unit

You compile programs by entering the command `cobol` in a prompt window.

If the program is to be animated, it must be compiled by means of the `cobol /ANIM` command.

Using the CPIC and XATMI COBOL interfaces

COBOL programs that use the CPIC or XATMI interfaces must be adapted for use with a MicroFocus compiler because of the Windows call conventions used.

- > Before the DATA DIVISION, the following `SPECIAL-NAMES` paragraph must be inserted to define the `WINAPI` call convention:

```
SPECIAL-NAMES .
```

```
CALL-CONVENTION 74 is WINAPI.
```

- > Each call of the CPIC or XATMI interface must comply with this convention. For example:

```
CALL WINAPI`CMACCP` USING CONVERSATION-ID CM_RETCODE
```

11.2 Programming examples in COBOL

This section provides you some simple examples of how to code a KDCS call and an example of a complete UTM application, including the KDCDEF generation.

11.2.1 Examples of individual KDCS calls

This section includes examples of code for the following KDCS calls:

- MGET
- MPUT
- DPUT
- MCOM with DPUT in a job complex
- APRO with MPUT for distributed processing

Since the other KDCS calls are coded in a similar manner, they are not all illustrated explicitly at this point in the manual.

In a KDCS call, KCPAC indicates the address of the KDCS parameter area and NB the address of the message area. It is assumed that you are using the COPY member KCOPC (constants for the operation codes).

MGET call

- An unformatted dialog message that is exactly 80 bytes long is to be received. If less than 80 characters are read, a prompt for re-entry of the message is to be issued.

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE MGET     TO KCOP.  
MOVE 80       TO KCLA.  
MOVE SPACES TO KCMF.  
CALL "KDCS" USING KCPAC, NB.  
  IF KCRCCC NOT = ZERO  
    THEN PERFORM MGET-RETURN-CODE.  1)  
  IF KCRLM NOT = KCLA  
    THEN PERFORM ITERATION.         2)
```

1) If more than 80 characters are read, error handling is activated.

2) The routine ITERATION sends a prompt to the terminal requesting that the entry be repeated.

- An ongoing service may receive input that consists of a short message generated with the function key F2 followed by 10 characters of data. This input is intended to trigger a special function. The F2 key was assigned the return code 21Z during generation.

```

...
MOVE LOW-VALUE TO KCPAC.
MOVE MGET TO KCOP.
.
CALL "KDCS" USING KCPAC, NB.
IF KCRCCC = "21Z"                1)
    THEN PERFORM MGET-2.
...
MGET-2.                          2)
MOVE LOW-VALUE TO KCPAC.
MOVE MGET TO KCOP.
MOVE 10 TO KCLA.
MOVE SPACES TO KCMF.
CALL "KDCS" USING KCPAC, NB.
IF KCRCCC NOT = ZERO
    THEN PERFORM MGET-RETURN-CODE.

```

- 1) A special function is called.
- 2) An additional MGET is needed for the 10 characters of data.

BS2000 systems

- The format "PIC15" has been requested by a terminal. The unprotected data is 500 characters long in various different format fields. This format is to be received by the program.

```

...
MOVE LOW-VALUE TO KCPAC.
MOVE MGET TO KCOP.
MOVE 500 TO KCLA.
MOVE "*PIC15 " TO KCMF.
CALL "KDCS" USING KCPAC, IPIC15.
IF KCRCCC = "05Z" GO TO FORMAT-ERROR.    1)
IF KCRCCC NOT = ZERO GO TO MGET-RETURN-CODE.
...

```

- 1) In the routine 'FORMAT-ERROR', the format has to be output again to enable you to continue working with the correct format.

MPUT call

- An 80-byte long unformatted message is to be sent to the terminal.

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE MPUT     TO KCOP.  
MOVE "NE"     TO KCOM.  
MOVE 80       TO KCLM.  
MOVE SPACES   TO KCRN.  
MOVE SPACES   TO KCMF.  
MOVE ZERO     TO KCDF.  
CALL "KDCS" USING KCPAC, NB.  
IF KCRCCC NOT = ZERO  
    THEN PERFORM MPUT-RETURN-CODE.
```

BS2000 systems

- A 500-byte long formatted message is to be sent to the terminal. The name of the format is "PIC15". The screen is to be deleted before the message is sent.

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE MPUT      TO KCOP.  
MOVE "NE"      TO KCOM.  
MOVE 500       TO KCLM.  
MOVE SPACES    TO KCRN.  
MOVE "*PIC15"  TO KCMF.  
MOVE KCREPL    TO KCDF.          1)  
CALL "KDCS" USING KCPAC, NB.  
IF KCRCCC NOT = ZERO  
    THEN PERFORM MPUT-RETURN-CODE.
```

¹⁾ REPLACE is executed by default whenever a format is replaced. The output is generated to preclude the possibility of errors resulting from undefined field contents.

- In a *format called "PIC10" which, according to the most recent terminal input, still exists, all unprotected fields are to be deleted by way of a response.

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE MPUT      TO KCOP.  
MOVE "NE"      TO KCOM.  
MOVE ZEROES    TO KCLM.  
MOVE SPACES    TO KCRN.  
MOVE "*PIC10"  TO KCMF.  
MOVE KCERAS    TO KCDF.  
CALL "KDCS" USING KCPAC, NB.  
IF KCRCCC NOT = ZERO  
    THEN PERFORM MPUT-RETURN-CODE.
```

DPUT call

- An asynchronous job with an 11-character long message is to be passed on November 11 (= the 315th day of the year) at 11.11 a.m. to a program unit (absolute time specification). The relevant TAC is "ALAAF".

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE DPUT      TO KCOP.  
MOVE "NE"      TO KCOM.  
MOVE 11        TO KCLM.  
MOVE "ALAAF"   TO KCRN.  
MOVE ZERO      TO KCDF.  
MOVE SPACES    TO KCMF.  
MOVE "A"       TO KCMOD.  
MOVE "315"     TO KCTAG.  
MOVE "11"      TO KCSTD.  
MOVE "11"      TO KCMIN.  
MOVE "00"      TO KCSEK.  
CALL "KDCS" USING KCPAC, NB.  
IF KCRCCC NOT = ZERO  
    THEN PERFORM DPUT-RETURN-CODE.
```

- An 80-character long message is to be output to the terminal 'DSS1' one hour from now (relative time specification), whereupon the screen function 'acoustic alarm' (BEL) is to be triggered.

```
...  
MOVE LOW-VALUE TO KCPAC.  
MOVE DPUT      TO KCOP.  
MOVE "NE"      TO KCOM.  
MOVE 80        TO KCLM.  
MOVE "DSS1"    TO KCRN.  
MOVE SPACES    TO KCMF.  
MOVE KCALARM   TO KCDF.  
MOVE "R"       TO KCMOD.  
MOVE "000"     TO KCTAG.  
MOVE "01"      TO KCSTD.  
MOVE "00"      TO KCMIN.  
MOVE "00"      TO KCSEK.  
CALL "KDCS" USING KCPAC, NB.  
IF KCRCCC NOT = ZERO  
    THEN PERFORM DPUT-RETURN-CODE.
```

Job complex: MCOM and DPUT calls

A formatted asynchronous message (of 200 bytes) is to be printed out at 6.00 p.m. (= 18.00 hours) on the same day on PRINTER2. The confirmation returned by the printer is to be handled by a program.

If positive confirmation is returned, an asynchronous program with the TAC PRINTPOS receives a confirmation job with a 20-byte long message. If negative confirmation is returned, an asynchronous program with the TAC PRINTNEG is started (without a message). 80 bytes of user information is also logged in the event of negative confirmation. This information can be read with DADM UI as soon as the confirmation job becomes the main job. Confirmation jobs cannot be addressed by means of a job ID.

The job complex is encapsulated within two MCOM calls, which determine the destinations for the print job (= the basic job) and confirmation jobs in the MCOM BC call; the complex ID is "*PRICOMP".

```
...
COMPLEX-BEGIN.
  MOVE LOW-VALUE  TO KCPAC.
  MOVE MCOM       TO KCOP.
  MOVE BC        TO KCOM.
  MOVE "PRINTER2" TO KCRN.
  MOVE "PRINTPOS" TO KCPOS.
  MOVE "PRINTNEG" TO KCNEG.
  MOVE "*PRICOMP" TO KCCOMID.
  CALL "KDCS" USING KCPAC.
  IF KCRCCC NOT = ZERO
    THEN PERFORM MCOM-RETURN-CODE.
DPUT-NE.
  MOVE DPUT      TO KCOP.
  MOVE "NE"      TO KCOM.
  MOVE 200      TO KCLM.
  MOVE "*PRICOMP" TO KCRN.
  MOVE "*FORM1"  TO KCMF. *** (only on BS2000 systems)
  MOVE ZERO     TO KCDF.
  MOVE "A"      TO KCMOD.
  MOVE KCTJHVG  TO KCTAG.
  MOVE "18"     TO KCSTD.
  MOVE "00"     TO KCMIN.
  MOVE "00"     TO KCSEK.
  CALL "KDCS" USING KCPAC, NB1.
  IF KCRCCC NOT = ZERO
    THEN PERFORM DPUT-RETURN-CODE.
DPUT-PLUS-T.
*****
* Confirmation job in positive case
*****
  MOVE LOW-VALUE  TO KCPAC.
  MOVE DPUT      TO KCOP.
  MOVE "+T"      TO KCOM.
  MOVE 20        TO KCLM.
  MOVE "*PRICOMP" TO KCRN.
  MOVE SPACES    TO KCMF.
  MOVE ZERO     TO KCDF.
  CALL "KDCS" USING KCPAC, NB2.
  IF KCRCCC NOT = ZERO
    THEN PERFORM DPUT-RETURN-CODE.
DPUT-USER-INFO.
*****
* User information for negative case
*****
  MOVE LOW-VALUE  TO KCPAC.
  MOVE DPUT      TO KCOP.
  MOVE "-I"      TO KCOM.
  MOVE 80        TO KCLM.
  MOVE "*PRICOMP" TO KCRN.
  MOVE SPACES    TO KCMF.
  MOVE ZERO     TO KCDF.
  CALL "KDCS" USING KCPAC, NB3.
```

```

        IF KCRCCC NOT = ZERO
            THEN PERFORM DPUT-RETURN-CODE.
    DPUT-MINUS-T.
    *****
    * Confirmation job in negative case
    *****
        MOVE LOW-VALUE   TO KCPAC.
        MOVE DPUT        TO KCOP.
        MOVE "-T"        TO KCOM.
        MOVE ZERO        TO KCLM.
        MOVE "*PRICOMP" TO KCRN.
        MOVE SPACES      TO KCMF.
        MOVE ZERO        TO KCDF.
        CALL "KDCS" USING KCPAC, NB4.
        IF KCRCCC NOT = ZERO
            THEN PERFORM DPUT-RETURN-CODE.
    COMPLEX-END.
        MOVE LOW-VALUE   TO KCPAC.
        MOVE MCOM        TO KCOP.
        MOVE EC          TO KCOM.
        MOVE "*PRICOMP" TO KCCOMID.
        CALL "KDCS" USING KCPAC.
        IF KCRCCC NOT = ZERO
            THEN PERFORM MCOM-RETURN-CODE.
    .
    .

```

Example of distributed processing: APRO call with a subsequent MPUT

The job-submitting service is to address the dialog service with the transaction code 'LTAC1' for the application 'PARTNER1' (double-step addressing). In this context, the jobreceiving service is to be assigned the service ID '>VGID1'. A 100-byte long MPUT message is then to be sent in line mode to the partner application.

```

    . . .
    MOVE LOW-VALUE   TO KCPAC.
    MOVE APRO        TO KCOP.
    MOVE "DM"        TO KCOM.
    MOVE ZERO        TO KCLM.
    MOVE "LTAC1"     TO KCRN.
    MOVE "PARTNER1" TO KCPA.
    MOVE ">VGID1"    TO KCPI.
    CALL "KDCS" USING KCPAC.
    IF KCRCCC NOT = ZERO
        THEN PERFORM APRO-RETURN-CODE.
    . . .
    MOVE LOW-VALUE   TO KCPAC.
    MOVE MPUT        TO KCOP.
    MOVE "NE"        TO KCOM.
    MOVE 100         TO KCLM.
    MOVE ">VGID1"    TO KCRN.
    MOVE SPACES      TO KCMF.
    MOVE ZEROES      TO KCDF.
    CALL "KDCS" USING KCPAC, NB.
    IF KCRCCC NOT = ZERO
        THEN PERFORM MPUT-RETURN-CODE.

```


11.2.2 Example of an INPUT exit (BS2000 systems)

The INPUT exit "FORINPUT" is called for input made in format mode and responds to such input as follows:

- User commands are issued:
 - Press the F1 key: KDCOUT
 - Press the F2 key: KDCDISP
 - KDCOFF: The first character in the input is "/"; this is accepted only outside of a service.
- Missing or invalid input elicits an error code with the message K098.

If the user is also to be permitted to enter KDCLAST and KDCFOR, the program will have to be extended accordingly.

This INPUT exit is generated with the KDCDEF generation tool in the EXIT statement with

KDCDEF statement

```
EXIT PROGRAM=FORINPUT,USAGE=( INPUT,FORMMODE)
```

Event exit INPUT

```
IDENTIFICATION DIVISION.
PROGRAM-ID.
    FORINPUT.
ENVIRONMENT DIVISION.
DATA DIVISION.
WORKING-STORAGE SECTION.
01 FUNC.
    05 FUNC2.
        10 COMMAND PIC X.
            88 KDCOFF VALUE "/".
        10 REST PIC X(7).
*
77 KDCDISP PIC 9(4) COMP VALUE 2.
*
77 KDCOUT PIC 9(4) COMP VALUE 1.
*
77 CV-END PIC X(2) VALUE "EC".
*
*****
LINKAGE SECTION.
COPY KCINPC.
*****
PROCEDURE DIVISION USING KCINPUTC.
*****
P1-KEY-CONTROL-SECTION.
*
                                Check F-keys *
IF KCIFKEY = KDCOUT
THEN
    MOVE "KDCOUT" TO KCINCMD
    MOVE "CD" TO KCICCD
    MOVE "N" TO KCICUT
    MOVE SPACES TO KCIERRCD
    GO TO P99-END.
```

```

IF KCIFKEY = KDCDISP
THEN
    MOVE "KDCDISP" TO KCINCMD
    MOVE "CD"      TO KCICCD
    MOVE "N"      TO KCICUT
    MOVE SPACES   TO KCIERRCD
    GO TO P99-END.
P2-CV-CONTROL.
IF KCICVST NOT = CV-END
THEN
    MOVE SPACES   TO KCINTAC
    MOVE "CC"     TO KCICCD
    MOVE "N"     TO KCICUT
    MOVE SPACES   TO KCIERRCD
    GO TO P99-END
ELSE
    PERFORM P10-FUNC-CONTROL
    GO TO P99-END.
*****
P10-FUNC-CONTROL.
*****
*                               Check the first character of input *
MOVE KCIFCH      TO FUNC2.
IF KDCOFF
THEN
    MOVE "KDCOFF" TO KCINCMD
    MOVE "CD"     TO KCICCD
    MOVE "N"     TO KCICUT
    MOVE SPACE    TO KCIERRCD
    GO TO P10-END.
IF KCICFINF NOT = "ON"
THEN
    MOVE SPACE    TO KCINTAC
    MOVE "ER"     TO KCICCD
    MOVE "N"     TO KCICUT
    MOVE "ER01"  TO KCIERRCD
    GO TO P10-END.
P10-END.
EXIT.
P99-END.
EXIT PROGRAM.

```


11.2.3 Example of an asynchronous MSGTAC program unit

The MSGTAC program unit NOHACK counts the number of incorrect sign-on attempts in TLS. If openUTM accepts a KDCSIGN (i.e. with the message K008 or K033), the TLS is deleted.

If, after three invalid KDCSIGN attempts, the fourth KDCSIGN attempt is also incorrect, the relevant terminal is to be disconnected by means of "asynchronous administration", using an FPUT call with KCRN="KDCPTRMA". The message area contains the following parameter of the administration command KDCPTRMA (see also the openUTM manual "Generating Applications"):

```
PTERM=pterm, PRONAM=processor,ACT=DIS
```

The administration command is then written with LPUT to the user log file and the TLS is deleted.

The K messages are each read with an FGET by the MSGTAC program unit. Once a K message has been "processed", an FGET immediately reads the next K message within the same program unit run.

