Global Information Assurance Certification Paper

Smart Cards – the All-in-One Security Platform for Today's Corporate World
GSEC Version 1.4

Ee Chin Chong
June 21, 2002

A. Abstract

My paper will illustrate that smart card is the comprehensive, user-friendly and scalable solution to secure today's organizations. We will see how the consolidation of multiple applications onto one device – the smart card, reduces administration load, provides a stronger Return On Investment (ROI) and increases security for today's enterprises, worldwide. Smart card, which enables multiple applications onto one platform, offers customers with security, flexibility and control. Thus, providing corporate identity, physical security access and logical security. In addition to smart card being a secure gadget to store passwords, it also provides user with the secure single-sign on capability. Smart card also eliminates the need for the multitude of tools – multiple sets of username and password, separate building access cards and multiple ID cards, just to name a few. The focus of this paper examines among others, the examples of some smart card applications and equipment.

"Worldwide smart card shipments reached 685.4 million units in 2001, up 10.4 percent over 2000," stated Clare Hirst, analyst of Gartner Dataquest. "Shipments of microprocessor cards for the financial segment will increase significantly over the next three years, helping to drive growth for leading card producers that already supply to that sector." (1)

B. Background

Before we discuss in the essence of the topic, let us begin by visiting the background technology.

What Is A Smart Card?

Smart card is a device that is the size of a credit card. It has an on-card Central Processing Unit (CPU); a processor that has an Operating System and delivers cryptographic capabilities. Smart card is tamper resistant. Therefore, it is a safe and stable place to store your private keys, as smart card will maintain data integrity for over 10 years. Besides, it will not be damaged if placed in proximity to magnetic and x-ray fields. In addition, smart card is highly portable, which has significant advantages over the standard PKI devices, where the private keys are stored in bulky hard drives and over biometric devices. Smart card enables us to authenticate ourselves, then bundles itself to other services and applications, Java applets, corporate e-purses and proximity technology, just to name a few. The potential utilization of smart card is just boundless.

What is PKI?
Public Key Infrastructure (PKI) is a comprehensive system that is required to provide public key encryption and digital services. It is supported by a common set of security services utilizing public key cryptography that enables seamless and trustworthy electronic business environment while being transparent and user friendly to the users involved in the transaction. [(2)] Here are the key benefits of PKI:

- Confidentiality – The information is kept secret
- Authentication – The right information is available to the right people at the right time
- Integrity – The information is not altered
- Non-Repudiation – User/party involvement cannot be denied

PKI technology secures our information capital. It maintains the confidentiality of our data, either as it is transmitted through a hostile environment and open infrastructure or when stored. In addition, PKI also provides a methodology for strong authentication (to verify users) thus enabling access control by granting the correct access, based on the credentials of each individual. Data integrity will also be preserved, and all parties will know if any data has been tampered with. Non-repudiation is especially important in today's e-business world as we need to ensure that proof of the actual activity occurred and that individuals involved in a particular transaction will not be able to deny involvement.

Why Smart Cards?
It is essential to understand how important the private key is to the corporation's security system. If the private key is exposed, the corporation's information capital is at risk. Therefore, the entire PKI technology has evolved in such a way as to safeguard the private key. It is therefore of paramount importance that the private key be protected and there is no more secure platform to store the private key than a smart card. If private keys were to be stored on hard drives, they would be prone to the dangers of the hard drives crashing, being stolen, being hacked, copied, or becoming obsolete. The tamper-resistant chips on smart cards will retain data for over 10 years. If the smart card is stolen or lost, the user will be aware of it, since the card itself will be physically missing. Also, should the smart card be lost, there is a layer of added security, because smart card provides strong authentication, much like ATM cards: you must have the card AND know the Personal Identification Number (PIN). It is very important to note that several incorrect PIN entries will result in the card being blocked and it would be of no use for the hacker. By storing the private key and digital signature on the card, many secure technologies and services are enabled. More applications and examples will be discussed in the later sections of this paper.

