Fujitsu Technology Solutions

SECOS (BS2000/OSD)

Version V5.4A
December 2012

Readme file

1 Introduction

This Readme file for SECOS V5.4A includes modifications of the following manuals:

[1] SECOS V5.3
Security Control System - Access Control
Edition: July 2010
Order Number: U5605-J-Z125-9-76

[2] SECOS V5.3
Security Control System - Audit
Edition: July 2010
Order Number: U41845-J-Z125-1-76

2 Increase of the number of input files for utility routine SATUT

The number of input files which may be specified for the operand INPUT-FILES in the statement SELECT-INPUT-FILES of the utility routine SATUT has been increased from 25 to 100.

See chapter 2.6.6, statement SELECT-INPUT-FILES
on page 153ff. in the manual [2].

```
SELECT-INPUT-FILES
------------------------------------------------------------------------
INPUT-FILES = *STD(...) / list-poss(100): <filename 1..54>

      *STD(...)
         |
         |
           ...
```

INPUT-FILES =
This defines the type of file to be used as input for preparation.

. . .

INPUT-FILES = list-poss(100): <filename 1..54>
File name of the analysis file to be used as the input file for SATUT.

3 Support of additional user attributes in the user groups

The commands ADD-USER-GROUP and MODIFY-USER-GROUP support a new Class-2 system parameter and additional 4 user attributes:

See chapter 3.4, commands ADD-USER-GROUP on page 143ff. and MODIFY-USER-GROUP on page 246ff. in the manual [1].

```
ADD-USER-GROUP

...
,ADDRESS-SPACE-LIMIT = *STD / <integer 1.. 2147483647>
...
,HARDWARE-AUDIT = *ALLOWED / *NOT-ALLOWED
,LINKAGE-AUDIT = *ALLOWED / *NOT-ALLOWED
,CRYPTO-SESSION-LIMIT = *STD / *MAXIMUM /
                        <integer 0..32767>
,NET-STORAGE-USAGE = *ALLOWED / *NOT-ALLOWED
...
```

```
MODIFY-USER-GROUP

...
,ADDRESS-SPACE-LIMIT = *UNCHANGED / *STD /
                       <integer 1.. 2147483647>
...
,HARDWARE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
,LINKAGE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
,CRYPTO-SESSION-LIMIT = *UNCHANGED / *STD / *MAXIMUM /
                        <integer 0..32767>
,NET-STORAGE-USAGE = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
...
```

ADDRESS-SPACE-LIMIT = *STD
The default value is provided by the startup parameter service in the Class-2 system parameter SYSGJASL. It is set to 16 MB by default.

HARDWARE-AUDIT = *ALLOWED / *NOT-ALLOWED
This determines whether the group administrator is authorized to grant group members or subgroups the right to use the hardware audit mode.

LINKAGE-AUDIT = *ALLOWED / *NOT-ALLOWED
This determines whether the group administrator is authorized to grant group members or subgroups the right to use the linkage audit mode.

CRYPTO-SESSION-LIMIT = *STD / *MAXIMUM / <integer 0..32767>
Specifies the maximum number of openCRYPT sessions within a BS2000[1] session. The group administrator is authorized to pass this upper limit or a lower value on to subgroups or group members.

NET-STORAGE-USAGE = *ALLOWED / *NOT-ALLOWED
This determines whether the group administrator is authorized to grant group members or subgroups the right to allocate storage space on a net-storage volume.

The command SHOW-USER-GROUP supports additional 4 user attributes:

– in the Show-layout:

```
...
HARDWARE-AUDIT     ......   CRYPTO-SESSION-LIMIT    ......
LINKAGE-AUDIT      ......   NET-STORAGE-USAGE       ......
...
```

– by creation of S-variables:

Name of the S variable	T	Contents
var(*LIST).HARDWARE-AUDIT	S	'*ALLOW' '*NOT-ALLOW'
var(*LIST).LINKAGE-AUDIT	S	'*ALLOW' '*NOT-ALLOW'
var(*LIST).CRYPTO-SESSION-LIM	I	<integer 0..32767>
var(*LIST).NET-STOR-USAGE	S	'*ALLOW' '*NOT-ALLOW'

See chapter 3.4, command SHOW-USER-GROUP on page 432ff.
in the manual [1].

[1] BS2000/OSD ® is a trademark of Fujitsu Technology Solutions.

4 Additional output layout for command SHOW-LOGON-PROTECTION

See chapter 3.4, command SHOW-LOGON-PROTECTION on page 325ff. in the manual [1].

```
SHOW-LOGON-PROTECTION

...
,INFORMATION = *ATTRIBUTES(...) / ...

   *ATTRIBUTES(...)
     |   SCOPE = *LOGON-DEFAULT / *USER-IDENTIFICATION /
     |           *ALL
...
```

SCOPE = *ALL

The protection attributes for access control which are currently effective are output.
To distinguish between the attributes which have been defined explicitly for the user ID and the current default attributes for access control the latter are marked with a '*'.