```
IDENTIFICATION DIVISION.
PROGRAM-ID.
    MSGTAC.
ENVIRONMENT DIVISION.
DATA DIVISION.
WORKING-STORAGE SECTION.
    COPY KCOPC.
77  ID-HACK-TLS          PIC X(8) VALUE "TLSHACK".
77  HACK-MAX            PIC 9(4) COMP VALUE 3.
01  ADM-SATZ.
    02  ADM-TXT.
        03  F            PIC X(07) VALUE "PTERM=(" .
        03  F            PIC X(08) .
        03  F            PIC X(09) VALUE " ),PRONAM=" .
        03  F            PIC X(08) .
        03  F            PIC X(11) VALUE " ,ACTION=DIS" .
01  UTM-FEHLER-ZEILE.
    03  F                PIC X(18) VALUE "Error in prog. unit".
    03  F-MODUL          PIC X(08) VALUE "NOHACK".
    03  F                PIC X(12) VALUE "; Vorg./TAC".
    03  F-VG            PIC X(08) .
    03  F                PIC X(01) VALUE "/" .
    03  F-AL            PIC X(08) .
    03  F                PIC X(05) VALUE " wg." .
    03  F-OP            PIC X(04) .
    03  F                PIC X(07) VALUE " (RC:" .
    03  F-RC            PIC X(08) .
    03  F                PIC X(01) VALUE " )".
LINKAGE SECTION.
    COPY KCKBC.
    05  FILLER          PIC X.
    COPY KCPAC.
    COPY KCMSGC.
    03  NB.
        05  HACKER-LTERM PIC X(8) .
        05  NB-ADM.
            07  F        PIC X(07) .
            07  PTRM     PIC X(08) .
            07  F        PIC X(09) .
            07  PRNM     PIC X(08) .
            07  F        PIC X(11) .
```

```

05 TLS-HACK.
07 HACK-ANZ          PIC 9(4) COMP.
PROCEDURE DIVISION USING KCKBC, KCSPAB.
MAIN SECTION .
INIT-ANF.
  MOVE LOW-VALUE TO KCPAC
  MOVE INIT       TO KCOP
  MOVE 0          TO KCLKBPRG
  COMPUTE KCLPAB  = FUNCTION LENGTH (KCSPAB)
  CALL "KDCS" USING KCPAC.
  IF KCRCCC NOT = ZERO
  THEN GO TO PEND-LPUT.
FGET-ANF.
  MOVE LOW-VALUE TO KCPAC
  MOVE FGET      TO KCOP
  COMPUTE KCLA   = FUNCTION LENGTH (KCMMSGC)
  MOVE SPACE    TO KCMF
  CALL "KDCS" USING KCPAC, KCMMSGC
  IF KCRCCC NOT = ZERO
  THEN
    IF KCRCCC = "10Z"
    THEN
      GO TO PEND-ANF
    ELSE
      GO TO PEND-LPUT.
  IF MSGNR = "K004"
*                                     Invalid identification *
    MOVE LTRM OF K004 TO HACKER-LTERM
  ELSE IF MSGNR = "K006"
*                                     Invalid password *
    MOVE LTRM OF K006 TO HACKER-LTERM
  ELSE IF MSGNR = "K008"
*                                     KDCSIGN accepted *
    MOVE LTRM OF K008 TO HACKER-LTERM
  ELSE IF MSGNR = "K031"
*                                     Card not ok *
    MOVE LTRM OF K031 TO HACKER-LTERM
  ELSE IF MSGNR = "K033"
*                                     if no K008 is generated *
    MOVE LTRM OF K033 TO HACKER-LTERM

  ELSE
    MOVE MSGNR TO KCOP
    GO TO PEND-LPUT.
  PERFORM ARBEIT
  IF KCRCCC NOT = ZERO
  GO TO PEND-LPUT.
*                                     More messages waiting ?? *
  GO TO FGET-ANF.
PEND-ANF.
  MOVE LOW-VALUE TO KCPAC
  MOVE PEND      TO KCOP
  MOVE "FI"     TO KCOM
  CALL "KDCS" USING KCPAC.
PROG-ENDE.
  EXIT PROGRAM.
PEND-LPUT.
  MOVE KCOP          TO F-OP
  MOVE KCTACVG      TO F-VG

```

```

MOVE KCTACAL          TO F-AL
MOVE KCRC             TO F-RC
MOVE LOW-VALUE TO KCPAC
MOVE LPUT            TO KCOP
COMPUTE KCLA        = FUNCTION LENGTH (UTM-ERROR-LINE)
CALL "KDCS" USING KCPAC, UTM-ERROR-LINE.
MOVE LOW-VALUE TO KCPAC
MOVE PEND           TO KCOP
MOVE "FI"          TO KCOM
CALL "KDCS" USING KCPAC.

M9.
  EXIT.
/
ARBEIT SECTION .
A0.
  MOVE LOW-VALUE      TO KCPAC
  MOVE GTDA          TO KCOP
  MOVE 2              TO KCLA
  MOVE ID-HACK-TLS   TO KCRN
  MOVE HACKER-LTERM  TO KCLT
  CALL "KDCS" USING KCPAC, TLS-HACK
  IF KCRCCC NOT = ZERO
    GO TO A9.
  IF KCRLM = 0
    THEN
      IF MSGNR = "K008"
        OR = "K033"
      THEN
        *                               Ok, no TLS exists *
          NEXT SENTENCE
        ELSE
          *                               Create TLS *
            MOVE LOW-VALUE      TO KCPAC
            MOVE PTDA          TO KCOP
            MOVE 2              TO KCLA
            MOVE 1              TO HACK-NO
            MOVE ID-HACK-TLS   TO KCRN
            MOVE HACKER-LTERM  TO KCLT
            CALL "KDCS" USING KCPAC, TLS-HACK
          ELSE
            IF MSGNR = "K008"
              OR = "K033"
            THEN
              *                               Ok; delete TLS *
                MOVE LOW-VALUE      TO KCPAC
                MOVE PTDA          TO KCOP
                MOVE 0              TO KCLA
                MOVE ID-HACK-TLS   TO KCRN
                MOVE HACKER-LTERM  TO KCLT
                CALL "KDCS" USING KCPAC, TLS-HACK
              ELSE
                PERFORM CHECK-NO.
  A9.
    EXIT.
/
PRUEF-ANZ SECTION .
P0.
  ADD 1 TO HACK-NO
  IF HACK-NO NOT > HACK-MAX

```

```

THEN
*
                                Try it once more *
    MOVE LOW-VALUE      TO KCPAC
    MOVE PTDA           TO KCOP
    MOVE 2              TO KCLA
    MOVE ID-HACK-TLS   TO KCRN
    MOVE HACKER-LTERM  TO KCLT
    CALL "KDCS" USING KCPAC, TLS-HACK
    GO TO P9.
*
                                Disconnect !! *
    MOVE ADM-TXT TO NB-ADM
    IF MSGNR = "K004"
        MOVE CORR K004 TO NB-ADM
    ELSE IF MSGNR = "K006"
        MOVE CORR K006 TO NB-ADM
    ELSE
        MOVE CORR K031 TO NB-ADM.
P-FPUT.
    MOVE LOW-VALUE      TO KCPAC
    MOVE FPUT           TO KCOP
    MOVE "NE"           TO KCOM
    MOVE "KDCPTRMA"    TO KCRN
    COMPUTE KCLM        = FUNCTION LENGTH (NB-ADM)
    MOVE SPACE          TO KCMF
    MOVE ZERO           TO KCDF
    CALL "KDCS" USING KCPAC, NB-ADM
    IF KCRCCC NOT = ZERO
        GO TO P9.
P-LPUT.
*
                                Write to user log *
    MOVE LOW-VALUE TO KCPAC
    MOVE LPUT      TO KCOP
    COMPUTE KCLA   = FUNCTION LENGTH (NB-ADM)
    CALL "KDCS" USING KCPAC, NB-ADM
    IF KCRCCC NOT = ZERO
        GO TO P9.
P-PTDA.
*
                                Delete TLS *
    MOVE LOW-VALUE      TO KCPAC
    MOVE PTDA           TO KCOP
    MOVE ZERO           TO KCLA
    MOVE ID-HACK-TLS   TO KCRN
    MOVE HACKER-LTERM  TO KCLT
    CALL "KDCS" USING KCPAC, TLS-HACK.
P9.
EXIT.

```

The above example for the MSGTAC program unit simply indicates appropriate ways of evaluating messages and administering the application.

However, the K094 message (SIGNON SILENT-ALARM) should be used to monitor security infringements since this also includes UPIC and OSI TP clients. Furthermore, wider-ranging administration of the UTM application is possible using the programmed administration capability (ADMI interface).

11.2.4 Example of a complete UTM application on BS2000 systems

Example of address management

This sample application for a UTM application on a BS2000 system allows you to manage address data stored in a file. The application provides the following management functions for this purpose; each function can be called by means of an entry in the appropriate field in the relevant TAC. Input and output are both made in a format.

i On Unix, Linux and Windows systems, you can find an example for a UTM application in the sample application (Unix and Linux systems) and the QuickStartKit (Windows systems) which are provided with openUTM.

TAC	Function	Explanation
1	Display	displays one of the addresses in the file. The search string consists of the surname and the first two letters of the forename, which must be entered in the appropriate fields.
2	Add	enters a new address in the file. The file must not already contain an address with the same search string (see above).
3	Update	modifies an address entry. The address must already exist in the file.
4	Delete	deletes an existing address from the file.

If the user makes an error, an error message is displayed in the bottom line of the format.

The figures indicated above are the transaction codes (TACs) which control the application. Transaction code 1 calls the program unit DISPLAY; transaction codes 2, 3 and 4 all call the program unit UPDATE. These program units then branch to the program unit FILES.

The program unit FILES is implemented as the START and SHUT exit and contains the subroutines which implement input to and output from the address file.

openUTM calls the program unit BADTACS automatically if an invalid TAC is entered. Once the connection to the application has been established and KDCSIGN has been called successfully, openUTM immediately outputs the format (start format). Subsequent interaction with the user is strictly dialog-driven; in other words, the application responds to the input of a TAC and a key by outputting the format which contains the address being searched for and/or by outputting a success or an error message in the bottom line.

i This program is intended merely to show you how you can program with openUTM. The file accesses depicted here are not subject to UTM's transaction management concept.

The following structure diagrams show the structure of the program units:

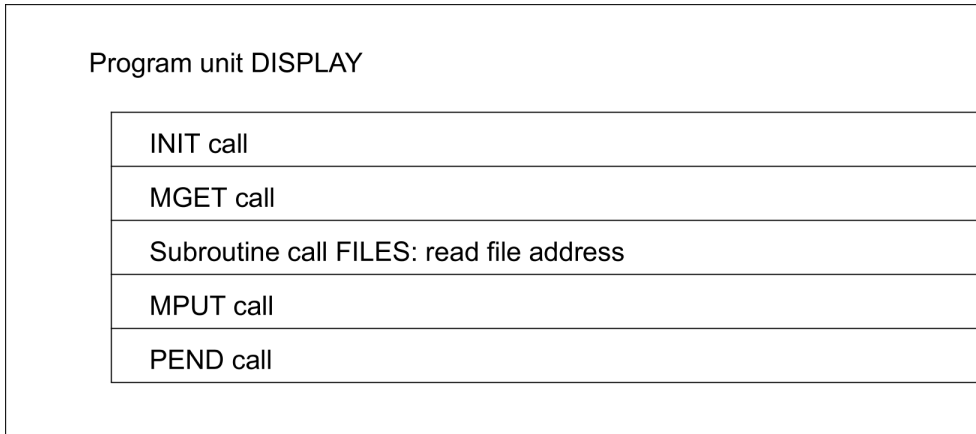


Figure: Structure diagram of program unit DISPLAY

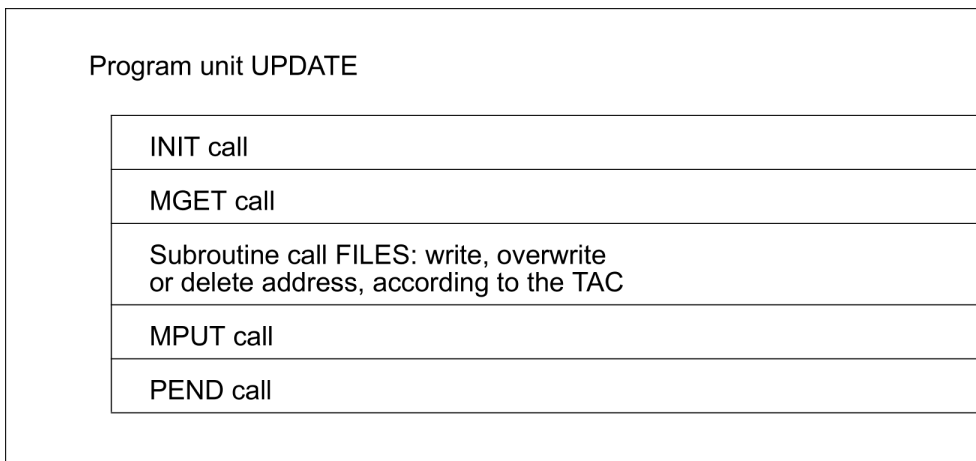


Figure: Structure diagram of program unit UPDATE

For the sake of completeness, the generation of the application has also been appended to the COBOL program listings. To find out the exact meanings of the individual operands and statements, please refer to the openUTM manual "Generating Applications".

The figure below shows the format used for this application:

```

*****
                A d d r e s s   M a n a g e m e n t
*****
Please select a function: .....

Current function: @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Last name:+++++                First name:++.....
Street:.....                No:.....
ZIP code:nnnnn                City:.....
Phone:.....

                                Function menu
1 = Display addresses          4 = Delete addresses
2 = Add new addresses         Quit with kdcoff
3 = Update addresses

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

```

Figure: The *format "FORMA" with which the application works

The structure of the addressing aid for this format is provided below:

```

*      USER-AREA-LEN: 228
41 TACO          PIC X(8).
41 FUNCTIONO    PIC X(26).
41 LASTNAMEO    PIC X(14).
41 FSTO         PIC X(2).
41 FSTRESTO     PIC X(18).
41 STREETO      PIC X(26).
41 HOUSENOO     PIC X(10).
41 ZIPO         PIC X(5).
41 CITYO        PIC X(26).
41 PHONEO       PIC X(18).
41 MSGTEXTO     PIC X(80).

```

The fields "FUNCTIONO" and "MSGTEXTO" are protected fields, the field "ZIPO" is numeric.

```

Program unit DISPLAY
IDENTIFICATION DIVISION.
PROGRAM-ID.      DISPLAY.
*****
ENVIRONMENT DIVISION.
*****
DATA DIVISION.
WORKING-STORAGE SECTION.
COPY KCOPC.
01 ERROR-TEXT.

```

```

05     FILLER          PIC X(21)
      VALUE "***  E R R O R  ***".
05     FILLER          PIC X(14)
      VALUE "PROGRAM UNIT: ".
05     F-TP           PIC X(08).
05     FILLER          PIC X(17)
      VALUE "    KDCS OPCODE: ".
05     F-OP           PIC X(04).
05     FILLER          PIC X(13)
      VALUE "RETURN CODE: ".
05     F-CD           PIC X(03).
LINKAGE SECTION.
COPY KCKBC.
05     KBPRG           PIC X(228).
COPY KCPAC.
03     NB.
      05     TAC           PIC X(008).
      05     DATA1       PIC X(220).
03     FILLER REDEFINES NB.
COPY FORMAO.
*****
PROCEDURE DIVISION USING KCKBC KCSPAB.
INIT-OPERATION-SECTION.
MOVE SPACES TO NB.
MOVE INIT TO KCOP.
MOVE 0 TO KCLKBPRG.
MOVE 512 TO KCLPAB.
CALL "KDCS" USING KCPAC.
IF KCRCCC NOT = ZERO
    THEN MOVE INIT TO F-OP GO TO ERROR-HANDLING.
MGET-OPERATION.
MOVE MGET TO KCOP.
MOVE 228 TO KCLA.
MOVE "*FORMA" TO KCMF.
CALL "KDCS" USING KCPAC DATA1.

