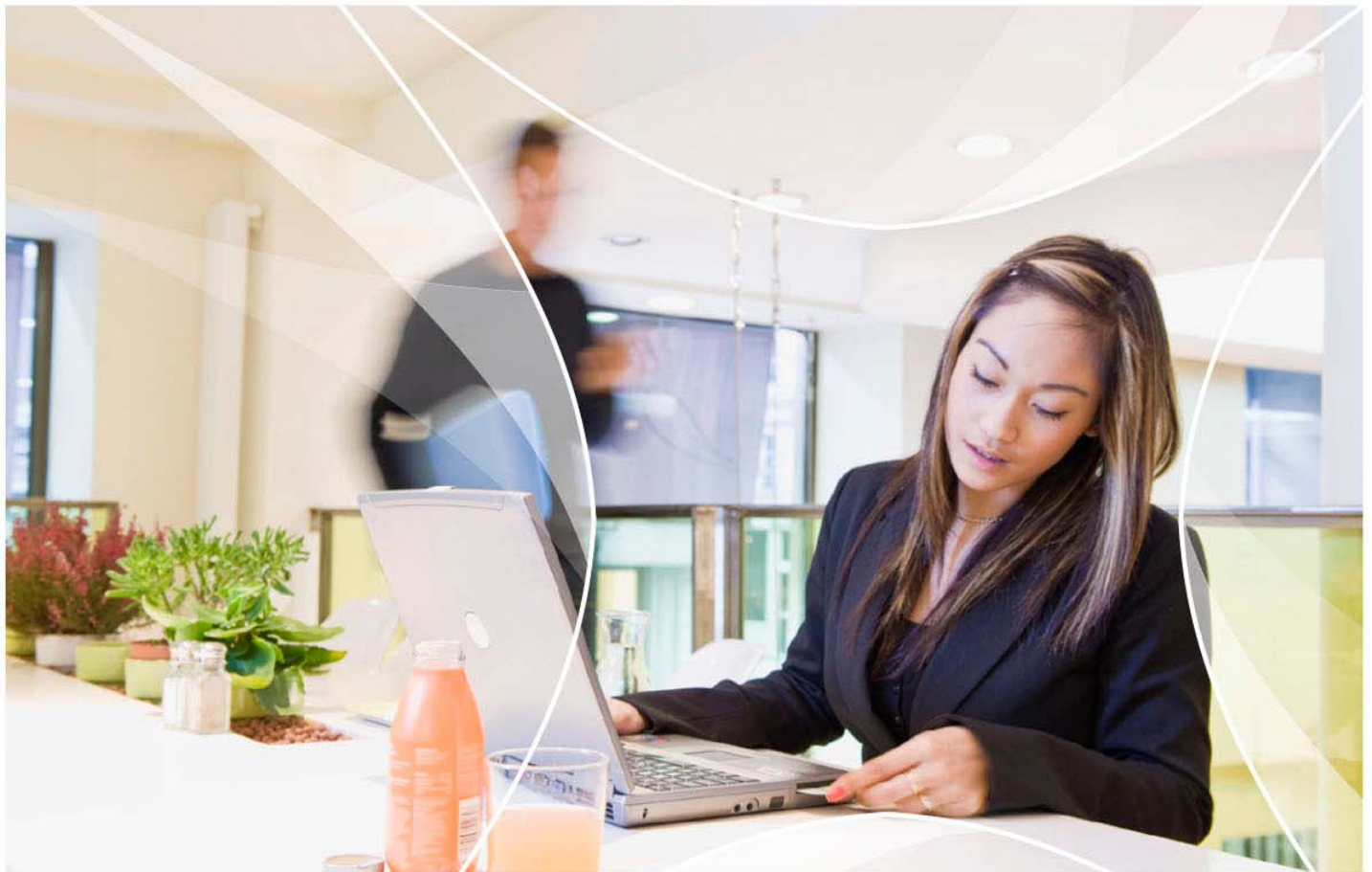


Mobile Data Secured by Smart Card

||||| Enabled smart card security anytime, anywhere



FINANCIAL SERVICES & RETAIL

ENTERPRISE

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

Table of contents

I. The Smart Card in a Mobile World	3
II. Smart Card for Protecting Mobile Data	5
a. Protection of flash memory encryption key	5
b. Immunity to various software and hardware attacks	5
c. Security without compromising user experience	6
III. Smart Card for Data Loss Prevention and increased ROI	8
IV. Conclusion	9

1. The Smart Card in a Mobile World



Transferring data from one point to another and carrying them around have become common practice, if not a habit. The end result is a mobile world that now seems to be a breeding ground for serious data thieves. Identity theft and data breach seem to hit the headlines far too often and reports of stolen laptops, lost USB tokens, financial data breach,

and unlawful use of personal credentials among others, are heard of everywhere. In most of these cases, the loss is irreparable, and for companies and individuals these may mean losing the public's trust.