C. Smart Card – All in One Tool

Secure Physical Access System

To say that physical security is important is an understatement. I am going to illustrate the smart card as a tool for physical security. The smart card can be combined with other security card technologies like photo ID, magnetic-stripe and even proximity card technology. The smart card can be used as an ID badge for one enterprise. It will bear the photo, name and all the information that is essential to identify a person. In addition of the smart card being an ID card, it can be used as a physical access control device, replacing the need for multitude of cards. One enabler technology is MIFARE, which is a 13.56MHz open standard contactless technology owned by Philips Electronics. This technology offers read/write capability. MIFARE offers 1 to 4 inches of reading range. Smart card with MIFARE antenna and chip is a passive card, which means that it has no battery. Instead, it uses Radio Frequency communication technology to transmit and receive data between the card and the physical access reader. It also provides a unique 32-bit serial number for each number for each card. How does it work? The door reader will read the serial number off the card and compare it with the physical access database. It if matches the allowed list of serial numbers, access is granted to the holder of the card.

Figure 1. HID Mifare Reader. (3)

The figure above shows a HID Mifare contactless smart card reader 6055B manufactured by HID Corporation, short for Hughes Identification Devices. The company, which was started in 1991, produces a chain of access control products. Below is the HID Mifare reader specification:

- Read range of 1 to 4 inch
- Operating frequency of 13.56 MHz
- Potted electronics protect against harsh weather and vandalism
- ISO 1443A compatible
- Two communication ports of RS-232 and Wiegand (4)

Press Release on April 1998 - Philip's Opening of the MIFARE Technology Platform

"At the Smart Card '98 show in London, in February, Philips Semiconductors announced the opening of its MIFARE Technology Platform as Global Standard for Contactless Smart Card ICs to the worldwide market. As a result, any company will be able to apply for a license to manufacture and use products compatible with the contactless MIFARE Interface Technology according to the emerging ISO/IEC 14443 Type A.
The MIFARE Architecture Platform is already well established as the defacto industry standard. It covers about 90% of today's contactless smart card market with more than 30 million card ICs in use around the world and has proven its reliability with more than a billion transactions carried out over the last three years. The increasing number of installations in applications such as public transport, road toll, airline ticketing and ID cards is enlarging the circle of system integrators, card manufacturers and service providers acting as MIFARE system partners. With such a dominant position, it was a natural step for Philips to open the platform as a way of resolving potential market issues relating to standards or monopoly." (5)

Secure Logons

Passwords alone are no longer effective. In addition to being prone to numerous security issues, i.e. password hackings, attacks, they are not user friendly and expensive for corporations to maintain. Besides, users almost always undermine security if security requirements become too cumbersome. Organizations may force users to engage more secure passwords, but security may not be improved because these more difficult and hard-to remember passwords are most likely be written down. On the other hand, smart cards provide a simple, yet powerful line of defense. The information on the smart card is protected by two-factor authentication: *what you have* and *what you know*. *What you have* is the physical smart card itself, and *what you know* is the PIN.

In addition, smart cards also play an important role as secure storage containers for multiple passwords for logons to computers, to the network and web pages and related applications.

Smart cards also help increase security for single sign-on (SSO) with its two-factor authentication. SSO is a user-friendly tool for users as it allows the users to enter their username and password once when they logon to their PC and they will be automatically be logged on to the other applications, which are tied together to the authentication system. However, SSO has its fair share of risk as well. If the password is exposed, it risks exposing the entire corporation's information capital. However, with smart cards and two-factor authentication, security for SSO can be greatly enhanced.

The result of this is the centralized authentication system. Instead of authenticating with username and password, not to mention different sets of passwords for different applications, the user now authenticates the smart card and PIN and will be able to SSO to other applications that are tied to the PKI system. What are the implications of this? As

the PIN is much more user-friendly for the user, there is bound to be a drop in helpdesk calls that are associated with password problems. This reduces the Total Cost of Ownership (TOC), as well as increasing ROI for the corporation. In addition, smart card provides user with a secure gadget to store passwords and is also capable to secure single sign-on.