IF KCRCCC NOT = ZERO
    THEN MOVE MGET TO F-OP GO TO ERROR-HANDLING.
* CALL PROGRAM UNIT "FILES" IN ORDER TO CALL *
* READ ROUTINE *
READ-OPERATION.
CALL "FILES" USING KCKBC, KCSPAB.
MPUT-OPERATION.
MOVE MPUT TO KCOP.
MOVE "NE" TO KCOM.
MOVE 228 TO KCLM.
MOVE SPACES TO KCRN.
MOVE "*FORMA" TO KCMF.
CALL "KDCS" USING KCPAC NB.
IF KCRCCC NOT = ZERO
    THEN MOVE MPUT TO F-OP GO TO ERROR-HANDLING.
PEND-OPERATION.
MOVE PEND TO KCOP.
MOVE "FI" TO KCOM.
CALL "KDCS" USING KCPAC NB.
PROG-END.
EXIT PROGRAM.
ERROR-HANDLING.
MOVE "DISPLAY" TO F-TP.

```



```

MOVE KCRCCC      TO F-CD.
MOVE ERROR-TEXT TO NB.
MOVE MPUT       TO KCOP.
MOVE "NE"      TO KCOM.
MOVE 80        TO KCLM.
MOVE SPACES    TO KCRN.
MOVE SPACES    TO KCMF.
MOVE ZEROES    TO KCDF.
CALL "KDCS"    USING KCPAC NB.
MOVE PEND      TO KCOP.
MOVE "ER"      TO KCOM.
CALL "KDCS"    USING KCPAC.
GO TO PROG-END.

```

Program unit UPDATE

```

IDENTIFICATION DIVISION.
PROGRAM-ID.      UPDATE.
*****
ENVIRONMENT DIVISION.
*****
DATA DIVISION.
WORKING-STORAGE SECTION.
COPY KCOPC.
01 ERROR-TEXT.
   05 FILLER          PIC X(21)
      VALUE "***  E R R O R  ***".
   05 FILLER          PIC X(14)
      VALUE "PROGRAM UNIT: ".
   05 F-TP           PIC X(08).
   05 FILLER          PIC X(17)
      VALUE "  KDCS OPCODE: ".
   05 F-OP           PIC X(04).
   05 FILLER          PIC X(13)
      VALUE "RETURN CODE: ".
   05 F-CD           PIC X(03).
LINKAGE SECTION.
COPY KCKBC.
   05 KBPRG           PIC X(228).
COPY KCPAC.
   03 NB.
      05 TAC          PIC X(008).
      05 DATA1       PIC X(220).
   03 FILLER REDEFINES NB.
COPY FORMAO.
*****
PROCEDURE DIVISION USING KCKBC, KCSPAB.
*****
INIT-OPERATION-SECTION.
MOVE SPACES TO NB.
MOVE INIT TO KCOP.
MOVE 0 TO KCLKBPRG.
MOVE 512 TO KCLPAB.
CALL "KDCS" USING KCPAC.
IF KCRCCC NOT = ZERO
    THEN MOVE INIT TO F-OP GO TO ERROR-HANDLING.
MGET-OPERATION.

```

```

MOVE MGET      TO KCOP.
MOVE 228       TO KCLA.
MOVE "*FORMA"  TO KCMF.

CALL "KDCS"    USING KCPAC DATA1.
IF KCRCCC NOT = ZERO
    THEN MOVE MGET TO F-OP GO TO ERROR-HANDLING.
* CALL PROGRAM UNIT "FILES" IN ORDER TO BRANCH TO *
* WRITING, OVERWRITING AND DELETING ROUTINES      *
* ACCORDING TO THE TAC                            *
FILE-OPERATION.
    CALL "FILES" USING KCKBC, KCSPAB.
MPUT-OPERATION.
    MOVE MPUT      TO KCOP.
    MOVE "NE"      TO KCOM.
    MOVE 228       TO KCLM.
    MOVE SPACES    TO KCRN.
    MOVE "*FORMA"  TO KCMF.
    CALL "KDCS"    USING KCPAC NB.
    IF KCRCCC NOT = ZERO
        THEN MOVE MPUT TO F-OP GO TO ERROR-HANDLING.
PEND-OPERATION.
    MOVE PEND      TO KCOP.
    MOVE "FI"      TO KCOM.
    CALL "KDCS"    USING KCPAC NB.
PROG-END.
    EXIT PROGRAM.
ERROR-HANDLING.
    MOVE "UPDATE"  TO F-TP.
    MOVE KCRCCC    TO F-CD.
    MOVE ERROR-TEXT TO NB.
    MOVE MPUT      TO KCOP.
    MOVE "NE"      TO KCOM.
    MOVE 80        TO KCLM.
    MOVE SPACES    TO KCRN.
    MOVE SPACES    TO KCMF.
    MOVE ZEROES    TO KCDF.
    CALL "KDCS"    USING KCPAC NB.
    MOVE PEND      TO KCOP.
    MOVE "ER"      TO KCOM.
    CALL "KDCS"    USING KCPAC.
    GO TO PROG-END.

```

Program unit FILES with START/SHUT exit and file access operations

```

IDENTIFICATION DIVISION.
PROGRAM-ID.      FILES.
ENVIRONMENT DIVISION.
*****
INPUT-OUTPUT SECTION.
*-----
FILE-CONTROL.
    SELECT ADDRESSES ASSIGN TO "addresses"
    ACCESS MODE IS RANDOM
    ORGANIZATION IS INDEXED
    RECORD KEY IS D-NAME
    FILE STATUS IS FILE-STATUS.

```

```

DATA DIVISION.
*****
FILE SECTION.
*-----
FD  ADDRESSES      LABEL RECORD IS STANDARD.
01  D-ADDRESSRECORD.
    05  D-NAME.
        10  D-LASTNAME      PIC X(14).
        10  D-FST           PIC X(02).
    05  D-FIRSTNAME      PIC X(18).
    05  D-STREET         PIC X(26).
    05  D-HOUSENO       PIC X(10).
    05  D-ZIP            PIC X(05).
    05  D-CITY           PIC X(26).
    05  D-PHONE         PIC X(18).
WORKING-STORAGE SECTION.
*-----
01  FILE-ERROR-LINE.
    05  FILLER           PIC X(24)
        VALUE "   *** FILE ERROR NO.: ".
    05  FILE-STATUS     PIC X(02).
    05  FILLER           PIC X(04)
        VALUE "   ***".
    05  FILLER           PIC X(50) VALUE SPACES.
LINKAGE SECTION.
*-----
    COPY KCKBC.
    05  KBPRG           PIC X(228).
    COPY KCPAC.
    03  NB.
        05  TAC         PIC X(008).
        05  DATA1     PIC X(220).
    03  FILLER REDEFINES NB.
    COPY FORMAO.
PROCEDURE DIVISION USING KCKBC KCSPAB.
*****
CONTROLLING SECTION.
*-----
CONTROLLING-BEGIN.
    IF KCTACVG = "STARTUP"
    THEN OPEN I-O ADDRESSES GO TO CONTROLLING-END.
    IF KCTACVG = "SHUTDOWN"
    THEN CLOSE ADDRESSES GO TO CONTROLLING-END.
    IF KCTACVG = "1"
    THEN GO TO READING-BEGIN.
    IF KCTACVG = "2"
    THEN GO TO WRITING-BEGIN.
    IF KCTACVG = "3"
    THEN GO TO OVERWRITING-BEGIN.
    IF KCTACVG = "4"
    THEN GO TO DELETING-BEGIN.
CONTROLLING-END.
    EXIT PROGRAM.
READING SECTION.
*-----
READING-BEGIN.
*   SET THE ISAM KEY
    MOVE LASTNAMEO TO D-LASTNAME.

```

```

MOVE FSTO    TO D-FST.
MOVE SPACES TO STREETO HOUSENOO CITYO PHONEO.
MOVE ZEROES TO ZIPO.
MOVE KCTACVG TO TACO.
MOVE "DISPLAY ADDRESSES" TO FUNCTIONO.
READ ADDRESSES RECORD
INVALID KEY PERFORM FILE-ERROR  GO TO READING-END.
MOVE D-LASTNAME TO LASTNAMEO.
MOVE D-FST      TO FSTO.
MOVE D-FIRSTNAME TO FSTRESTO.
MOVE D-STREET  TO STREETO.
MOVE D-HOUSENO TO HOUSENOO.
MOVE D-ZIP     TO ZIPO.
MOVE D-CITY    TO CITYO.
MOVE D-PHONE   TO PHONEO.
READING-END.
EXIT PROGRAM.
WRITING SECTION.
*-----
WRITING-BEGIN.
ENTRY  "WRITING"          USING  ADDRESSRECORD.
MOVE FSTO    TO D-FST.
MOVE FSTRESTO TO D-FIRSTNAME.
MOVE STREETO TO D-STREET.
MOVE HOUSENOO TO D-HOUSENO.
MOVE ZIPO     TO D-ZIP.
MOVE CITYO    TO D-CITY.
MOVE PHONEO   TO D-PHONE.
MOVE KCTACVG TO TACO.
MOVE "ADD NEW ADDRESSES" TO FUNCTIONO.
MOVE " * ADDRESS ADDED * " TO MSGTEXTO.
WRITE D-ADDRESSRECORD INVALID KEY PERFORM FILE-ERROR.
WRITING-END.
EXIT PROGRAM.
OVERWRITING SECTION.
*-----
OVERWRITING-BEGIN.
*   Read record to lock record
MOVE LASTNAMEO TO D-LASTNAME.
MOVE FSTO      TO D-FST.
MOVE "UPDATE ADDRESSES      " TO FUNCTIONO.
READ ADDRESSES RECORD
INVALID KEY PERFORM FILE-ERROR  GO TO OVERWRITING-END.
MOVE FSTRESTO TO D-FIRSTNAME.
MOVE STREETO  TO D-STREET.
MOVE HOUSENOO TO D-HOUSENO.
MOVE ZIPO     TO D-ZIP.
MOVE CITYO    TO D-CITY.
MOVE PHONEO   TO D-PHONE.
MOVE " * ADDRESS UPDATED * " TO MSGTEXTO.
REWRITE D-ADDRESSRECORD INVALID KEY PERFORM FILE-ERROR.
OVERWRITING-END.
EXIT PROGRAM.
DELETING SECTION.
*-----
DELETING-BEGIN.
*   Read record to lock record
MOVE LASTNAMEO TO D-LASTNAME.
MOVE FSTO      TO D-FST.

```

```

MOVE "DELETE ADDRESSES" TO FUNCTIONO.
READ ADDRESSES RECORD
INVALID KEY PERFORM FILE-ERROR GO TO DELETING-END.
DELETE ADDRESSES RECORD
INVALID KEY PERFORM FILE-ERROR GO TO DELETING-END.
MOVE KCTACVG TO TACO.
MOVE "*" ADDRESS DELETED "*" TO MSGTEXTO.
DELETING-END.
EXIT PROGRAM.
FILE-ERROR SECTION.
*-----
FILE-ERROR-BEGIN.
IF FILE-STATUS = 22 THEN
MOVE "*** ADDRESS WITH THIS NAME ALREADY EXISTS ***"
TO MSGTEXTO GO TO FILE-ERROR-END.
IF FILE-STATUS = 23 THEN
MOVE "*** ADDRESS WITH THIS NAME DOES NOT EXIST ***"
TO MSGTEXTO GO TO FILE-ERROR-END.
MOVE FILE-ERROR-LINE TO MSGTEXTO.
FILE-ERROR-END.
EXIT.

```

Program unit BADTACS

```

IDENTIFICATION DIVISION.
PROGRAM-ID. BADTACS.
*****
ENVIRONMENT DIVISION.
*****
DATA DIVISION.
WORKING-STORAGE SECTION.
77 BTEXT PIC X(41) VALUE
"INCORRECT TAC - PLEASE REPEAT INPUT".
77 STAR PIC X(6) VALUE ALL "*".
COPY KCOPC.
01 ERRORETEXT.
05 FILLER PIC X(21)
VALUE "*** E R R O R ***".
05 FILLER PIC X(14)
VALUE "PROGRAM UNIT: ".
05 F-TP PIC X(08).
05 FILLER PIC X(17)
VALUE " KDCS OPCODE: ".
05 F-OP PIC X(04).
05 FILLER PIC X(13)
VALUE "RETURN CODE: ".
05 F-CD PIC X(03).
LINKAGE SECTION.
COPY KCKBC.
COPY KCPAC.
03 NB.
05 TRANSAC PIC X(08).
05 DATA1 PIC X(220).
03 NB-A REDEFINES NB.
COPY FORMAO.
41 ERROR1 REDEFINES MSGTEXTO.
45 STAR1 PIC X(6).

```

```

    45  BADTEXT          PIC X(41).
    45  STAR2           PIC X(6).
    45  REST            PIC X(27).
*****
PROCEDURE DIVISION USING KCKBC KCSPAB.
*****
INIT-OPERATION-SECTION.
    MOVE SPACES      TO NB.
    MOVE INIT        TO KCOP.
    MOVE 0           TO KCLKBPRG.
    MOVE 228         TO KCLPAB.

    CALL "KDCS"      USING KCPAC.
    IF KCRCCC NOT = ZERO
        THEN MOVE INIT TO F-OP GO TO ERROR-HANDLING.
MGET-OPERATION.
    MOVE MGET        TO KCOP.
    MOVE 228         TO KCLA.
    MOVE "*FORMA"    TO KCMF.
    CALL "KDCS"      USING KCPAC, DATA1.
    IF KCRCCC = "05Z"
        THEN MOVE SPACES TO NB-A.
        GO TO MPUT-OPERATION.
    IF KCRCCC NOT = ZERO
        THEN MOVE MGET TO F-OP GO TO ERROR-HANDLING.
MPUT-OPERATION.
    MOVE BTEXT       TO BADTEXT.
    MOVE STAR        TO STAR1.
    MOVE STAR        TO STAR2.
    MOVE SPACES      TO REST.
    MOVE SPACES      TO TAC.
    MOVE MPUT        TO KCOP.
    MOVE "NE"        TO KCOM.
    MOVE 228         TO KCLM.
    MOVE SPACES      TO KCRN.
    MOVE "*FORMA"    TO KCMF.
    CALL "KDCS"      USING KCPAC, NB.
    IF KCRCCC NOT = ZERO
        THEN MOVE MPUT TO F-OP GO TO ERROR-HANDLING.
PEND-OPERATION.
    MOVE PEND        TO KCOP.
    MOVE "FI"        TO KCOM.
    CALL "KDCS"      USING KCPAC.
PROG-END.
    EXIT PROGRAM.
ERROR-HANDLING.
    MOVE "BADTACS"   TO F-TP.
    MOVE KCRCCC      TO F-CD.
    MOVE ERRORTTEXT  TO NB.
    MOVE MPUT        TO KCOP.
    MOVE "NE"        TO KCOM.
    MOVE 80          TO KCLM.
    MOVE SPACES      TO KCRN.
    MOVE SPACES      TO KCMF.
    MOVE ZEROES      TO KCDF.
    CALL "KDCS"      USING KCPAC NB.
    MOVE PEND        TO KCOP.
    MOVE "ER"        TO KCOM.
    CALL "KDCS"      USING KCPAC.

```

GO TO PROG-END.

Generation of the sample application

```
REM *****
REM ***          D E F  -  S T A T E M E N T S          ***
REM ***
REM ***          KDCFILE = APPLI          ***
REM *****
MAX APPLINAME=A
MAX KDCFILE=(KDCFILE.APPLI,S),TASKS=2,ASYNTASKS=0
MAX CONRTIME=5,LOGACKWAIT=60
ROOT ADR1ROOT
OPTION GEN=ALL
REM *****
REM *****          PROGRAM STATEMENTS          *****
REM *****
PROGRAM KDCADM,COMP=C
PROGRAM DISPLAY,COMP=COB1
PROGRAM UPDATE,COMP=COB1
PROGRAM FILES,COMP=COB1
PROGRAM BADTACS,COMP=COB1
REM *****
REM *****          EXIT STATEMENTS          *****
REM *****
EXIT PROGRAM=TPFILE,USAGE=START
EXIT PROGRAM=TPFILE,USAGE=SHUT
REM *****
REM *****          TAC STATEMENTS          *****
REM *****
DEFAULT TAC ADMIN=Y,PROGRAM=KDCADM
TAC KDCTAC
TAC KDCLTERM
TAC KDCPTERM
TAC KDCSWTCH
TAC KDCUSER
TAC KDCSEND
TAC KDCAPPL
TAC KCDIAG
TAC KDCLOG
TAC KDCINF
TAC KDCHELP
TAC KDCSHUT
DEFAULT TAC TYPE=A,ADMIN=Y,PROGRAM=KDCADM
TAC KDCTACA
TAC KDCLTRMA
TAC KDCPTRMA
TAC KDCSWCHA
TAC KDCUSERA
TAC KDCSEDA
TAC KDCAPPLA
TAC KCDIAGA
TAC KDCLOGA
TAC KDCINF A
TAC KDCHELPA
TAC KDCSHUTA
TAC KDCTCLA
```

