Schlumberger

the e-gate advantage for smart card

executive summary

introduction

SchlumbergerSema e-gate is a technology innovation that is today paving the way for new opportunities and revised economics for smart card based applications. e-gate technology will power SchlumbergerSema traditional smart card product range.

Relying on the widely available USB standard, e-gate technology enables e-gate powered smart devices to directly plug into a Personal Computer without the need of a smart card reader.

Fully compliant with the traditional ISO smart card standard, e-gate powered smart cards combine the best of both worlds and leverage smart card proven security with a seamless integration into the PC world.

Used in PKI deployment, e-gate powered smart cards dramatically contribute to reduce the Total Cost of Ownership of the infrastructure, eliminating readers and highly reducing the cost and time incurred in installation, maintenance and support.

the e-gate technology breakthrough in the smart card industry

Since almost twenty years, smart cards are proving to be the ideal, tamperproof medium for storing high value credentials. Especially in Europe, GSM operators and banks have long successfully been using smart cards to provide to their clients the best way to carry their portable digital ID, retrieve money, authenticate, etc. In other parts of the world, smart cards are increasingly adopted. This is shown for example by American banks recent considerations, through the Europay-MasterCard-Visa (EMV) initiative, or within the new generation wireless network standards. Furthermore, smart cards are increasingly endorsed as the best way to secure e-commerce transactions in open networks.

Since its early days, the smart card industry has been relying on the International Standardization Organization (ISO) standard as the communication protocol between the smart card and the reader.

The ISO standard sets the physical properties, the data transmission and the instruction set specifications for smart cards. ISO specifies the physical dimensions and the placement of the chip connectors on the card as well as the communication protocol used by the card to communicate with readers.

Until now, the ISO standard has provided the high level of security and reliability and the high interoperability that has contributed to the success and wide availability of smart card applications.

As smart card applications and PC environments are today getting more and more intricate, a seamless integration of smart card infrastructure with PC becomes essential for rapid, easy and low cost deployment of smart cards. Smart card based e-commerce applications, corporate security projects or loyalty programs are increasingly based on PC standards and platforms.

Because PC environments and smart card applications were deployed on separate grounds at the time when the ISO smart card standard was developed, integration of ISO-only smart cards with PC platforms today relies on complex interfaces. For example, ISO-only smart cards can only be read through an ISO-smart card reader, which embeds the complex electronics necessary to adapt card communication to PC standards.

The universal serial bus (USB) is a standardized interface included on all personal computers built since 1997. USB has imposed itself as the de facto communication protocol standard of the PC world.

e-gate technology targets at combining the best of both worlds. As a hardware and software add-on that complements the traditional ISO-only smart card with the appropriate USB communication module, e-gate is a cross-platform and transversal technology innovation that bridges the gap between PC and smart cards through dual-standard communication.

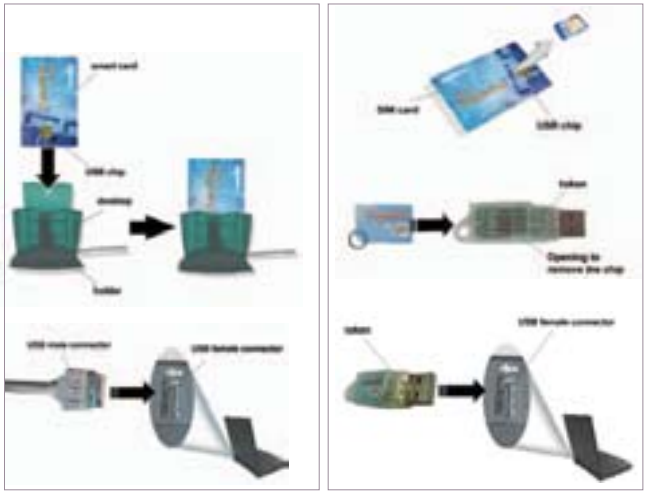
e-gate technology overview

At the core of e-gate technology lies the ambition of its promoters to incorporate into the chip on the smart card itself the complex electronics normally found in a smart card reader.

Thanks to a close development effort with silicon founders, SchlumbergerSema has been able to develop and integrate on a new generation of chips the hardware and software modules needed for the USB protocol to be implemented on the card.

Because of this evolution of the chip, e-gate powered smart cards can today plug directly into the USB port on a computer via a simple connector. This connector does not carry any electronics and represents the potential for a significant cost reduction compared to traditional ISO-only smart card readers.

Because of their innovative design, e-gate powered smart devices combine the convenience of USB protocol with the proven advantages of traditional smart cards.



e-gate powered smart cards seamlessly integrate into standard PC environment

e-gate technology turns the e-gate powered smart card into a full USB peripheral. This feature brings a new era of convenience to smart card use and deployments.

User convenience
Most computers installed today have a USB port ready and most operating systems natively support the USB protocol. USB ports are often located at the front of recent workstations, and at the side of laptops.

e-gate powered smart cards becomes hot plug & play with any USB ready computer. This means that the user can connect the smart device when necessary, while the computer is running, without the need to shut down and re-boot.