The expansion and increasing sophistication of identity theft has undoubtedly paved the way for stronger security technologies in strategic initiatives such as e-government and e-business. Governments, financial institutions and organizations have begun turning to *smart cards* to secure the credentials of billions of people worldwide.

In 2008 alone, 5.045 billion smart cards were shipped worldwide—an impressive 13.2% increase over the 2007 figure of 4.455 billion¹.

- Around 100 countries have adopted smart card based national eID/ Healthcare systems that serve more than 400 million people. These include passports that secure personal credentials in a smart card
- Financial institutions around the world issued 650 million credit/ debit cards that use smart cards in 2008. United States accounted for 47.4 million of these cards¹.
- In 2008 there were over 250 million GSM subscribers in United States and 3.2 billion subscribers worldwide². GSM mobile phones include a subscriber identity module (SIM),

¹ World Banking and Loyalty Smart Card Market: Frost and Sullivan Dec 2008

which is a smart card configured with information essential to authenticating the phone, allowing a phone to receive service whenever the phone is within coverage of a suitable network.

Near Field Communication (NFC) technology along with the smart card technology enables mobile phones to be used for payment and identity transactions.

- Over 200 million people worldwide use smart card based payment cards to pay for their travel through public transport systems.

Smart card technology conforms to international security standards and is available in a variety of form factors, including plastic cards, key fobs, watches, the subscriber identification modules used in GSM mobile phones, and USB-based tokens. Smart cards are essentially miniature computers without display screens or keyboards. They contain an embedded integrated circuit (or chip), a powerful minicomputer that can be programmed in different ways. Smart cards can perform many functions, such as storing and processing data, executing calculations and encryption algorithms, managing files, and make possible sophisticated and portable data processing.

Because of their portability and size, smart cards provide an flexible solution for secure data exchange.

² World SIM Smart Card Market: Frost and Sullivan Dec 2008

2. Smart Card for Protecting Mobile Data



Millions of USB drives are used today as a convenient way to transferring necessary data between systems. Widespread use of smart cards as a defacto standard for securing user credential has prompted the use of smart card technology for protection of mobile data on USB drives. Today smart cards can be used to generate and store encryption keys for flash drives and user authentication data. The benefits of this integrated approach include:

> Protection of flash memory encryption key

- **Secure storage:** Flash encryption keys are stored on tamper-proof smart card and can only be accessed through the smart card operating system by those with proper access rights. Flash encryption key never leaves the USB token.
- **PIN Block and Unblock:** Smart card can block the access after predefined set of unsuccessful PIN attempts have occurred. To enable access, smart card deploys stringent PKI based challenge-response process. This prohibits any unauthorized access to the flash encryption keys and protects the authorized user.

> Immunity to various software and hardware attacks

- **Brute force and Parallel Attacks:** Brute force attacks guess the password or the encryption key. A parallel attack is a brute force attack variant in which the attacker copies the encrypted data from the stolen USB flash drive, shares the data with as many computers as possible that are under his/her control, and then puts them to work in parallel to guess the password offline and unlock the encrypted data.

Smart card based integrated encryption thwarts brute force and parallel attacks as the data is never copied from device to host memory and smart card limits the number of attempts for successful authentication.

- **Coldboot Attack:** DRAM memory is used to store data while the PC is running. After power is removed, all content is deleted in a gradual process that can take anywhere between a few seconds and up to a few minutes. If the chip is cooled by artificial means, the content can be retained for as long as 10 minutes. This characteristic of DRAM memory enables a hacker to read the memory content by cutting power and then performing a cold boot with a malicious operating system.

In a smart card based approach, encryption keys are generated and stored on tamper-proof smart card and never leave the USB flash drive. Coldboot attacks on such implementation will not yield any fruitful result.

- **Authentication Counter Attack:** An authentication counter tries to limit the number of security enforcing procedures that the system can perform in all the system life. Various physical attacks can be carried out on the authentication counter implementation including dumping and restoring the authentication counter after decrement and fault attack³ on decrement.

In a smart card based implementation, tamperproof storage cannot be compromised and counter decrement cannot be avoided.