```

DEFAULT TAC TYPE=D,PROGRAM=(STD)
TAC KDCBADTC,PROGRAM=BADTACS
TAC 1,LOCK=1,PROGRAM=DISPLAY
TAC 2,LOCK=2,PROGRAM=UPDATE
TAC 3,LOCK=2,PROGRAM=UPDATE
TAC 4,LOCK=2,PROGRAM=UPDATE
REM *****
REM *****          USER STATEMENTS          *****
REM *****
USER  GUENTER,PASS=C'AUFGEHTS',KSET=BUND1,PERMIT=ADMIN,FORMAT=*FORMA
USER  BESSY,PASS=C'HH',KSET=BUND2,STATUS=ON,FORMAT=*FORMA
USER  HAPPY,KSET=BUND3,STATUS=ON,FORMAT=*FORMA
REM *****
REM *****          FORMSYS STATEMENTS          *****
REM *****
FORMSYS TYPE=FHS
REM *****
REM *****          PTERM/LTERM STATEMENTS          *****
REM *****
DEFAULT PTERM PRONAM=DSR01,PTYPE=T9750
PTERM DSS01,LTERM=UTMDST1
PTERM DSS02,LTERM=UTMDST2
PTERM DSS03,LTERM=UTMDST3
DEFAULT PTERM PRONAM=DSR01,PTYPE=T9022,USAGE=0
PTERM G01,LTERM=DRUCKER,CONNECT=A
LTERM UTMDST1,KSET=BUND1
LTERM UTMDST2,LOCK=4,KSET=BUND1
LTERM UTMDST3,LOCK=5,KSET=BUND1
LTERM DRUCKER,USAGE=0
REM *****
REM *****          KSET STATEMENTS          *****
REM *****
KSET  BUND1,KEYS=(1,2,3,4,5)
KSET  BUND2,KEYS=(1,2,4)
KSET  BUND3,KEYS=(1)
REM *****
REM *****          TLS STATEMENTS          *****
REM *****
TLS   TLSA
TLS   TLSB
END

```

12 Appendix

- Overview of all KDCS calls
- Different field names for C/C++ and COBOL
- ASCII-EBCDIC code conversion
 - BS2000 systems
 - Unix, Linux and Windows systems
 - Modifying the code conversion tables on Unix and Linux systems
 - Modifying the code conversion tables on Windows systems

12.1 Overview of all KDCS calls

Overview of the entries in the KDCS parameter area and message area (NB) for KDCS calls. Binary zero should be set in fields that are not listed.

In the table below, the field names in C/C++ are listed only if they differ from the field names in COBOL by more than just their case.

The key to the tables below is as follows:

- 0 binär null
- B Leerzeichen (Blanks)
- X sonstige Angaben
- * Rückgaben

KDCS parameter area								NB / 2nd parameter area
KCOP	KCOM	KCLA KCLKBPRG /kclcapa	KCLM KCLPAB /kclspa	KCRN	KCMCOM			
					KCMF /kcfn KCLT KCUS KCPA KCGTM	KCDF KCLI KCQRC	KCAPRO KCDPUT KCDGET KCQCRE KCEVENT KCPADM KCSGCL /kc_sgcl KCNORPLY	
APRO	AM DM		X X	X X	X X		X X	[X] [X]
CTRL	PR PE AB	0 0 0	0 0 0	X X X	B B B		X/0 X/0 0	Currently not used; must be passed
DADM	RQ UI CS DL DA MV MA	X X 0 0 0 0 0	0 0 0 0 0 0 0	X X X X B X B	X 0 0 X X X X	0 0 0 0 0 0 0	X ¹ X X X ¹ X ¹ X X	* * * * * * *
DGET	FT NT BF BN PF PN	X X X X X X	0 0 0 0 0 0	X X X X X X	B B X X X X	0 0 0 0 0 0	X X X X X X	* * * * * *

KDCS parameter area								NB / 2nd parameter area
KCOP	KCOM	KCLA KCLKBPRG /kclcapa	KCLM KCLPAB /kclspa	KCRN	KCMCOM			
					KCMF /kcfn KCLT KCUS KCPA KCGTM	KCDF KCLI KCQRC	KCAPRO KCDPUT KCDGET KCQCRE KCEVENT KCPADM KCSGCL /kc_sgcl KCNORPLY	
DPUT	NT		X	X	X	X	X	X
	NE		X	X	X	X	X	X
	NI	0	X	X	B	0	X	X
	QT	0	X	X	X	0	X ¹	X
	QE	0	X	X	X	0	X ¹	X
	QI	0	X	X	B	0	X	X
	+T	0	X	X	B	0	0	X
	-T	0	X	X	B	0	0	X
	+I	0	X	X	B	0	0	X
	-I	0	X	X	B	0	0	X
	RP ²	0	X	X	B	0	X	X
FGET		X			X			*
FPUT	NT		X	X	X	X		X
	NE		X	X	X	X		X
	RP ²		X	X	B	0		X
GTDA		X		X	X			*
INFO	CD	X			X			*
	DT	X						*
	LO	X						*
	PC	X						*
	SI	X						*
	CK							X
INIT		X	X					
	PU	X	X	0	0	X	0	*
	MD	X	0	0	0	0	0	
LPUT		X					X	
MCOM	BC	0	0	X		X		
	EC	0	0	0		X		

KDCS parameter area								NB / 2nd parameter area
KCOP	KCOM	KCLA KCLKBPRG /kclcapa	KCLM KCLPAB /kclspa	KCRN	KCMCOM			
					KCMF /kcfn KCLT KCUS KCPA KCGTM	KCDF KCLI KCQRC	KCAPRO KCDPUT KCDGET KCQCRE KCEVENT KCPADM KCSGCL /kc_sgcl KCNORPLY	
MGET	NT	X X		X	X X			* *
MPUT	NT NE PM RM EM ES HM		X X X X 0 X 0	X X B X X 0 X	X X X 0 B X B	X X X X 0 0 0		X X X X X X X
PADM	OK PR AT AC CA CS AI PI	0 0 0 0 0 0 X X	0 0 0 0 0 0 0 0	X X X X X X X X	X X X X X X X X	0 0 0 0 0 0 0 0	0 0 0 0 X X 0 0	* * * * * * * *
PEND	PA PR PS KP RE SP FC RS FR FI ER			X X X X X X B B			0 0 0 0 0 0	
PGWT	KP PR CM RB	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	X X X X	0 0 0 0	* * * *

KDCS parameter area								NB / 2nd parameter area
KCOP	KCOM	KCLA KCLKBPRG /kclcapa	KCLM KCLPAB /kclspa	KCRN	KCMCOM			
					KCMF /kcfn KCLT KCUS KCPA KCGTM	KCDF KCLI KCQRC	KCAPRO KCDPUT KCDGET KCQCRE KCEVENT KCPADM KCSGCL /kc_sgcl KCNORPLY	
PTDA		X		X	X			X
QCRE	NN WN	X X	0 0	B X	B B	0 0	X X	
QREL	RL	0	0	X	B	0	0	
RSET								
SGET	KP RL GB US	X X X X		X X X X				* * * *
SIGN	ST ON CP CK OF OB CL ²	X X X X 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 X 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	X X X X
SPUT	DL MS ES GB US	X X X X X	0	X X X X X	X	0	0	X X X X X
SREL	LB GB			X X				
UNLK	GB DA US	0	0	X X X	X X	0	0	

¹ If KCLT contains the name of a USER or temporary queue, a value of U or Q must be specified in the KCQTYP field.

² Only on BS2000 systems

Overview of the values returned to the KDCS communication area for KDCS calls.

In the tables below, an asterisk (*) always indicates a return value.

Call		KDCS communication area							
KCOP	KCOM	KB header	KB return area						KB program area
			K C R D F	K C R L M	KCRINFCC KCRMGT KCRST KCRSIGN	KCRCCC KCRCDC	KCRMF /kcrfn	KCRPI KCRUS KCRWVG KCRQN KCRQRC KCRGTM KCRDPID KCRRC	
APRO	AM DM					*	*		
CTRL	PR PE AB					*	*	*	
DADM	RQ UI CS DL DA MV MA			*	*	*	*	*	
DGET	FT NT BF BN PF PN			*	*	*	*	*	*
DPUT	NT NE NI QT QE QI +T -T +I -I RP ¹					*	*	*	*

Call		KDCS communication area							
KCOP	KCOM	KB header	KB return area						KB program area
			K C R D F	K C R L M	KCRINFCC KCRMGT KCRST KCRSIGN	KCRCCC KCRCDC	KCRMF /kcrfn	KCRPI KCRUS KCRWVG KCRQN KCRQRC KCRGTM KCRDPID KCRRC	
FGET				*			*	*	
FPUT	NT NE RP ¹						*		
							*		
GTDA				*			*		
INFO	CD DT LO PC SI			*			*		
	CK			*	*		*		
INIT		*					*	*	*
	PU MD	*		*			*	*	*
LPUT							*		
MCOM							*		
	BC EC						*		
MGET	NT		*	*	*	*	*	*	
MPUT			*				*		
	NT						*		
	NE						*		
	PM						*		
	RM						*		
	EM						*		
	ES HM						*		

Call		KDCS communication area							
KCOP	KCOM	KB header	KB return area					KB program area	
			K C R D F	K C R L M	KCRINFCC KCRMGT KCRST KCRSIGN	KCRCCC KCRCDC	KCRMF /kcrfn		KCRPI KCRUS KCRWVG KCRQN KCRQRC KCRGTM KCRDPID KCRRC
PADM	OK PR AT AC CA CS AI PI			*		*		*	
PEND	PA PR PS KP RE SP FI FC RS ER FR					*			
PGWT ²	KP PR CM RB			*		*	*	*	
PTDA						*			
QCRE	NN WN					*		*	
QREL	RL					*			
RSET						*			*

Call		KDCS communication area							
KCOP	KCOM	KB header	KB return area						KB program area
			K C R D F	K C R L M	KCRINFCC KCRMGT KCRST KCRSIGN	KCRCCC KCRCDC	KCRMF /kcrfn	KCRPI KCRUS KCRWVG KCRQN KCRQRC KCRGTM KCRDPID KCRRC	
SGET	KP RL GB US			*		*			
SIGN	ST			*	*	*	*	*	
	ON CP CK OF OB CL ¹				*	*	*	*	
SPUT	DL MS ES GB US					*	*	*	
SREL	LB GB					*	*		
UNLK	GB DA US					*	*	*	

¹ Only on BS2000 systems

² KCRLM is only supplied when KCLI>0 was specified.

12.2 Different field names for C/C++ and COBOL

Throughout this manual, the COBOL field names (which are always written as uppercase letters) are used for the communication area and the KDCS parameter area. In C/C++, field names always use lowercase letters.

Since the field names for C/C++ are (unlike those for COBOL) derived from the corresponding English terms, further differences arise between the KB fields and those in the KDCS parameter area, apart from the different cases used.

Throughout this manual, wherever discrepancies arise which go beyond the simple issue of uppercase and lowercase, the C/C++ field name specified immediately following the COBOL field name; the two are separated by a slash. For example: "KCTAG/kcday".

In the tables on the next few pages, all COBOL field names which differ from C/C++ field names in more than just the case used are shaded gray.

Moreover, you should also note the following points:

- in the data structures *kcdad.h* and *kcpad.h*, the fields for time specifications in C/C++ are **not** combined in a group.
- In the data structure *kcini.h*, the field names are structured differently to their counterparts in the COBOL data structure KCINIC (see table on "[INIT Initialize program unit](#)"). These data structures allow you to structure the message area for the INIT call with the modifier PU, and for the call with KCLI>0.
- On BS2000 systems, the screen function for reading the ID card reader in C/C++ has the symbolic name KCCARDRD.

Field names in the KB header area KCKBKOPF (ca_hdr)

COBOL name	C/C++ name	Meaning
KCBENID	kcuserid	user identification
KCTACVG	kccv_tac	service: name of the transaction code
KCTAGVG	kccv_day	start of service: day
KCMONVG	kccv_month	start of service: month
KCJHRVG	kccv_year	start of service: year
KCTJHVG	kccv_doy	start of service: day of the year
KCSTDVG	kccv_hour	start time of service: hour
KCMINVG	kccv_minute	start time of service: minute
KCSEKVG	kccv_second	start time of service: second
KCKNZVG	kccv_status	service: status information
KCTACAL	kcpr_tac	program run: name of the transaction code
KCSTDAL	kcpr_hour	start time of program run: hour

COBOL name	C/C++ name	Meaning
KCMINAL	kcpr_minute	start time of program run: minute
KCSEKAL	kcpr_second	start time of program run: second
KCAUSWEIS	kccard	status of card reader
KCTAIND	kctaind	transaction indicator
KCLOGTER	kclogter	logical terminal name
KCTERMN	kctermn	terminal mnemonic
KCLKBPB	kclpa	length of program area
KCHSTA	kchsta	stack level
KCDSTA	kcdsta	change in stack level
KCPRIND	kcprind	program indicator
KCOF1	kcof1	OSI TP functional unit
KCCP	kccp	client protocol
KCTARB	kctarb	transaction rollback indicator
KCYEARVG	kccv_year4	start of service: day of the year, 4-digit

Field names in the KB return area KCRFELD (ca_rti)

COBOL name	C/C++ name	Meaning
KCRDF	kcrdf	device feature
KCRLM	kcrIm	input message length
KCRINFCC	kcrinfcc	return information from INFO CK
KCVGST	kcpcv_state	service state of partner
KCTAST	kcpta_state	transaction state of partner
KCRMGT	kcrmgt	type of message
KCRSIGN	kcrsign	status of SIGN ON (complete code)
KCRSIGN1	kcrsign1	primary code of SIGN ON
KCRSIGN2 ¹	—	secondary code of SIGN ON
KCRCCC	kcrccc	compatible return code
KCRCKZ	krcid	identifier of DC system
KCRCDC	krcdc	return code of DC system
KCRMF	kcrfn	format name
KCRPI	kcrpi	service identification
KCRQN	kcrqn	return queue name
KCRWVG	kcrwvg	return number waiting vg
KCRUS	kcrus	return user (SIGN ST, DGET FT)
KCRQRC	kcrqrc	queue specific redelivery counter
KCRGTM	kcrgtm	creation time of DGET message
KCRDPID	kcrdpid	DPUT ID of DGET message
KCRRC	kcrrc ²	redelivery counter of DGET message

¹ The field KCRSIGN2 is not defined in the C/C++ data structure ca_rti; the secondary code for the SIGN call is defined in the second and third byte of kcrinfcc.

² There is no field in the C data structure of the appropriate type that can be used directly. The field KCRRC from kcmac.h of type unsigned short must be used.

Field names in the KDCS parameter area KCPAC (kc_pa)

COBOL name	C/C++ name	Meaning
KCOP	kcop	operation code
KCOM	kcom	operation modification
KCLA	kcla	length of data area
KCLKBPRG	kclcapa	length of ca program area
KCLM	kclm	length of message (segment)
KCWTIME	kcwtime	waiting time for DGET messages
KCLPAB	kclspa	length of standard primary area
KCRN	kcrn	reference name
KCMF	kcfm	format name
KCLT	kclt	logical terminal name
KCUS	kcus	name of user
KCPA	kcpa	partner application name
KCOF	kcof	OSI functions
KCDF	kcdf	device feature
KCLI	kcli	length of init area
EXTENT	kcext	extensions for DPUT, APRO and PADM
KCDPUT	kcdput	extension for DPUT function
KCMOD	kcmmod	DPUT: modifier
KCTAG	kcdays	DPUT: days
KCSTD	kchour	DPUT: hours
KCMIN	kcmmin	DPUT: minutes
KCSEK	kcsec	DPUT: seconds
KCQTYP	kcqtyp	queue type
KCQMODE	kcqmode	queue mode
KCAPRO	kcapro	extension for APRO function

COBOL name	C/C++ name	Meaning
KCPI	kcpi	APRO: process identification
KCPADM	kcpadm	extension for PADM function
KCACT	kcact	PADM: action
KCADRLT	kcadrlt	PADM: lterm name
KCNORPLY	kcnorply	CTRL: reply message not permitted
KCMCOM	kcmcom	redefinition for MCOM function
KCPOS	kcpos	MCOM: destination in positive case
KCNEG	kcneg	MCOM: destination in negative case
KCCOMID	kccomid	MCOM: complex identification
KCSGCL ¹	kc_sgcl	extensions for SIGN CL
KCLANGID ¹	kclangid	language ID of user
KCTERRID ¹	kcterrid	territorial ID of user
KCCSNAME ¹	kccsname	character set name of user
KCGTM	kcgtm	creation time of message (generation time)
KCQRC	kcqrc	queue-specific redelivery counter
KCDPID	kcdpid	DPUT ID of message

¹ Only on BS2000 systems

12.3 ASCII-EBCDIC code conversion

If the UTM application and the communication partner use different codes (EBCDIC, ASCII compatible code), UTM provides the option of initiating generation of a partner-specific automatic code conversion.

To do this, UTM provides four code conversions that convert data as follows:

BS2000, Unix and Linux systems:

- SYS1/SYS/SYSTEM: ISO8859-i EBCDIC.DF.04.i (EDF04i)
- SYS2: ISO8859-1 EBCDIC.DF.04.DRV (EDF04DRV)
- SYS3: ISO646-IRV EBCDIC.03.DF.03.IRV (EDF03IRV)
- SYS4: ISO646-IRV EBCDIC.03.DF.03.DRV (EDF03DRV).

Windows systems:

- SYS1/SYS/SYSTEM: Windows-1252 EBCDIC.DF.04.F (EDF04F)
- SYS2: Windows-1252 EBCDIC.DF.04.DRV (EDF04DRV)
- SYS3: ISO646-IRV EBCDIC.03.DF.03.IRV (EDF03IRV)
- SYS4: ISO646-IRV EBCDIC.03.DF.03.DRV (EDF03DRV).

SYS1 and SYS2 are conversions between two 8-bit codes. SYS3 and SYS4 are conversions between two 7-bit codes.

The following sections outline the following for the individual platforms:

- the partners for which the conversion tables can be used,
- how you can modify/replace them.



Please refer to the chapter "Code Conversion" in the openUTM manual "Generating Applications" for an overview of how to generate the code conversion.

12.3.1 BS2000 systems

On BS2000 systems, an automatic code conversion can be generated for communication between the UTM application and a TS application of the SOCKET-USP type (operand MAP= in the PTERM or TPOOL statement) and for HTTP clients (CHAR-SET statement and operand CONVERT-TEXT in the HTTP-DESCRIPTOR statement). This is because socket USP applications and HTTP clients generally uses an ASCII compatible code, while the UTM application normally uses an EBCDIC code.

Modifying code conversion tables on BS2000 systems

The tables are defined in the assembler module KDCEA. The source for KDCEA is located in the library SYSLIB.UTM.070.EXAMPLE.

To change a table, proceed as follows:

1. Modify the table in the KDCEA module.
2. Assemble the KDCEA module.
3. Link KDCEA to the application using the INCLUDE-MODULES statement **before** the RESOLVE-BY-AUTOLINK statement is effective for the library SYSLNK.UTM.070.

12.3.2 Unix, Linux and Windows systems

On Unix, Linux and Windows systems, an automatic conversion can be generated for UPIC clients and TS applications of the APPLI and SOCKET-USP type, and also for server-server communication with LU6.1 and OSI TP partners (operand MAP= in the PTERM, TPOOL, OSI-CON, and SESCHA statement).

The code conversion tables are defined in the C source `kcsaeea.c`, which is located in the following directory:

utmpath/src/kcsaeea.c (Unix and Linux systems)

utmpath\src\kcsaeea.c (Windows systems)

12.3.2.1 Modifying the code conversion tables on Unix and Linux systems

On Unix and Linux systems, you can modify these tables as follows:

1. Copy the file `kcsaeee.c` to a separate file directory.
2. Modify the conversion tables according to your requirements. To do this, edit the file `kcsaeee.c` with a text editor. For each of the four code conversions, `kcsaeee.c` contains two character arrays with a length of 256. One array is used for ASCII EBCDIC conversion, the other for EBCDIC ASCII conversion.
3. Compile the modified source file and use it to generate a shared object.
4. Link this additional shared object to the application program.

12.3.2.2 Modifying the code conversion tables on Windows systems

The code conversion tables are located in the library `utmconvt.dll`. `utmconvt.dll` is located in the same directory as `libwork.dll`.

You can adapt these conversion tables to your own requirements by modifying the source file `kcsaeea.c` supplied in the directory `utmpath\src` and creating a modified `utmconvt.dll`.

i In addition `utmpath\src` contains the resource file `utmconvt.rc` with version and copyright information. This information is displayed if you right-click the dll file and select *Properties*. It is not essential for this file to be included.

Modifying the library `utmconvt.dll`

To modify the library `utmconvt.dll` the following steps are necessary:

1. Copy the file `kcsaeea.c` to a separate file directory.
2. Modify the conversion tables according to your requirements. To do this, edit the file `kcsaeea.c` with a text editor. For each of the four code conversions, `kcsaeea.c` contains two character arrays with a length of 256. One array is used for ASCII EBCDIC conversion, the other for EBCDIC ASCII conversion.
3. Start Microsoft Visual Studio and proceed as follows:
 - a. In the `utmpath` directory, create a new Win32 or X64 project with the name `utmconvt` and with the application type *Dynamic Link Library*.
 - b. Add the following files to the project:
 - The modified code table file `kcsaeea.c`,
 - and, if required, `utmconvt.rc`.
 - c. Assign the file `utmconvt.def` to the project as module definition file (Project properties Linker Module Definition File).
 - d. From this project, create the library `utmconvt.dll`.
 - e. Close Microsoft Visual Studio
4. Replace the old library `utmconvt.dll` with the new library:
 - First back up the library under a different name, so that you can access it again if anything goes wrong.
 - Copy the new `utmconvt.dll` to the directory which contains the UTM library `libwork.dll` (this is generally `utmpath\ex`). Make sure that the original `utmconvt.dll` is actually replaced by the new `utmconvt.dll`.

The new conversion library is ready for use.

13 Glossary

A term in *italic* font means that it is explained somewhere else in the glossary.

abnormal termination of a UTM application

Termination of a *UTM application*, where the *KDCFILE* is not updated. Abnormal termination is caused by a serious error, such as a crashed computer or an error in the system software. If you then restart the application, openUTM carries out a *warm start*.

abstract syntax (OSI)

Abstract syntax is defined as the set of formally described data types which can be exchanged between applications via *OSI TP*. Abstract syntax is independent of the hardware and programming language used.

acceptor (CPI-C)

The communication partners in a *conversation* are referred to as the *initiator* and the acceptor. The acceptor accepts the conversation initiated by the initiator with *Accept_Conversation*.

access list

An access list defines the authorization for access to a particular *service*, *TAC queue* or *USER queue*. An access list is defined as a *key set* and contains one or more *key codes*, each of which represent a role in the application. Users or LTERMs or (OSI) LPAPs can only access the service or *TAC queue* or *USER queue* when the corresponding roles have been assigned to them (i.e. when their *key set* and the access list contain at least one common *key code*).

access point (OSI)

See *service access point*.

ACID properties