Email – Encryption and Digital signature
The smart card can also be used as a tool, together with the components in PKI system, to secure the email system. The private and signing keys, which are stored on the smart card, will protect the integrity of the information capital. Let us look at Bob and Alice of Corporation A. Bob would like to send an email to Alice, describing the details to the tender Corporation A is bidding for. However, one concern that he has top-secret information that needs to get to Alice (and Alice alone) and he needs to ensure that only the information is not tapped or altered during the process. Alice, on the other hand, needs to ensure that the information is genuine (and never altered) and that it came from Bob (and Bob alone). Therefore, Bob opens his email client, encrypts and digitally signs the email using the keys on his smart card. When this email reaches Alice, before she could decrypt the email, she needs to authenticate herself with PIN.

The smart card can be used together with email clients like Eudora, Microsoft ® Outlook or Netscape® Mail, etc, to send and receive encrypted and digitally signed email.

Data security
Data on your computer needs to be secured. The information also needs to be encrypted so that only the right persons could access it.

PKI Enabler - Entrust®
Entrust Inc. was established in 1994, with headquarters in Addison, Texas. Entrust dominates a 39 percent share of the PKI software market. Entrust provides Entrust Authority™ (PKI-based security management solution), Entrust Entelligence™ (to secure Client-side applications), Entrust GetAccess™ (to secure single sign-on, identification and entitlements for Web users) and Entrust TruePass™ (to secure identification, verification and privacy for Web applications) among others. (6)

"When compared with its competitors, Entrust Authority stands out in the PKI market for its track record in the industry: one major revision per year; six-time FIPS 140-1 third-party certification, as well as Common Criteria EAL3; and its reputation for providing comprehensive certificate life cycle services." (7)

Remote Desktop - Citrix®
A great amount of computing work and software has been moved from the mainframe environment to the desktop. This has caused problems such as the installation of unauthorized software on computers, helpdesk visits and the ever increasing hardware

and software upgrades and the support cost increases beyond the cost of the computer itself. Therefore, these dramatically high support costs drive the companies to put some applications back on the server. And as a result, there is a substantial increase in the need for the use of smart card as network authentication device.

There are several ways to provide non-desktop based solutions, but the focus of this paper will be on Citrix® Metaframe XP™ on a non-desktop thin client manufactured by Wyse.

Citrix Systems, one of the world leaders in server-based computing solutions, has just recently released the latest Citrix Metaframe XP for Windows®, Feature Release 2. This release offers smart card support. The new Feature Release 2 "provides secure access to applications and data using smart card technologies". What are the benefits? It "simplifies authentication and enhances logon security by allowing smart card authentication to published applications, as well as "smart card aware" applications such as Microsoft Outlook®." (8)

Previously, the users have to login to the Citrix, and if they haves to run some applications that need authentication, users have to enter the application's respective username and password. Now, with Citrix Feature Release 2, users will need to logon once, insert their smart cards into the smart card readers and enter their PIN. When one opens other applications like Microsoft Outlook, it will be seamless application. No re-authentication is needed as the credentials are tied to other applications as well.

Thin Client – WYSE® Winterm™

One of the market leaders in Windows-based and application terminals and also ICA equipment is WYSE Technology, which provides thin client solutions to a multitude of corporations worldwide. WYSE Winterm thin clients are devices that run applications from central servers and at the same time, displaying the applications on user's monitor.

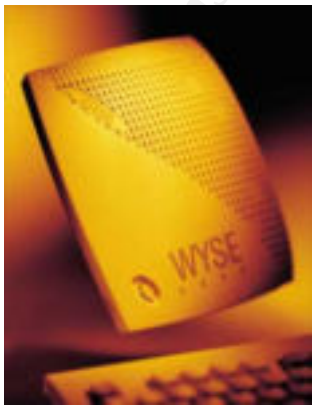

Figure 2: Winterm 3235LE. (9)

Figure 3: Smart Card Reader attached to USB port. (10)

"The Winterm Local Smart Card Add-On software for Windows CE-based Winterm 3000 Series terminals allows end users a quick and easy way to logon to their thin clients and offers administrators an even more secure thin-client environment. The add-on software, coupled with the Winterm Smart Card Manager software, allows administrators to add a local Smart Card to any Winterm 3000 Series thin client in their environment. With the use of a local Smart Card, users can automatically launch their RDP or ICA sessions without the need to enter their logon multiple times, saving time and increasing productivity. The Winterm Local Smart Card solution is the most cost-effective and easy to implement in the industry, and is excellent for environments where security and speed are a must - including healthcare, kiosks, and Point of Sale." (10)