Several devices can be attached to USB port with inexpensive hubs, solving the slot monopolization issue. Moreover, the card is powered through the USB connection, which eliminates the need for additional cabling.

Easy and fast deployment, limited maintenance
e-gate technology suppresses the need for readers and therefore allows for easy and fast smart card deployment. In particular, e-gate removes the requirement of the reader driver installation, which is the cause of the majority of set-up complications that occur in traditional smart card deployments.

Because there is no electronics in e-gate connectors, the cost and pains of maintenance and support for the smart card reader are eliminated.

Thanks to these powerful features, e-gate powered smart cards installation becomes simple and straightforward for any computer user. Assistance to deployment, support and hotline costs usually associated with any smart card project gets therefore dramatically reduced by e-gate technology.

e-gate technology at SchlumbergerSema

As a pioneer of the technology, SchlumbergerSema will progressively have its existing product portfolio "e-gate ready". e-gate powered version of currently existing ISO-only smart cards products will be offered to customers.

Moreover, as e-gate technology dramatically impacts the connectivity between the computer and the smart card, innovation in the smart card form factor becomes stimulated. Thus, in order to provide its customers with maximal flexibility, SchlumbergerSema has chosen to offer the e-gate powered smart cards in two formats:

- A standard ISO format card, which is the exact size and shape of a credit card. This format appears to be adapted with desktop usage, and allows bundled services such as physical security, graphical personalization…
- A small, thumb-sized cut-down card that can be inserted into a token. This is an ideal format for itinerant people or laptop, that can be easily attached to a key ring…

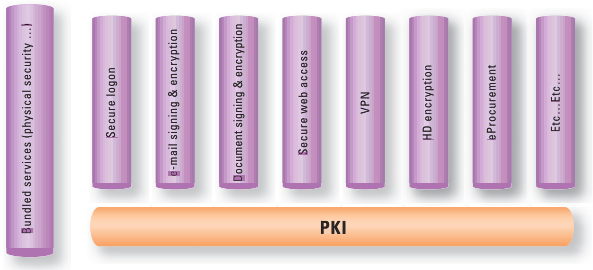
business scenarios for e-gate powered smart cards within a corporate PKI deployment

Smart cards in a Public Key Infrastructure

Public key infrastructure (PKI) is today recognized as the standard, state-of-the-art security technology for both safeguarding a firm's total economic value and for creating new business opportunities.

A PKI relies on the secure delivery to each end-user of a digital certificate that is the basis for convenient, sophisticated services:

Organizations planning to deploy public-key infrastructures face critical decisions. They have to balance the Total Cost of Deployment in regard of the Return on Investment and risk reduction. For example, they have to consider whether to insource or outsource their PKI services, to select a PKI provider or technology, or to choose the appropriate authentication device technology for end-users…



The choice of the end-user authentication device clearly appears as one of the key challenges as it greatly impacts return on investment, security and convenience of a PKI.

Authentication devices, as smart cards or tokens are the visible elements of PKI systems. Carried by end-users, they hold the secrets (e.g. private key) that are used to transparently authenticate, to decrypt documents, to sign documents digitally, etc.

It is essential that strict confidentiality of that private key be ensured. Great care must therefore be taken to select the right technology for storage and transport of the private key.

Authentication devices have to be convenient. They must be portable, in order for an end-user to carry its digital ID everywhere he needs to use it.

Authentication devices should also make bundled services possible, as physical access control, e-purse, or tailor-made applications, allowing to mutualize the costs and increase the return of investment of the infrastructure.

The three most commonly considered solutions for end-user authentication in a public-key infrastructure are:

- Software-based solutions, where the private key is resident on your hard drive
- Dongles
- Smart cards

Software-based solutions
Hard drives are highly inefficient and risky places to store your private keys. Hard drives can and do crash; PCs are replenished on a regular basis, destroying the old private key and certificates in the process; hard drives offer only minor portability (the key and certificate data is stored in a proprietary browser storage area and must be exported or imported in order to be moved from one workstation to another). Also, and perhaps most importantly, private keys on hard drives can be stolen or deleted without such activity being detected. Hackers are capable of stealing a user's keys without the user knowing that the keys have been compromised.

Also, protection of the key itself is not strong. The user simply needs to know the password. With smart cards and other tokens, the user must actually possess the token and also know the PIN code of the token. Moreover, the password that protects the access to your private key can be deactivated on most Internet Browsers, allowing anybody who has access to your desktop to sign or authenticate on your behalf!

For all these reasons, most of current legislations do not grant full legal value to the digital signature created with software certificate.

Dongles
Dongles plug into the USB port of personal computers. Some dongles contain a processor used for safeguarding the private key and performing the cryptographic calculations. This means that the private key can exist entirely on the dongle and not in software and/or on the hard drive.

Dongles are portable and convenient, especially for people who want to carry their digital ID with them on their key rings. This makes dongles particularly adapted to targeted users as itinerant people.

Unfortunately, dongles with cryptographic capabilities are very expensive and use non-standard, proprietary technologies. Although they allow on-board key generation, USB dongles cannot be personalized en masse, implying that end-users must put certificates on them "by hand" one at a time.