Acronym for the fundamental properties of *transactions*: atomicity, consistency, isolation and durability.

administration

Administration and control of a *UTM application* by an *administrator* or an *administration program*.

administration command

Commands used by the *administrator* of a *UTM application* to carry out administration functions for this application. The administration commands are implemented in the form of *transaction codes*.

administration journal

See *cluster administration journal*.

administration program

Program unit containing calls to the *program interface for administration*. This can be either the standard administration program *KDCADM* that is supplied with openUTM or a program written by the user.

administrator

User who possesses administration authorization.

AES

AES (Advanced Encryption Standard) is the current symmetric encryption standard defined by the National Institute of Standards and Technology (NIST) and based on the Rijndael algorithm developed at the University of Leuven (Belgium). If the AES method is used, the UPIC client generates an AES key for each session.

Apache Axis

Apache Axis (Apache eXtensible Interaction System) is a SOAP engine for the design of Web services and client applications. There are implementations in C++ and Java.

Apache Tomcat

Apache Tomcat provides an environment for the execution of Java code on Web servers. It was developed as part of the Apache Software Foundation's Jakarta project. It consists of a servlet container written in Java which can use the JSP Jasper compiler to convert JavaServer pages into servlets and run them. It also provides a fully featured HTTP server.

application cold start

See *cold start*.

application context (OSI)

The application context is the set of rules designed to govern communication between two applications. This includes, for instance, abstract syntaxes and any assigned transfer syntaxes.

application entity (OSI)

An application entity (AE) represents all the aspects of a real application which are relevant to communications. An application entity is identified by a globally unique name (“globally” is used here in its literal sense, i.e. worldwide), the *application entity title* (AET). Every application entity represents precisely one *application process*. One application process can encompass several application entities.

application entity qualifier (OSI)

Component of the *application entity title*. The application entity qualifier identifies a *service access point* within an application. The structure of an application entity qualifier can vary. openUTM supports the type “number”.

application entity title (OSI)

An application entity title is a globally unique name for an *application entity* (“globally” is used here in its literal sense, i.e. worldwide). It is made up of the *application process title* of the relevant *application process* and the *application entity qualifier*.

application information

This is the entire set of data used by the *UTM application*. The information comprises memory areas and messages of the UTM application including the data currently shown on the screen. If operation of the UTM application is coordinated with a database system, the data stored in the database also forms part of the application information.

application process (OSI)

The application process represents an application in the *OSI reference model*. It is uniquely identified globally by the *application process title*.

application process title (OSI)

According to the OSI standard, the application process title (APT) is used for the unique identification of applications on a global (i.e. worldwide) basis. The structure of an application process title can vary. openUTM supports the type *Object Identifier*.

application program

An application program is the core component of a *UTM application*. It comprises the main routine *KDCROOT* and any *program units* and processes all jobs sent to a *UTM application*.

application restart

see *warm start*

application service element (OSI)

An application service element (ASE) represents a functional group of the application layer (layer 7) of the *OSI reference model*.

application warm start

see *warm start*.

association (OSI)

An association is a communication relationship between two application entities. The term "association" corresponds to the term *session* in *LU6.1*.

asynchronous conversation

CPI-C conversation where only the *initiator* is permitted to send. An asynchronous transaction code for the *acceptor* must have been generated in the *UTM application*.

asynchronous job

Job carried out by the job submitter at a later time. openUTM includes *message queuing* functions for processing asynchronous jobs (see *UTM-controlled queue* and *service-controlled queue*). An asynchronous job is described by the *asynchronous message*, the recipient and, where applicable, the required execution time. If the recipient is a terminal, a printer or a transport system application, the asynchronous job is a *queued output job*. If the recipient is an *asynchronous service* of the same application or a remote application, the job is a *background job*. Asynchronous jobs can be *time-driven jobs* or can be integrated in a *job complex*.

asynchronous message

Asynchronous messages are messages directed to a *message queue*. They are stored temporarily by the local *UTM application* and then further processed regardless of the job submitter. Distinctions are drawn between the following types of asynchronous messages, depending on the recipient:

- In the case of asynchronous messages to a *UTM-controlled queue*, all further processing is controlled by openUTM. This type includes messages that start a local or remote *asynchronous service* (see also *background job*) and messages sent for output on a terminal, a printer or a transport system application (see also *queued output job*).
- In the case of asynchronous messages to a *service-controlled queue*, further processing is controlled by a *service* of the application. This type includes messages to a *TAC queue*, messages to a *USER queue* and messages to a *temporary queue*. The USER queue and the temporary queue must belong to the local application, whereas the TAC queue can be in both the local application and the remote application.

asynchronous program

Program unit started by a *background job*.

asynchronous service (KDCS)

Service which processes a *background job*. Processing is carried out independently of the job submitter. An asynchronous service can comprise one or more program units/transactions. It is started via an asynchronous *transaction code*.

audit (BS2000 systems)

During execution of a *UTM application*, UTM events which are of relevance in terms of security can be logged by *SAT* for auditing purposes.

authentication

See *system access control*.

authorization

See *data access control*.

Axis

See *Apache Axis*.

background job

Background jobs are *asynchronous jobs* destined for an *asynchronous service* of the current application or of a remote application. Background jobs are particularly suitable for time-intensive processing or processing which is not time-critical and where the results do not directly influence the current dialog.

basic format

Format in which terminal users can make all entries required to start a service.

basic job

Asynchronous job in a *job complex*.

browsing asynchronous messages

A *service* sequentially reads the *asynchronous messages* in a *service-controlled queue*. The messages are not locked while they are being read and they remain in the queue after they have been read. This means that they can be read simultaneously by different services.

bypass mode (BS2000 systems)

Operating mode of a printer connected locally to a terminal. In bypass mode, any *asynchronous message* sent to the printer is sent to the terminal and then redirected to the printer by the terminal without being displayed on screen.

cache

Used for buffering application data for all the processes of a *UTM application*. The cache is used to optimize access to the *page pool* and, in the case of UTM cluster applications, the *cluster page pool*.

CCR (Commitment, Concurrency and Recovery)

CCR is an Application Service Element (ASE) defined by OSI used for OSI TP communication which contains the protocol elements (services) related to the beginning and end (commit or rollback) of a *transaction*. CCR supports the two-phase commitment.

CCS name (BS2000 systems)

See *coded character set name*.

client

Clients of a *UTM application* can be:

- terminals
- UPIC client programs
- transport system applications (e.g. DCAM, PDN, CMX, socket applications or UTM applications which have been generated as *transport system applications*).

Clients are connected to the UTM application via LTERM partners.

Note: UTM clients which use the OpenCPIC carrier system are treated just like *OSI TP partners*.

client side of a conversation

This term has been superseded by *initiator*.

cluster

A number of computers connected over a fast network and which in many cases can be seen as a single computer externally. The objective of clustering is generally to increase the computing capacity or availability in comparison with a single computer.

cluster administration journal

The cluster administration journal consists of:

- two log files with the extensions JRN1 and JRN2 for global administration actions,
- the JKAA file which contains a copy of the KDCS Application Area (KAA). Administrative changes that are no longer present in the two log files are taken over from this copy.

The administration journal files serve to pass on to the other node applications those administrative actions that are to apply throughout the cluster to all node applications in a UTM cluster application.

cluster configuration file

File containing the central configuration data of a *UTM cluster application*. The cluster configuration file is created using the UTM generation tool *KDCDEF*.

cluster filebase

Filename prefix or directory name for the *UTM cluster files*.

cluster GSSB file

File used to administer GSSBs in a *UTM cluster application*. The cluster GSSB file is created using the UTM generation tool *KDCDEF*.

cluster lock file

File in a *UTM cluster application* used to manage cross-node locks of user data areas.

cluster page pool

The cluster page pool consists of an administration file and up to 10 files containing a *UTM cluster application's* user data that is available globally in the cluster (service data including LSSB, GSSB and ULS). The cluster page pool is created using the UTM generation tool *KDCDEF*.

cluster start serialization file

Lock file used to serialize the start-up of individual node applications (only on Unix, Linux and Windows systems).

cluster ULS file

File used to administer the ULS areas of a *UTM cluster application*. The cluster ULS file is created using the UTM generation tool *KDCDEF*.

cluster user file

File containing the user management data of a *UTM cluster application*. The cluster user file is created using the UTM generation tool *KDCDEF*.

coded character set name (BS2000 systems)

If the product *XHCS* (eXtended Host Code Support) is used, each character set used is uniquely identified by a coded character set name (abbreviation: "CCS name" or "CCSN").

cold start

Start of a *UTM application* after the application terminates normally (*normal termination*) or after a new generation (see also *warm start*).

communication area (KDCS)

KDCS *primary storage area*, secured by transaction logging and which contains service-specific data. The communication area comprises 3 parts:

- the KB header with general service data
- the KB return area for returning values to KDCS calls
- the KB program area for exchanging data between UTM program units within a single *service*.

communication end point

see *transport system end point*

communication resource manager

In distributed systems, communication resource managers (CRMs) control communication between the application programs. openUTM provides CRMs for the international OSI TP standard, for the LU6.1 industry standard and for the proprietary openUTM protocol UPIC.

configuration

Sum of all the properties of a *UTM application*. The configuration describes:

- application parameters and operating parameters
- the objects of an application and the properties of these objects. Objects can be *program units* and *transaction codes*, communication partners, printers, *user IDs*, etc.
- defined measures for controlling data and system access.

The configuration of a UTM application is defined at generation time (*static configuration*) and can be changed dynamically by the administrator (while the application is running, *dynamic configuration*). The configuration is stored in the *KDCFILE*.

confirmation job

Component of a *job complex* where the confirmation job is assigned to the *basic job*. There are positive and negative confirmation jobs. If the *basic job* returns a positive result, the positive confirmation job is activated, otherwise, the negative confirmation job is activated.

connection bundle

see *LTERM bundle*.

connection user ID

User ID under which a *TS application* or a *UPIC client* is signed on at the *UTM application* directly after the connection has been established. The following applies, depending on the client (= LTERM partner) generation:

- The connection user ID is the same as the USER in the LTERM statement (explicit connection user ID). An explicit connection user ID must be generated with a USER statement and cannot be used as a "genuine" *user ID*.
- The connection user ID is the same as the LTERM partner (implicit connection user ID) if no USER was specified in the LTERM statement or if an LTERM pool has been generated.

In a *UTM cluster application*, the service belonging to a connection user ID (RESTART=YES in LTERM or USER) is bound to the connection and is therefore local to the node.

A connection user ID generated with RESTART=YES can have a separate service in each *node application*.

contention loser

Every connection between two partners is managed by one of the partners. The partner that manages the connection is known as the *contention winner*. The other partner is the contention loser.

contention winner

A connection's contention winner is responsible for managing the connection. Jobs can be started by the contention winner or by the *contention loser*. If a conflict occurs, i.e. if both partners in the communication want to start a job at the same time, then the job stemming from the contention winner uses the connection.

conversation

In CPI-C, communication between two CPI-C application programs is referred to as a conversation. The communication partners in a conversation are referred to as the *initiator* and the *acceptor*.

conversation ID

CPI-C assigns a local conversation ID to each *conversation*, i.e. the *initiator* and *acceptor* each have their own conversation ID. The conversation ID uniquely assigns each CPI-C call in a program to a conversation.

CPI-C

CPI-C (**C**ommon **P**rogramming **I**nterface for **C**ommunication) is a program interface for program-to-program communication in open networks standardized by X/Open and CIW (**C**PI-C **I**mplementor's **W**orkshop).

The CPI-C implemented in openUTM complies with X/Open's CPI-C V2.0 CAE Specification. The interface is available in COBOL and C. In openUTM, CPI-C can communicate via the OSI TP, LU6.1 and UPIC protocols and with openUTM-LU62.

Cross Coupled System / XCS

Cluster of BS2000 computers with the *Highly Integrated System Complex Multiple System Control Facility* (HIPLEX[®] MSCF).

data access control

In data access control openUTM checks whether the communication partner is authorized to access a particular object belonging to the application. The access rights are defined as part of the configuration.

data space (BS2000 systems)

Virtual address space of BS2000 which can be employed in its entirety by the user. Only data and programs stored as data can be addressed in a data space; no program code can be executed.

dead letter queue

The dead letter queue is a TAC queue which has the fixed name KDCDLETQ. It is always available to save queued messages sent to transaction codes, TAC queues, LPAP or OSI-LPAP partners but which could not be processed. The saving of queued messages in the dead letter queue can be activated or deactivated for each message destination individually using the TAC, LPAP or OSI-LPAP statement's DEAD-LETTER-Q parameter.

DES

DES (Data Encryption Standard) is an international standard for encrypting data. One key is used in this method for encoding and decoding. If the DES method is used, the UPIC client generates a DES key for each session.

dialog conversation

CPI-C conversation in which both the *initiator* and the *acceptor* are permitted to send. A dialog transaction code for the *acceptor* must have been generated in the *UTM application*.

dialog job, interactive job

Job which starts a *dialog service*. The job can be issued by a *client* or, when two servers communicate with each other (*server-server communication*), by a different application.

dialog message

A message which requires a response or which is itself a response to a request. The request and the response both take place within a single service. The request and reply together form a dialog step.

dialog program

Program unit which partially or completely processes a *dialog step*.

dialog service

Service which processes a *job* interactively (synchronously) in conjunction with the job submitter (*client* or another server application). A dialog service processes *dialog messages* received from the job submitter and generates dialog messages to be sent to the job submitter. A dialog service comprises at least one *transaction*. In general, a dialog service encompasses at least one dialog step. Exception: in the event of *service chaining*, it is possible for more than one service to comprise a dialog step.

dialog step

A dialog step starts when a *dialog message* is received by the *UTM application*. It ends when the UTM application responds.

dialog terminal process (Unix , Linux and Windows systems)

A dialog terminal process connects a terminal of a Unix, Linux or Windows system with the work processes of the *UTM application*. Dialog terminal processes are started either when the user enters utmdtp or via the LOGIN shell. A separate dialog terminal process is required for each terminal to be connected to a UTM application.

distributed processing