New S-variables:

See page 335ff. in the manual [1].

Name of the S variable	T	Contents
var(*LIST).EXPIR-DATE-DEF	B	FALSE TRUE
var(*LIST).EXPIR-WARN-DEF	B	FALSE TRUE
var(*LIST).PASS.MANAGE-DEF	B	FALSE TRUE
var(*LIST).PASS.MIN-LEN-DEF	B	FALSE TRUE
var(*LIST).PASS.MIN-COMPLEX-DEF	B	FALSE TRUE
var(*LIST).PASS.LIFETIME-DEF	B	FALSE TRUE
var(*LIST).PASS.EXPIR-DATE-DEF	B	FALSE TRUE
var(*LIST).PASS.EXPIR-WARN-DEF	B	FALSE TRUE
var(*LIST).PASS.UNLOCK-EXPIR-DEF	B	FALSE TRUE
var(*LIST).PASS.PASS-MEMORY-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.PAR-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.COUNT-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.OBS-TIME-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.SUS-TIME-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.SUBJECT-DEF	B	FALSE TRUE
var(*LIST).INACTIVITY.PAR-DEF	B	FALSE TRUE
var(*LIST).DIALOG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).BATCH.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-TER.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-PROG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-CONS.ACCESS-DEF	B	FALSE TRUE
var(*LIST).POSIX-RLOG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).POSIX-REM.ACCESS-DEF	B	FALSE TRUE
var(*LIST).NET-DIALOG.ACCESS-DEF	B	FALSE TRUE

5 Extension of macro SRMSUG

The macro SRMSUG supports additional 4 user attributes:

```
          SRMSUG XPAND=INFO,VERSION=6,MF=D
```

```
SRMAUG   DSECT ,
...
SRMAIND1 DS    X          INDICATOR BYTE 1:
SRMANSTU EQU   X'01'         NET-STORAGE-USAGE
**                              S: ALLOWED
**                              R: NOT ALLOWED
...
SRMAADSL DS    F          ADDRESS SPACE LIMIT
SRMAREPA DS    F          RESIDENT PAGES
SRMACRSL DS    F          CRYPTO SESSION LIMIT
...
```

See chapter 3.5, macro SRMSUG on page 447ff. in the manual [1].

6 Dialog-Logon in NET-DIALOG, redirect to DIALOG

See chapter 3.3.6 on page 104ff. in the manual [1].

By the following option in the subsystem information file SYSSSI.SRPMOPT.054:

NET-DIALOG-REJECT-FALLBACK=Y

the dialog-logon is executed in the access class DIALOG when the Kerberos authentication in the access class NET-DIALOG did not yield a result because
1) the ticket could not be deciphered or
2) the principal contained in the ticket has no permission.

7 Correction of an example for Single Sign On

Chapter 3.3.6 Single Sign On with Kerberos, on page 109/110 in the manual [1].

The examples for the command ADD-KEYTAB-ENTRY in the first bullet point

```
/ADD-KEYTAB-ENTRY *STD('host/hostname@NT-DNS-REALM-NAME' -
/  ,KEY    = *PASSWORD('password')
```

and

```
/ADD-KEYTAB-ENTRY *STD ('host/d016ze04.mch.fts.net@FTS.NET' -
/  ,KEY    = *PASSWORD('betterlongthanshort')
```

are replaced by

```
/ADD-KEYTAB-ENTRY *STD, 'host/hostname@NT-DNS-REALM-NAME' -
/  ,KEY    = *PASSWORD('password')
```

and

```
/ADD-KEYTAB-ENTRY *STD, 'host/d016ze04.mch.fts.net@FTS.NET' -
/  ,KEY    = *PASSWORD(' betterlongthanshort',KEY-VERSION=3)
```

8 Correction at CONVERT-KEYTAB

Chapter 3.4 SRPM Commands, on page 160 in the manual [1].

In "Usage conditions" the text passage

Therefore
- the SRPMOPT Option (file: SYSSSI.SRPMOPT.053) SECURITY-ADMIN-STD-PROCESSING=Y has to be set, or
- The security administrator must assign the privilege STD-PROCESSING to himself.

is replaced by

Therefore
- the SRPMOPT Option (file: SYSSSI.SRPMOPT.054) SECURITY-ADMIN-STD-PROCESSING=Y has to be set, **and**
- the security administrator must assign the privilege STD-PROCESSING to himself.