- **Malicious Code:** Malicious code can run on a PC into which a USB flash drive is inserted and can disable the encryption and protection mechanism on the USB flash drive. Malicious code can also copy data from the USB flash drive after it has been authenticated, or it can copy the user password and use it after the user logs out of the drive.

> Security without compromising user experience

Smart card based encryption of the flash memory is automatic and built-in device. It cannot be disabled by the end-user or attacker and assures protection of stored data. The user experience is not altered and the performance of the device is not affected by this integrated approach. Users still enjoy the speed and convenience of standard off-the-shelf USB drive.

³ The Sorcerer's Apprentice Guide to Fault Attacks: Hagai Bar-EI et. al.
(<http://eprint.iacr.org/2004/100.pdf>)

Smart card based encryption has clear advantages compared to software-based and hardware-based encryption, when security of the encryption method and attack resistance is considered. It is also critical to take into account issues like performance and encryption availability before making a decision on the type of encryption to implement. The following table summarizes the key differences among available encryption approaches.

	Software Based Encryption	Hardware Based Encryption	Smart Card Based Encryption
Bruteforce Attacks (including parallel attacks)	Difficult to prevent	Prevented, as encrypted data is never copied from the device to the host memory.	Immune to attack as encrypted data is never copied from the device to the host memory.
Security of Encryption Key at rest/after operation (e.g. resistance to Cold Boot Attacks)	Can be prevented if secure memory is available on the PC	Prevented by not using RAM or other common memory space to store encryption keys, and by the fact that the keys never leave the USB flash drive	Immune to attack as encryption keys are generated and stored on tamperproof smart card and never leave the USB flash drive
Security of Encryption Key in operation (e.g. resistance to fault attacks, decompiling, dumping, debugging etc.)	Encryption key can be access through various software attacks	Encryption key can be accessed through various hardware attacks (Controller Memory could be dumped; Controller software could be reversed etc.)	Encryption key cannot be accessed as it is copied from SC to controller memory only, after user is successfully authenticated
Attacks on Authentication Counter leading to Bruteforce Attacks	Not applicable	Resistant to software attacks. Possible physical attacks on auth counter management (dump / restore after decrement, fault attack on decrement etc.)	Software and hardware attacks Prevented by EAL4+ tamper resistant storage location. Cannot be compromised and counter decrement cannot be avoided
Malicious code	No way to prevent if the PC and its OS are infected	Prevented by using a security system independent of the PC and its OS	Prevented by using a security system independent of the PC and its OS
Always-on Encryption	Can be disabled by user or attacker	Built into device. Encryption is automatic	Built into device. Encryption is automatic
Performance	Slower, since existing processing capacity is used	Fast, since dedicated hardware is used for encryption processes	Fast, since dedicated smart card hardware is used for encryption processes

3. Smart Card for Data Loss Prevention and Increased ROI

Integrated smart card based encrypted devices can also be used to provide additional services like systems logon, digital signatures, hard disk and folder encryption. Today Data Loss Prevention (DLP) solutions such as endpoint access control and desktop encryption help reduce the risk of sensitive information being lost or stolen. These solutions when integrated with the devices offer several advantages that include:

- **Enforcement of security policies for removable media:** Even if the drive is lost or stolen, no unauthorized access to data is possible.
- **Stronger security for desktop encryption:** Encryption keys are more secure when generated and stored on a secure platform such as a smart card embedded in the USB token. This also enables two-factor authentication based on something the user has – a smart card or token – and something the user knows – a PIN code.
- **Long term investment lifecycle:** Support for PKI certificates from all leading Certificate Authorities extends investment lifecycle
- **Increased ROI with a platform for multiple applications:** The same personalized USB token can be used for multiple security applications.

In addition other smart card services like OTP and PKI-based systems authentication and digital signatures can also be used with this integrated approach. Examples of applications include VPN gateway for remote access to company network, Web server authentication and strong primary authentication to Web Single-Sign-On (SSO)

4. Conclusion

Smart cards are accepted as default standard for security of personal credentials across the globe. Many governments across the world trust smart card technology to secure data of their citizens when issuing passports, national IDs and healthcare IDs. Financial institutions use smart cards to guarantee identity of their customers and enhancing security of financial transactions. Public transport users use smart cards to cut lines and make faster payments for their travel. Cell phone users count on smart card technology to enable mobile payments.

Proven and trusted smart card technology when used to secure mobile data clearly demonstrates advantages over other methods of securing mobile data. Governments and organizations can also increase the ROI on their investment by deploying additional security services.

||||| The world leader in digital security

www.gemalto.com

gemalto 
security to be free