Processing of *dialog jobs* by several different applications or the transfer of *background jobs* to another application. The higher-level protocols *LU6.1* and *OSI TP* are used for distributed processing. openUTM-LU62 also permits distributed processing with LU6.2 partners. A distinction is made between distributed processing with *distributed transactions* (transaction logging across different applications) and distributed processing without distributed transactions (local transaction logging only). Distributed processing is also known as server-server communication.

distributed transaction

Transaction which encompasses more than one application and is executed in several different (sub-)transactions in distributed systems.

distributed transaction processing

Distributed processing with *distributed transactions*.

dynamic configuration

Changes to the *configuration* made by the administrator. UTM objects such as *program units*, *transaction codes*, *clients*, *LU6.1 connections*, printers or *user IDs* can be added, modified or in some cases deleted from the configuration while the application is running. To do this, it is necessary to create separate *administration programs* which use the functions of the *program interface for administration*. The WinAdmin administration program or the WebAdmin administration program can be used to do this, or separate *administration programs* must be created that utilize the functions of the *administration program interface*.

encryption level

The encryption level specifies if and to what extent a client message and password are to be encrypted.

event-driven service

This term has been superseded by *event service*.

event exit

Routine in an application program which is started automatically whenever certain events occur (e.g. when a process is started, when a service is terminated). Unlike *event services*, an event exit must not contain any KDCS, CPI-C or XATMI calls.

event function

Collective term for *event exits* and *event services*.

event service

Service started when certain events occur, e.g. when certain UTM messages are issued. The *program units* for event-driven services must contain KDCS calls.

filebase

UTM application filebase

On BS2000 systems, filebase is the prefix for the *KDCFILE*, the *user log file* USLOG and the *system log file* SYSLOG.

On Unix, Linux and Windows systems, filebase is the name of the directory under which the *KDCFILE*, the user log file USLOG, the system log file SYSLOG and other files relating to the UTM application are stored.

Functional Unit (FU)

A subset of the *OSI TP* protocol providing a particular functionality. The OSI TP protocol is divided into the following functional units:

- Dialog
- Shared Control
- Polarized Control
- Handshake
- Commit
- Chained Transactions
- Unchained Transactions
- Recovery

Manufacturers implementing OSI TP need not include all functional units, but can concentrate on a subset instead. Communications between applications of two different OSI TP implementations is only possible if the included functional units are compatible with each other.

generation

See *UTM generation*.

global secondary storage area

See *secondary storage area*.

hardcopy mode

Operating mode of a printer connected locally to a terminal. Any message which is displayed on screen will also be sent to the printer.

heterogeneous link

In the case of *server-server communication*: a link between a *UTM application* and a non-UTM application, e.g. a CICS or TUXEDO application.

Highly Integrated System Complex / HIPLEX[®]

Product family for implementing an operating, load sharing and availability cluster made up of a number of BS2000 servers.

HIPLEX® MSCF

(MSCF = **M**ultiple **S**ystem **C**ontrol **F**acility)

Provides the infrastructure and basic functions for distributed applications with HIPLEX®.

homogeneous link

In the case of *server-server communication*, a link between two *UTM applications*. It is of no significance whether the applications are running on the same operating system platforms or on different platforms.

inbound conversation (CPI-C)

See *incoming conversation*.

incoming conversation (CPI-C)

A conversation in which the local CPI-C program is the *acceptor* is referred to as an incoming conversation. In the X/Open specification, the term "inbound conversation" is used synonymously with "incoming conversation".

initial KDCFILE

In a *UTM cluster application*, this is the *KDCFILE* generated by *KDCDEF* and which must be copied for each node application before the node applications are started.

initiator (CPI-C)

The communication partners in a *conversation* are referred to as the initiator and the *acceptor*. The initiator sets up the conversation with the CPI-C calls `Initialize_Conversation` and `Allocate`.

insert

Field in a message text in which openUTM enters current values.

inverse KDCDEF

A function which uses the dynamically adapted configuration data in the *KDCFILE* to generate control statements for a *KDCDEF* run. An inverse KDCDEF can be started "offline" under *KDCDEF* or "online" via the *program interface for administration*.

IUTMDB

Interface used for the coordinated interaction with resource managers on BS2000 systems. This includes data repositories (LEASY) and data base systems (SESAM/SQL, UDS/SQL).

JConnect client

Designation for clients based on the product openUTM-JConnect. The communication with the UTM application is carried out via the *UPIC protocol*.

JDK

Java Development Kit

Standard development environment from Oracle Corporation for the development of Java applications.

job

Request for a *service* provided by a *UTM application*. The request is issued by specifying a transaction code. See also: *queued output job*, *dialog job*, *background job*, *job complex*.

job complex

Job complexes are used to assign *confirmation jobs* to *asynchronous jobs*. An asynchronous job within a job complex is referred to as a *basic job*.

job-receiving service (KDCS)

A job-receiving service is a *service* started by a *job-submitting service* of another server application.

job-submitting service (KDCS)

A job-submitting service is a *service* which requests another service from a different server application (*job-receiving service*) in order to process a job.

KDCADM

Standard administration program supplied with openUTM. KDCADM provides administration functions which are called with transaction codes (*administration commands*).

KDCDEF

UTM tool for the *generation* of *UTM applications*. KDCDEF uses the configuration information in the KDCDEF control statements to create the UTM objects *KDCFILE* and the ROOT table sources for the main routine *KDCROOT*.

In UTM cluster applications, KDCDEF also creates the *cluster configuration file*, the *cluster user file*, the *cluster page pool*, the *cluster GSSB file* and the *cluster ULS file*.

KDCFILE

One or more files containing data required for a *UTM application* to run. The KDCFILE is created with the UTM generation tool *KDCDEF*. Among other things, it contains the *configuration* of the application.

KDCROOT

Main routine of an *application program* which forms the link between the *program units* and the UTM system code. KDCROOT is linked with the *program units* to form the *application program*.

KDCS message area

For KDCS calls: buffer area in which messages or data for openUTM or for the *program unit* are made available.

KDCS parameter area

See *parameter area*.

KDCS program interface

Universal UTM program interface compliant with the national DIN 66 265 standard and which includes some extensions. KDCS (compatible data communications interface) allows dialog services to be created, for instance, and permits the use of *message queuing* functions. In addition, KDCS provides calls for *distributed processing*.

Kerberos

Kerberos is a standardized network authentication protocol (RFC1510) based on encryption procedures in which no passwords are sent to the network in clear text.

Kerberos principal

Owner of a key.

Kerberos uses symmetrical encryption, i.e. all the keys are present at two locations, namely with the key owner (principal) and the KDC (Key Distribution Center).

key code

Code that represents specific access authorization or a specific role. Several key codes are grouped into a *key set*.

key set

Group of one or more *key codes* under a particular a name. A key set defines authorization within the framework of the authorization concept used (lock/key code concept or *access list* concept). A key set can be assigned to a *user ID*, an *LTERM partner* an *(OSI) LPAP partner*, a *service* or a *TAC queue*.

linkage program

See *KDCROOT*.

local secondary storage area

See *secondary storage area*.

Log4j

Log4j is part of the Apache Jakarta project. Log4j provides information for logging information (runtime information, trace records, etc.) and configuring the log output. *WS4UTM* uses the software product Log4j for trace and logging functionality.

lock code

Code protecting an LTERM partner or transaction code against unauthorized access. Access is only possible if the *key set* of the accesser contains the appropriate *key code* (lock/key code concept).

logging process

Process in Unix, Linux and Windows systems that controls the logging of account records or monitoring data.

LPAP bundle

LPAP bundles allow messages to be distributed to LPAP partners across several partner applications. If a UTM application has to exchange a very large number of messages with a partner application then load distribution may be improved by starting multiple instances of the partner application and distributing the messages across the individual instances. In an LPAP bundle, openUTM is responsible for distributing the messages to the partner application instances. An LPAP bundle consists of a master LPAP and multiple slave LPAPs. The slave LPAPs are assigned to the master LPAP on UTM generation. LPAP bundles exist for both the OSI TP protocol and the LU6.1 protocol.

LPAP partner

In the case of *distributed processing* via the *LU6.1* protocol, an LPAP partner for each partner application must be configured in the local application. The LPAP partner represents the partner application in the local application. During communication, the partner application is addressed by the name of the assigned LPAP partner and not by the application name or address.

LTERM bundle

An LTERM bundle (connection bundle) consists of a master LTERM and multiple slave LTERMs. An LTERM bundle (connection bundle) allows you to distribute queued messages to a logical partner application evenly across multiple parallel connections.

LTERM group

An LTERM group consists of one or more alias LTERMs, the group LTERMs and a primary LTERM. In an LTERM group, you assign multiple LTERMs to a connection.

LTERM partner

LTERM partners must be configured in the application if you want to connect clients or printers to a *UTM application*. A client or printer can only be connected if an LTERM partner with the appropriate properties is assigned to it. This assignment is generally made in the *configuration*, but can also be made dynamically using terminal pools.

LTERM pool

The TPOOL statement allows you to define a pool of LTERM partners instead of issuing one LTERM and one PTERM statement for each *client*. If a client establishes a connection via an LTERM pool, an LTERM partner is assigned to it dynamically from the pool.

LU6.1

Device-independent data exchange protocol (industrial standard) for transaction-oriented *server-server communication*.

LU6.1-LPAP bundle

LPAP bundle for *LU6.1* partner applications.

LU6.1 partner

Partner of the *UTM application* that communicates with the UTM application via the *LU6.1* protocol. Examples of this type of partner are:

- a UTM application that communicates via LU6.1
- an application in the IBM environment (e.g. CICS, IMS or TXSeries) that communicates via LU6.1

main process (Unix /Linux / Windows systems)

Process which starts the *UTM application*. It starts the *work processes*, the *UTM system processes*, *printer processes*, *network processes*, *logging process* and the *timer process* and monitors the *UTM application*.

main routine KDCROOT

See *KDCROOT*.

management unit

SE Servers component, in combination with the *SE Manager*, permits centralized, web-based management of all the units of an SE server.

message definition file

The message definition file is supplied with openUTM and, by default, contains the UTM message texts in German and English together with the definitions of the message properties. Users can take this file as a basis for their own message modules.

message destination

Output medium for a *message*. Possible message destinations for a message from the openUTM transaction monitor include, for instance, terminals, *TS applications*, the *event service* MSGTAC, the *system log file* SYSLOG or *TAC queues, asynchronous TACs, USER queues, SYSOUT/SYSLST* or *stderr/stdout*.

The message destinations for the messages of the UTM tools are SYSOUT/SYSLST and *stderr/stdout*.

message queue

Queue in which specific messages are kept with transaction management until further processed. A distinction is drawn between *service-controlled queues* and *UTM-controlled queues*, depending on who monitors further processing.

message queuing

Message queuing (MQ) is a form of communication in which the messages are exchanged via intermediate queues rather than directly. The sender and recipient can be separated in space or time. The transfer of the message is independent of whether a network connection is available at the time or not. In openUTM there are *UTM-controlled queues* and *service-controlled queues*.

MSGTAC

Special event service that processes messages with the message destination MSGTAC by means of a program. MSGTAC is an asynchronous service and is created by the operator of the application.

multiplex connection (BS2000 systems)

Special method offered by *OMNIS* to connect terminals to a *UTM application*. A multiplex connection enables several terminals to share a single transport connection.

multi-step service (KDCS)

Service carried out in a number of *dialog steps*.

multi-step transaction

Transaction which comprises more than one *processing step*.

Network File System/Service / NFS

Allows Unix systems to access file systems across the network.

network process (Unix / Linux / Windows systems)

A process in a *UTM application* for connection to the network.

network selector

The network selector identifies a service access point to the network layer of the *OSI reference model* in the local system.

node

Individual computer of a *cluster*.

node application

UTM application that is executed on an individual *node* as part of a *UTM cluster application*.

node bound service

A node bound service belonging to a user can only be continued at the node application at which the user was last signed on. The following services are always node bound:

- Services that have started communications with a job receiver via LU6.1 or OSI TP and for which the job-receiving service has not yet been terminated
- Inserted services in a service stack
- Services that have completed a SESAM transaction

In addition, a user's service is node bound as long as the user is signed-on at a node application.

node filebase

Filename prefix or directory name for the *node application's KDCFILE*, *user log file* and *system log file*.

node recovery

If a node application terminates abnormally and no rapid warm start of the application is possible on its associated *node computer* then it is possible to perform a node recovery for this node on another node in the UTM cluster. In this way, it is possible to release locks resulting from the failed node application in order to prevent unnecessary impairments to the running *UTM cluster application*.

normal termination of a UTM application

Controlled termination of a *UTM application*. Among other things, this means that the administration data in the *KDCFILE* are updated. The *administrator* initiates normal termination (e.g. with *KDCSHUT N*). After a normal termination, openUTM carries out any subsequent start as a *cold start*.

object identifier

An object identifier is an identifier for objects in an OSI environment which is unique throughout the world. An object identifier comprises a sequence of integers which represent a path in a tree structure.

OMNIS (BS2000 systems)

OMNIS is a "session manager" which lets you set up connections from one terminal to a number of partners in a network concurrently. OMNIS also allows you to work with multiplex connections.

online import

In a *UTM cluster application*, online import refers to the import of application data from a normally terminated node application into a running node application.

online update

In a *UTM cluster application*, online update refers to a change to the application configuration or the application program or the use of a new UTM revision level while a *UTM cluster application* is running.

open terminal pool

Terminal pool which is not restricted to clients of a single computer or particular type. Any client for which no computer- or type-specific terminal pool has been generated can connect to this terminal pool.

OpenCPIC

Carrier system for UTM clients that use the *OSI TP* protocol.

OpenCPIC client

OSI TP partner application with the *OpenCPIC* carrier system.

openSM2

The openSM2 product line offers a consistent solution for the enterprise-wide performance management of server and storage systems. openSM2 offers the acquisition of monitoring data, online monitoring and offline evaluation.

openUTM cluster

From the perspective of UPIC clients, **not** from the perspective of the server: Combination of several node applications of a UTM cluster application to form one logical application that is addressed via a common symbolic destination name.

openUTM-D

openUTM-D (openUTM distributed) is a component of openUTM which allows *distributed processing*. openUTM-D is an integral component of openUTM.

OSI-LPAP bundle

LPAP bundle for *OSI TP* partner applications.

OSI-LPAP partner

OSI-LPAP partners are the addresses of the *OSI TP partners* generated in openUTM. In the case of *distributed processing* via the *OSI TP* protocol, an OSI-LPAP partner for each partner application must be configured in the local application. The OSI-LPAP partner represents the partner application in the local application. During communication, the partner application is addressed by the name of the assigned OSI-LPAP partner and not by the application name or address.

OSI reference model

The OSI reference model provides a framework for standardizing communications in open systems. ISO, the International Organization for Standardization, described this model in the ISO IS7498 standard. The OSI reference model divides the necessary functions for system communication into seven logical layers. These layers have clearly defined interfaces to the neighboring layers.

OSI TP

Communication protocol for distributed transaction processing defined by ISO. OSI TP stands for Open System Interconnection Transaction Processing.