Smart Cards
Smart cards today provide the most secure and convenient storage for high value digital credentials. This is the consensus of many of the leading security and IT analysts, and the use of smart card as the authentication device for end-user is a constant requirement for most large-scale PKI deployments today.

There are several reasons for this conclusion:

- Storing the digital certificate and private key on the smart card provides the best protection against theft or impersonation. Requiring a PIN to access the smart card provides an added layer of protection if the smart card itself is lost or stolen
- With smart cards the certificate and private key are highly portable, and can be used on multiple workstations. They allow to access systems remotely, whether they are at work, at home, or on the road. They can be read on any standard smart card reader.
- Since additional pieces of software, photo ID, magnetic stripe and contact-less chip can easily be placed on smart cards, it also allows for many bundled services, mutualising costs on diverse applications: physical access control, or tailor-made applications as work time accountancy, cafeteria e-purse, etc.

In the perspective of a corporate PKI deployment, easy integration of the smart card solution with the existing PC infrastructure is of critical importance for IT managers and appears as the key to maximize the return on investment. As a matter of fact, even small compatibility issues may dramatically affect installation and deployment complexity. Moreover, hardware readers, as all hardware devices, do require specific maintenance that has to be taken into consideration.

e-gate technology is specifically designed to help companies unleash the full potential of smart cards within a PKI project. e-gate technology, combined with state of the art corporate security smart cards, brings to companies the promise of seamless, flexible and economic smart card deployments.

The following real life smart card deployments highlight the value proposition for e-gate powered smart cards in corporate security:

Internal deployment

In order to secure its internal network and prevent it from unauthorized external access and risk of data destruction, an international telecom company has decided on a worldwide basis to deploy a fully-fledged public key infrastructure.

To ensure state-of-the-art security and compliance with international standards, all employee of the company should be equipped with digital credentials stored on a personal smart card. However, some local subsidiaries had already engaged in PKI-related smart card deployments and deployed ISO-only smart card readers. Deployment decisions had to take into account the existing infrastructures and guaranty full backward compatibility.

Moreover, a large number of users were itinerant salesforces, equipped with laptop and favouring key-like form factor over traditional smart cards for their authentication device.

e-gate powered smart cards provided strong and compelling answers to both of these requirements :

- New smart cards were issued powered by the e-gate technology. Associated with low cost connectors, this contributed to a strong reduction in the per-seat cost of ownership of the infrastructure while meeting the strong security requirements imposed by the telecom company. Backward compatibility issues with the already in place ISO-only smart card readers was solved by the dual-standard capability of e-gate powered smart cards.
- Each user was offered to choose which of the form factors would best meet its personal requirements. Salesforces mostly elected key-like token that were often put on the personal key ring, while fixed workers decided to opt for traditional smart cards connected to the PC through a simple connector. Both devices were based on e-gate technology, required no specific development, underwent the same personalization process and therefore took advantage of large economies of scale. Only at the very end of the process would the form factor be considered.

e-gate technology is seamlessly penetrating the company with no migration issues, full flexibility at the user level and significant economies for IT managers.

Secure Extranet deployment

To establish an internet-based paperless information flow with its customers, an insurance broker sought to encrypt the communication and enables the transaction partners to digitally sign the messages exchanged.

After having carefully considered all the commercially available options, IT department and company management turned to PKI as being the most secure, standard and perennial technology on the marketplace.

Smart cards got strong interest from project leader for the storage of the digital credentials. They carried out the strongest security image and contributed to a full portability of the application. They could also be easily distributed to partners and carried the graphical logo of the insurance broker.

However, deployment issues associated with the smart card readers, such as complex installation at partners' premises or concerns about the cost of the smart card reader, have long prohibited the use of smart cards in this application.

Digital credentials were therefore stored directly on PC hard disk, raising security concerns among the users and limiting the convenience of the application.

e-gate technology value proposition drove the project leader to reconsider the smart card equation within the projects. As a matter of fact, deployment of e-gate powered smart cards at partners' premises took large advantage of e-gate hot plug&play feature and largely reduced the need for deployment assistance and hotline resources. Users, mostly risk managers with no specific IT competences, simply had to insert the e-gate connector into the USB port of their PC, connect the e-gate powered smart card sent via snail mail and launch the application. Costs incurred by the insured broker were this way strongly reduced.

In this case, e-gate technology helped the insurance broker to deliver to its corporate customers the promise of state-of-the-art smart card based security and full user convenience and contribute to bridge the gap between unsatisfying software based deployments and complex smart cards issues.

Conclusion

e-gate powered smart cards today constitute a mature, powerful and economic answer to the challenge of the integration of smart card application into the PC environment. Thanks to simple connectivity, high-speed communication and openness in the choice of the form factor, e-gate technology will contribute to turn the smart card into the personal and ubiquitous security device for IT infrastructure or e-commerce applications.

ASIA • **TEL: +852 2956 3331**
EUROPE • **TEL: +33 1 46 00 66 67**
JAPAN • **TEL: +81 3 3434 7300**
NAM • **TEL: +1 888 343 5773**
SAM • **TEL: 54 11 43 44 51 32**

www.schlumbergersema.com

Schlumberger