OSI TP partner

Partner of the UTM application that communicates with the UTM application via the OSI TP protocol. Examples of such partners are:

- a UTM application that communicates via OSI TP
- an application in the IBM environment (e.g. CICS) that is connected via openUTM-LU62
- an *OpenCPIC client*
- applications from other TP monitors that support OSI TP

outbound conversation (CPI-C)

See *outgoing conversation*.

outgoing conversation (CPI-C)

A conversation in which the local CPI-C program is the *initiator* is referred to as an outgoing conversation. In the X/Open specification, the term “outbound conversation” is used synonymously with “outgoing conversation”.

page pool

Part of the *KDCFILE* in which user data is stored.

In a *standalone application* this data consists, for example, of *dialog messages*, messages sent to *message queues*, *secondary memory areas*.

In a UTM cluster application, it consists, for example, of messages to *message queues*, *TLS*.

parameter area

Data structure in which a program unit passes the operands required for a UTM call to openUTM.

partner application

Partner of a UTM application during *distributed processing*. Higher communication protocols are used for distributed processing (*LU6.1*, *OSI TP* or *LU6.2* via the openUTM-LU62 gateway).

postselection (BS2000 systems)

Selection of logged UTM events from the SAT logging file which are to be evaluated. Selection is carried out using the SATUT tool.

prepare to commit (PTC)

Specific state of a distributed transaction

Although the end of the distributed transaction has been initiated, the system waits for the partner to confirm the end of the transaction.

preselection (BS2000 systems)

Definition of the UTM events which are to be logged for the *SAT audit*. Preselection is carried out with the UTM-SAT administration functions. A distinction is made between event-specific, user-specific and job-specific (TAC-specific) preselection.

presentation selector

The presentation selector identifies a service access point to the presentation layer of the *OS/ reference model* in the local system.

primary storage area

Area in main memory to which the *KDCS program unit* has direct access, e.g. *standard primary working area, communication area*.

print administration

Functions for *print control* and the administration of *queued output jobs*, sent to a printer.

print control

openUTM functions for controlling print output.

printer control LTERM

A printer control LTERM allows a client or terminal user to connect to a UTM application. The printers assigned to the printer control LTERM can then be administered from the client program or the terminal. No administration rights are required for these functions.

printer control terminal

This term has been superseded by *printer control LTERM*.

printer group (Unix systems)

For each printer, a Unix system sets up one printer group by default that contains this one printer only. It is also possible to assign several printers to one printer group or to assign one printer to several different printer groups.

printer pool

Several printers assigned to the same *LTERM partner*.

printer process (Unix / Linux systems)

Process set up by the *main process* for outputting *asynchronous messages* to a *printer group*. The process exists as long as the printer group is connected to the *UTM application*. One printer process exists for each connected printer group.

process

The openUTM manuals use the term “process” as a collective term for processes (Unix / Linux / Windows systems) and tasks (BS2000 systems).

processing step

A processing step starts with the receipt of a *dialog message* sent to the *UTM application* by a *client* or another server application. The processing step ends either when a response is sent, thus also terminating the *dialog step*, or when a dialog message is sent to a third party.

program interface for administration

UTM program interface which helps users to create their own *administration programs*. Among other things, the program interface for administration provides functions for *dynamic configuration*, for modifying properties and application parameters and for querying information on the configuration and the current workload of the application.

program space (BS2000 systems)

Virtual address space of BS2000 which is divided into memory classes and in which both executable programs and pure data are addressed.

program unit

UTM *services* are implemented in the form of one or more program units. The program units are components of the *application program*. Depending on the employed API, they may have to contain KDCS, XATMI or CPIC calls. They can be addressed using *transaction codes*. Several different transaction codes can be assigned to a single program unit.

queue

See *message queue*.

queued output job

Queued output jobs are *asynchronous jobs* which output a message, such as a document, to a printer, a terminal or a transport system application.

Queued output jobs are processed by UTM system functions exclusively, i.e. it is not necessary to create program units to process them.

Quick Start Kit

A sample application supplied with openUTM (Windows systems).

redelivery

Repeated delivery of an *asynchronous message* that could not be processed correctly because, for example, the *transaction* was rolled back or the *asynchronous service* was terminated abnormally.

The message is returned to the message queue and can then be read and/or processed again.

reentrant program

Program whose code is not altered when it runs. On BS2000 systems this constitutes a prerequisite for using *shared code*.

request

Request from a *client* or another server for a *service function*.

requestor

In XATMI, the term requestor refers to an application which calls a service.

resource manager

Resource managers (RMs) manage data resources. Database systems are examples of resource managers. openUTM, however, also provides its own resource managers for accessing message queues, local memory areas and logging files, for instance. Applications access RMs via special resource manager interfaces. In the case of database systems, this will generally be SQL and in the case of openUTM RMs, it is the KDCS interface.

restart

See *screen restart*.

see *service restart*.

RFC1006

A protocol defined by the IETF (Internet Engineering Task Force) belonging to the TCP/IP family that implements the ISO transport services (transport class 0) based on TCP/IP.

RSA

Abbreviation for the inventors of the RSA encryption method (Rivest, Shamir and Adleman). This method uses a pair of keys that consists of a public key and a private key. A message is encrypted using the public key, and this message can only be decrypted using the private key. The pair of RSA keys is created by the UTM application.

SAT audit (BS2000 systems)

Audit carried out by the SAT (Security Audit Trail) component of the BS2000 software product SECOS.

screen restart

If a *dialog service* is interrupted, openUTM again displays the *dialog message* of the last completed *transaction* on screen when the service restarts provided that the last transaction output a message on the screen.

SE manager

Web-based graphical user interface (GUI) for the SE series of Business Servers. SE Manager runs on the *management unit* and permits the central operation and administration of server units (with /390 architecture and/or x86 architecture), application units (x86 architecture), net unit and peripherals.

SE server

A Business Server from Fujitsu's SE series.

secondary storage area

Memory area secured by transaction logging and which can be accessed by the KDCS *program unit* with special calls. Local secondary storage areas (LSSBs) are assigned to one *service*. Global secondary storage areas (GSSBs) can be accessed by all services in a *UTM application*. Other secondary storage areas include the *terminal-specific long-term storage (TLS)* and the *user-specific long-term storage (ULS)*.

selector

A selector identifies a service access point to services of one of the layers of the *OSI reference model* in the local system. Each selector is part of the address of the access point.

semaphore (Unix / Linux / Windows systems)

Unix, Linux and Windows systems resource used to control and synchronize processes.

server

A server is an *application* which provides *services*. The computer on which the applications are running is often also referred to as the server.

server-server communication

See *distributed processing*.

server side of a conversation (CPI-C)

This term has been superseded by *acceptor*.

service

Services process the *jobs* that are sent to a server application. A service of a UTM application comprises one or more transactions. The service is called with the *service TAC*. Services can be requested by *clients* or by other servers.

service access point

In the OSI reference model, a layer has access to the services of the layer below at the service access point. In the local system, the service access point is identified by a *selector*. During communication, the *UTM application* links up to a service access point. A connection is established between two service access points.

service chaining (KDCS)

When service chaining is used, a follow-up service is started without a *dialog message* specification after a *dialog service* has completed.

service-controlled queue

Message queue in which the calling and further processing of messages is controlled by *services*. A service must explicitly issue a KDCS call (DGET) to read the message. There are service-controlled queues in openUTM in the variants *USER queue*, *TAC queue* and *temporary queue*.

service restart (KDCS)

If a service is interrupted, e.g. as a result of a terminal user signing off or a *UTM application* being terminated, openUTM carries out a *service restart*. An *asynchronous service* is restarted or execution is continued at the most recent *synchronization point*, and a *dialog service* continues execution at the most recent *synchronization point*. As far as the terminal user is concerned, the service restart for a dialog service appears as a *screen restart* provided that a dialog message was sent to the terminal user at the last synchronization point.

service routine

See *program unit*.

service stacking (KDCS)

A terminal user can interrupt a running *dialog service* and insert a new dialog service. When the inserted *service* has completed, the interrupted service continues.

service TAC (KDCS)

Transaction code used to start a *service*.

session

Communication relationship between two addressable units in the network via the SNA protocol *LU6.1*.

session selector

The session selector identifies an *access point* in the local system to the services of the session layer of the *OSI reference model*.

shared code (BS2000 systems)

Code which can be shared by several different processes.

shared memory

Virtual memory area which can be accessed by several different processes simultaneously.

shared objects (Unix / Linux / Windows systems)

Parts of the *application program* can be created as shared objects. These objects are linked to the application dynamically and can be replaced during live operation. Shared objects are defined with the KDCDEF statement SHARED-OBJECT.

sign-on check

See *system access control*.

sign-on service (KDCS)

Special *dialog service* for a user in which *program units* control how a user signs on to a UTM application.

single-step service

Dialog service which encompasses precisely one *dialog step*.

single-step transaction

Transaction which encompasses precisely one *dialog step*.

SOA

(Service-Oriented Architecture)

SOA is a system architecture concept in which functions are implemented in the form of re-usable, technically independent, loosely coupled *services*. Services can be called independently of the underlying implementations via interfaces which may possess public and, consequently, trusted specifications. Service interaction is performed via a communication infrastructure made available for this purpose.

SOAP

SOAP (Simple Object Access Protocol) is a protocol used to exchange data between systems and run remote procedure calls. SOAP also makes use of the services provided by other standards, XML for the representation of the data and Internet transport and application layer protocols for message transfer.

socket connection

Transport system connection that uses the socket interface. The socket interface is a standard program interface for communication via TCP/IP.

standalone application

See *standalone UTM application*.

standalone UTM application

Traditional *UTM application* that is not part of a *UTM cluster application*.

standard primary working area (KDCS)

Area in main memory available to all KDCS *program units*. The contents of the area are either undefined or occupied with a fill character when the program unit starts execution.

start format

Format output to a terminal by openUTM when a user has successfully signed on to a *UTM application* (except after a *service restart* and during sign-on via the *sign-on service*).

static configuration

Definition of the *configuration* during generation using the UTM tool *KDCDEF*.

SYSLOG file

See *system log file*.

synchronization point, consistency point

The end of a *transaction*. At this time, all the changes made to the *application information* during the transaction are saved to prevent loss in the event of a crash and are made visible to others. Any locks set during the transaction are released.

system access control

A check carried out by openUTM to determine whether a certain *user ID* is authorized to work with the *UTM application*. The authorization check is not carried out if the UTM application was generated without user IDs.

system log file

File or file generation to which openUTM logs all UTM messages for which SYSLOG has been defined as the *message destination* during execution of a *UTM application*.

TAC

See *transaction code*.

TAC queue

Message queue generated explicitly by means of a KDCDEF statement. A TAC queue is a *service-controlled queue* that can be addressed from any service using the generated name.

temporary queue

Message queue created dynamically by means of a program that can be deleted again by means of a program (see *service-controlled queue*).

terminal-specific long-term storage (KDCS)

Secondary storage area assigned to an *LTERM*, *LPAP* or *OSI-PAP partner* and which is retained after the application has terminated.

time-driven job

Job which is buffered by openUTM in a *message queue* up to a specific time until it is sent to the recipient. The recipient can be an *asynchronous service* of the same application, a *TAC queue*, a partner application, a terminal or a printer. Time-driven jobs can only be issued by *KDCS program units*.

timer process (Unix / Linux / Windows systems)

Process which accepts jobs for controlling the time at which *work processes* are executed. It does this by entering them in a job list and releasing them for processing after a time period defined in the job list has elapsed.

TLS termination proxy

A TLS termination proxy is a [proxy server](#) that is used to handle incoming [TLS](#) connections, decrypting the data and passing on the unencrypted request to other servers.

TNS (Unix / Linux / Windows systems)

Abbreviation for the Transport Name Service. TNS assigns a transport selector and a transport system to an application name. The application can be reached through the transport system.

Tomcat

see *Apache Tomcat*

transaction

Processing section within a *service* for which adherence to the *ACID properties* is guaranteed. If, during the course of a transaction, changes are made to the *application information*, they are either made consistently and in their entirety or not at all (all-or-nothing rule). The end of the transaction forms a *synchronization point*.

transaction code/TAC

Name which can be used to identify a *program unit*. The transaction code is assigned to the program unit during *static* or *dynamic configuration*. It is also possible to assign more than one transaction code to a program unit.

transaction rate

Number of *transactions* successfully executed per unit of time.

transfer syntax

With *OSI TP*, the data to be transferred between two computer systems is converted from the local format into transfer syntax. Transfer syntax describes the data in a neutral format which can be interpreted by all the partners involved. An *Object Identifier* must be assigned to each transfer syntax.

transport connection

In the *OSI reference model*, this is a connection between two entities of layer 4 (transport layer).

transport layer security

Transport layer security is a hybrid encryption protocol for secure data transmission in the Internet.

transport selector

The transport selector identifies a service access point to the transport layer of the *OSI reference model* in the local system.

transport system access point

See transport system end point.

transport system application

Application which is based directly on a transport system interface (e.g. CMX, DCAM or socket). When transport system applications are connected, the partner type APPLI or SOCKET must be specified during *configuration*. A transport system application cannot be integrated in a *distributed transaction*.

transport system end point

Client/server or server/server communication establishes a connection between two transport system end points. A transport system end point is also referred to as a local application name and is defined using the BCAMAPPL statement or MAX APPLINAME.

TS application

See *transport system application*.

typed buffer (XATMI)

Buffer for exchanging typed and structured data between communication partners. Typed buffers ensure that the structure of the exchanged data is known to both partners implicitly.

UPIC

Carrier system for openUTM clients. UPIC stands for Universal Programming Interface for Communication. The communication with the UTM application is carried out via the *UPIC protocol*.

UPIC Analyzer

Component used to analyze the UPIC communication recorded with *UPIC Capture*. This step is used to prepare the recording for playback using *UPIC Replay*.

UPIC Capture

Used to record communication between UPIC clients and UTM applications so that this can be replayed subsequently (*UPIC Replay*).

UPIC client

The designation for openUTM clients with the UPIC carrier system and for *JConnect clients*.

UPIC protocol

Protocol for the client server communication with *UTM applications*. The UPIC protocol is used by *UPIC clients* and *JConnect clients*.

UPIC Replay

Component used to replay the UPIC communication recorded with *UPIC Capture* and prepared with *UPIC Analyzer*.

user exit

This term has been superseded by *event exit*.

user ID

Identifier for a user defined in the *configuration* for the *UTM application* (with an optional password for *system access control*) and to whom special data access rights (*system access control*) have been assigned. A terminal user must specify this ID (and any password which has been assigned) when signing on to the UTM application. On BS2000 systems, system access control is also possible via *Kerberos*.

For other clients, the specification of a user ID is optional, see also *connection user ID*.

UTM applications can also be generated without user IDs.

user log file

File or file generation to which users write variable-length records with the KDCS LPUT call. The data from the KB header of the *KDCS communication area* is prefixed to every record. The user log file is subject to transaction management by openUTM.

USER queue

Message queue made available to every user ID by openUTM. A USER queue is a *service-controlled queue* and is always assigned to the relevant user ID. You can restrict the access of other UTM users to your own USER queue.

user-specific long-term storage

Secondary storage area assigned to a *user ID*, a *session* or an *association* and which is retained after the application has terminated.

USLOG file

See *user log file*.

UTM application

A UTM application provides *services* which process jobs from *clients* or other applications. openUTM is responsible for transaction logging and for managing the communication and system resources. From a technical point of view, a UTM application is a process group which forms a logical server unit at runtime.

UTM client

See *client*.

UTM cluster application

UTM application that has been generated for use on a cluster and that can be viewed logically as a **single** application.

In physical terms, a UTM cluster application is made up of several identically generated UTM applications running on the individual cluster *nodes*.

UTM cluster files

Blanket term for all the files that are required for the execution of a UTM cluster application on Unix, Linux and Windows systems. This includes the following files:

- *Cluster configuration file*
- *Cluster user file*
- Files belonging to the *cluster page pool*
- *Cluster GSSB file*
- *Cluster ULS file*
- Files belonging to the *cluster administration journal**
- *Cluster lock file**
- Lock file for start serialization*

The files indicated by * are created when the first node application is started. All the other files are created on generation using KDCDEF.

UTM-controlled queue

Message queues in which the calling and further processing of messages is entirely under the control of openUTM. See also *asynchronous job*, *background job* and *asynchronous message*.

UTM-D

See *openUTM-D*.

UTM-F

UTM applications can be generated as UTM-F applications (UTM fast). In the case of UTM-F applications, input from and output to hard disk is avoided in order to increase performance. This affects input and output which *UTM-S* uses to save user data and transaction data. Only changes to the administration data are saved.

In UTM cluster applications that are generated as UTM-F applications (APPLI-MODE=FAST), application data that is valid throughout the cluster is also saved. In this case, GSSB and ULS data is treated in exactly the same way as in UTM cluster applications generated with UTM-S. However, service data relating to users with RESTART=YES is written only when the relevant user signs off and not at the end of each transaction.

UTM generation

Static configuration of a UTM application using the UTM tool KDCDEF and creation of an application program.

UTM message

Messages are issued to *UTM message destinations* by the openUTM transaction monitor or by UTM tools (such as *KDCDEF*). A message comprises a message number and a message text, which can contain *inserts* with current values. Depending on the message destination, either the entire message is output or only certain parts of the message, such as the inserts).

UTM page

A UTM page is a unit of storage with a size of either 2K, 4K or 8 K. In *standalone UTM applications*, the size of a UTM page on generation of the UTM application can be set to 2K, 4K or 8 K. The size of a UTM page in a *UTM cluster application* is always 4K or 8 K. The *page pool* and the restart area for the KDCFILE and *UTM cluster files* are divided into units of the size of a UTM page.

utmpath (Unix / Linux / Windows systems)

The directory under which the openUTM components are installed is referred to as *utmpath* in this manual.

To ensure that openUTM runs correctly, the environment variable UTMPATH must be set to the value of *utmpath*. On Unix and Linux systems, you must set UTMPATH before a UTM application is started. On Windows systems UTMPATH is set in accordance with the UTM version installed most recently.

UTM-S

In the case of UTM-S applications, openUTM saves all user data as well as the administration data beyond the end of an application and any system crash which may occur. In addition, UTM-S guarantees the security and consistency of the application data in the event of any malfunction. UTM applications are usually generated as UTM-S applications (UTM secure).

UTM SAT administration (BS2000 systems)

UTM SAT administration functions control which UTM events relevant to security which occur during operation of a *UTM application* are to be logged by *SAT*. Special authorization is required for UTM SAT administration.

UTM socket protocol (USP)

Proprietary openUTM protocol above TCP/IP for the transformation of the Socket interface received byte streams in messages.

UTM system process

UTM process that is started in addition to the processes specified via the start parameters and which only handles selected jobs. UTM system processes ensure that UTM applications continue to be reactive even under very high loads.

UTM terminal

This term has been superseded by *LTERM partner*.

UTM tool

Program which is provided together with openUTM and which is needed for UTM specific tasks (e.g for configuring).

virtual connection

Assignment of two communication partners.

warm start

Start of a *UTM-S* application after it has terminated abnormally. The *application information* is reset to the most recent consistent state. Interrupted *dialog services* are rolled back to the most recent *synchronization point*, allowing processing to be resumed in a consistent state from this point (*service restart*). Interrupted *asynchronous services* are rolled back and restarted or restarted at the most recent *synchronization point*.

For *UTM-F* applications, only configuration data which has been dynamically changed is rolled back to the most recent consistent state after a restart due to a preceding abnormal termination.

In UTM cluster applications, the global locks applied to GSSB and ULS on abnormal termination of this node application are released. In addition, users who were signed on at this node application when the abnormal termination occurred are signed off.

WebAdmin

Web-based tool for the administration of openUTM applications via a Web browser. WebAdmin includes not only the full function scope of the *administration program interface* but also additional functions.

Web service

Application which runs on a Web server and is (publicly) available via a standardized, programmable interface. Web services technology makes it possible to make UTM program units available for modern Web client applications independently of the programming language in which they were developed.

WinAdmin

Java-based tool for the administration of openUTM applications via a graphical user interface. WinAdmin includes not only the full function scope of the *administration program interface* but also additional functions.

work process (Unix / Linux / Windows systems)

A process within which the *services* of a *UTM application* run.

workload capture & replay

Family of programs used to simulate load situations; consisting of the main components *UPIC Capture*, *UPIC Analyzer* and *Upic Replay* and - on Unix, Linux and Windows systems - the utility program *kdcsort*. Workload Capture & Replay can be used to record UPIC sessions with UTM applications, analyze these and then play them back with modified load parameters.

WS4UTM

WS4UTM (**WebServices** for open**UTM**) provides you with a convenient way of making a service of a UTM application available as a Web service.

XATMI

XATMI (X/Open Application Transaction Manager Interface) is a program interface standardized by X/Open for program-program communication in open networks.

The XATMI interface implemented in openUTM complies with X/Open's XATMI CAE Specification. The interface is available in COBOL and C. In openUTM, XATMI can communicate via the OSI TP, *LU6.1* and UPIC protocols.

XHCS (BS2000 systems)

XHCS (Extended Host Code Support) is a BS2000 software product providing support for international character sets.

XML

XML (eXtensible Markup Language) is a metalanguage standardized by the W3C (WWW Consortium) in which the interchange formats for data and the associated information can be defined.

14 Abbreviations

Please note: Some of the abbreviations used here derive from the German acronyms used in the original German product(s).

ACSE	Association Control Service Element
AEQ	Application Entity Qualifier
AES	Advanced Encryption Standard
AET	Application Entity Title
APT	Application Process Title
ASCII	American Standard Code for Information Interchange
ASE	Application Service Element
Axis	Apache eXtensible Interaction System
BCAM	Basic Communication Access Method
BER	Basic Encoding Rules
BLS	Binder - Loader - Starter (BS2000 systems)
CCP	Communication Control Program
CCR	Commitment, Concurrency and Recovery
CCS	Coded Character Set
CCSN	Coded Character Set Name
CICS	Customer Information Control System
CID	Control Identification
CMX	Communication Manager in Unix, Linux and Windows Systems
COM	Component Object Model
CPI-C	Common Programming Interface for Communication
CRM	Communication Resource Manager
CRTE	Common Runtime Environment (BS2000 systems)
DB	Database
DBH	Database Handler
DC	Data Communication
DCAM	Data Communication Access Method
DES	Data Encryption Standard

DLM	Distributed Lock Manager (BS2000 systems)
DMS	Data Management System
DNS	Domain Name Service
DP	Distributed Processing
DSS	Terminal (Datensichtstation)
DTD	Document Type Definition
DTP	Distributed Transaction Processing
EBCDIC	Extended Binary-Coded Decimal Interchange Code
EJB	Enterprise JavaBeans™
FGG	File Generation Group
FHS	Format Handling System
FT	File Transfer
GCM	Galois/Counter Mode
GSSB	Global Secondary Storage Area
HIPLEX®	Highly Integrated System Complex (BS2000 systems)
HLL	High-Level Language
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IFG	Interactive Format Generator
ILCS	Inter-Language Communication Services (BS2000 systems)
IMS	Information Management System (IBM)
IPC	Inter-Process Communication
IRV	International Reference Version
ISO	International Organization for Standardization
Java EE	Java Platform, Enterprise Edition
JCA	Java EE Connector Architecture
JDK	Java Development Kit
KAA	KDCS Application Area
KB	Communication Area

KBPRG	KB Program Area
KDCADMI	KDC Administration Interface
KDCS	Compatible Data Communication Interface
KTA	KDCS Task Area
LAN	Local Area Network
LCF	Local Configuration File
LLM	Link and Load Module (BS2000 systems)
LSSB	Local Secondary Storage Area
LU	Logical Unit
MQ	Message Queuing
MSCF	Multiple System Control Facility (BS2000 systems)
NB	Message Area
NEA	Network Architecture for BS2000 Systems
NFS	Network File System/Service
NLS	Native Language Support
OLTP	Online Transaction Processing
OML	Object Module Library
OSI	Open System Interconnection
OSI TP	Open System Interconnection Transaction Processing
OSS	OSI Session Service
PCMX	Portable Communication Manager
PID	Process Identification
PIN	Personal Identification Number
PLU	Primary Logical Unit
PTC	Prepare to commit
RAV	Computer Center Accounting Procedure
RDF	Resource Definition File
RM	Resource Manager
RSA	Encryption algorithm according to Rivest, Shamir, Adleman
RSO	Remote SPOOL Output (BS2000 systems)

RTS	Runtime System
SAT	Security Audit Trail (BS2000 systems)
SECOS	Security Control System
SEM	SE Manager
SGML	Standard Generalized Markup Language
SLU	Secondary Logical Unit
SM2	Software Monitor 2
SNA	Systems Network Architecture
SOA	Service-oriented Architecture
SOAP	Simple Object Access Protocol
SPAB	Standard Primary Working Area
SQL	Structured Query Language
SSB	Secondary Storage Area
SSL	Secure Socket Layer
SSO	Single Sign-On
TAC	Transaction Code
TCEP	Transport Connection End Point
TCP/IP	Transport Control Protocol / Internet Protocol
TIAM	Terminal Interactive Access Method
TLS	Terminal-Specific Long-Term Storage
TLS	Transport Layer Security
TM	Transaction Manager
TNS	Transport Name Service
TP	Transaction Processing (Transaction Mode)
TPR	Privileged Function State in BS2000 systems (Task Privileged)
TPSU	Transaction Protocol Service User
TSAP	Transport Service Access Point
TSN	Task Sequence Number
TU	Non-Privileged Function State in BS2000 systems (Task User)
TX	Transaction Demarcation (X/Open)

UDDI	Universal Description, Discovery and Integration
UDS	Universal Database System
UDT	Unstructured Data Transfer
ULS	User-Specific Long-Term Storage
UPIC	Universal Programming Interface for Communication
USP	UTM Socket Protocol
UTM	Universal Transaction Monitor
UTM-D	UTM Variant for Distributed Processing in BS2000 systems
UTM-F	UTM Fast Variant
UTM-S	UTM Secure Variant
UTM-XML	openUTM XML Interface
VGID	Service ID
VTSU	Virtual Terminal Support
WAN	Wide Area Network
WS4UTM	Web-Services for openUTM
WSDD	Web Service Deployment Descriptor
WSDL	Web Services Description Language
XA	X/Open Access Interface (X/Open interface for access to the resource manager)
XAP	X/OPEN ACSE/Presentation programming interface
XAP-TP	X/OPEN ACSE/Presentation programming interface Transaction Processing extension
XATMI	X/Open Application Transaction Manager Interface
XCS	Cross Coupled System
XHCS	eXtended Host Code Support
XML	eXtensible Markup Language

15 Related publications

You will find the manuals on the internet at <https://bs2manuals.ts.fujitsu.com>.

openUTM documentation

openUTM Concepts and Functions

User Guide

openUTM Programming Applications with KDCS for COBOL, C and C++

Core Manual

openUTM Generating Applications

User Guide

openUTM Using UTM Applications on BS2000 Systems

User Guide

openUTM Using UTM Applications on Unix, Linux and Windows Systems

User Guide

openUTM Administering Applications

User Guide

openUTM Messages, Debugging and Diagnostics on BS2000 Systems

User Guide

openUTM Messages, Debugging and Diagnostics on Unix, Linux and Windows Systems

User Guide

openUTM Creating Applications with X/Open Interfaces

User Guide

openUTM XML for openUTM

openUTM Client (Unix systems) for the OpenCPIC Carrier System Client-Server Communication with openUTM

User Guide

openUTM Client for the UPIC Carrier System Client-Server Communication with openUTM

User Guide

openUTM WinAdmin
Graphical Administration Workstation for openUTM

Description and online help system

openUTM WebAdmin
Web Interface for Administering openUTM

Description and online help system

openUTM, openUTM-LU62
Distributed Transaction Processing between openUTM and CICS, IMS and LU6.2 Applications

User Guide

openUTM (BS2000)
Programming Applications with KDCS for Assembler
Supplement to Core Manual

openUTM (BS2000)
Programming Applications with KDCS for Fortran
Supplement to Core Manual

openUTM (BS2000)
Programming Applications with KDCS for Pascal-XT
Supplement to Core Manual

openUTM (BS2000)
Programming Applications with KDCS for PL/I
Supplement to Core Manual

WS4UTM (Unix systems and Windows systems)
WebServices for openUTM

Documentation for the openSEAS product environment

BeanConnect

User Guide

openUTM-JConnect
Connecting Java Clients to openUTM

User documentation and Java docs

WebTransactions
Concepts and Functions

WebTransactions
Template Language

WebTransactions
Web Access to openUTM Applications via UPIC

WebTransactions
Web Access to MVS Applications

WebTransactions
Web Access to OSD Applications

Documentation for the BS2000 environment

AID Advanced Interactive Debugger Core Manual

User Guide

AID Advanced Interactive Debugger Debugging of COBOL Programs

User Guide

AID Advanced Interactive Debugger Debugging of C/C++ Programs

User Guide

BCAM **BCAM Volume 1/2**

User Guide

BINDER
User Guide

BS2000 OSD/BC **Commands Volume 1 - 7**

User Guide

BS2000 OSD/BC **Executive Macros**

User Guide

BS2IDE
Eclipse-based Integrated Development Environment for BS2000
User Guide and Installation Guide
Web page: <https://bs2000.ts.fujitsu.com/bs2ide/>

BLSSERV
Dynamic Binder Loader / Starter in BS2000/OSD

User Guide

DCAM
COBOL Calls

User Guide

DCAM
Macros

User Guide

DCAM
Program Interfaces

Description

FHS
Format Handling System for openUTM, TIAM, DCAM

User Guide

IFG for FHS

User Guide

HIPLEX AF
High-Availability of Applications in BS2000/OSD

Product Manual

HIPLEX MSCF
BS2000 Processor Networks

User Guide

IMON
Installation Monitor

User Guide

MT9750 (MS Windows)
9750 Emulation under Windows

Product Manual

OMNIS/OMNIS-MENU
Functions and Commands

User Guide

OMNIS/OMNIS-MENU
Administration and Programming

User Guide

OSS (BS2000)

OSI Session Service

User Guide

openSM2
Software Monitor

User Guide

RSO
Remote SPOOL Output

User Guide

SECOS
Security Control System

User Guide

SECOS
Security Control System

Ready Reference

SESAM/SQL
Database Operation

User Guide

TIAM
User Guide

UDS/SQL
Database Operation

User Guide

Unicode in BS2000/OSD
Introduction

VTSU
Virtual Terminal Support

User Guide

XHCS
8-Bit Code and Unicode Support in BS2000/OSD

User Guide

Documentation for the Unix, Linux and Windows system environment

CMX V6.0 (Unix systems)

Betrieb und Administration (only available in German)

User Guide

CMX V6.0

Programming CMX Applications

Programming Guide

OSS (UNIX)

OSI Session Service

User Guide

PRIMECLUSTER™

Concepts Guide (Solaris, Linux)

openSM2

The documentation of openSM2 is provided in the form of detailed online help systems, which are delivered with the product.

Other publications

CPI-C

X/Open CAE Specification

Distributed Transaction Processing:

The CPI-C Specification, Version 2

ISBN 1 85912 135 7

Reference Model

X/Open Guide

Distributed Transaction Processing:

Reference Model, Version 2

ISBN 1 85912 019 9

REST

Architectural Styles and the Design of Network-based Software Architectures

Dissertation Roy Fielding

TX

X/Open CAE Specification

Distributed Transaction Processing:

The TX (Transaction Demarcation) Specification

ISBN 1 85912 094 6

XATMI

X/Open CAE Specification

Distributed Transaction Processing

The XATMI Specification

ISBN 1 85912 130 6

XML

W3C specification (www consortium)

Web page: <http://www.w3org/XML>