Smart Cards and Readers – SchlumbergerSema

SchlumbergerSema, a business unit of Schlumberger Limited is the world's leading smart card provider. Gartner Dataquest Worldwide Chip Card Market Share 2001: Card Vendors and Semiconductor Vendors reported that SchlumbergerSema shipped 198 million smart cards last year. This values accounts for 29% of the total shipments in the world. Schlumberger offers myriads of different types of smart cards. The table below illustrates the microprocessor cards catering for securing information security, network and physical access.

Product	EEPROM	OS	Compliance	Security	Description
Cyberflex Access	32K	Java 2.1	VOP 2.0.1	DES, T-DES, RSA, SHA-1	Multi-application card for digital credential security
Cryptoflex	8K, 16K	Schlumberger		DES, T-DES, RSA 1024 bit	Secure portable identity with PKI cryptography
Cryptoflex for Win 2000 & Win XP	8K	Schlumberger		DES, T-DES, RSA 1024 bit	Plug & play security for Windows 2000 and Windows XP(middleware already integrated)
Cryptoflex Corporate	8K	Schlumberger	Mifare, ISO 14443 Type A	DES, T-DES, RSA 1024 bit	Dual interface card for logical and physical access security
Payflex S	450 bytes, 1K, 2K, 4K, 8K	Schlumberger	ISO 7816	T-DES	Multi-application card for identification, e-purse, loyalty, health, network access and campus applications

Table 1: Schlumberger Microprocessor cards. (11)

Schlumberger also has a wide range of smart card readers. In this paper, we are going to focus on Reflex USB and Reflex 20.

Reflex USB

The reader shown below is Reflex USB V.2 (dimension: 90 mm x 16.5 mm x 70 mm). It is to be attached on the Universal Serial Bus (USB) port with permissible data rate up to 115kbps. Reflex USB is the industry's first USB reader to offer on-board flash, which permits future firmware and software enhancements. In addition, this reader is Plug and Play and hot pluggable. Reflex USB does not need separate power supply as the reader draws power directly from the USB bus. Moreover, Reflex USB offers the ultimate in performance and user convenience. (11)

Figure 4: Reflex USB V.2 Reader (12)

Reflex 20

The figure below shows a Reflex 20 smart card reader (dimension: 9 cm x 5.5 cm x 0.4 cm) to be used in a Type 11 PCMCIA slot in notebook computers. This PC/SC Plug and Play reader is made from high quality alloy, which is built to withstand the high usage and temperature fluctuations. This reader does not need separate power supply as it draws electrical power from PCMCIA slot. The portability of Reflex 20 offers convenience for users who travel. (12)

Figure 5: Reflex 20 Reader (13)

Smart Card Reader Compatibility
To check the compatibility of smart card readers with the various Microsoft platforms (i.e. Windows XP, Windows 2000, Windows Me) go to http://www.microsoft.com/hcl

Figure 6: Microsoft Hardware Compatibility List. (14)

D. State of the Art Developments
More and more smart card development is happening. One good example is the integration of the biometrics system into the smart card system, which will bring an authentication level beyond its most secure level: three-factor authentication, which incorporates:

- *What you ha*ve – which is your smart card
- *What you know* – which is the PIN to your smart card
- *What you are* – your biometric factor, for example, your fingerprint or retinal scan.

SchlumbergerSema and Precise Biometrix announced "the integration of the Precise Biometrics Match-on-Card™ technology with its Cyberflex Access™Java™-based smart cards. The integration enables SchlumbergerSema to bring to market smart cards that use the card-owner's fingerprint as identification authentication, instead of, or in addition to, a personal identification number (PIN)" (15)

RSA SecurID® on Smart Card
RSA SecurID solution is created and owned by RSA Security. RSA Security with headquarters in Bedford, Massachusetts, is prominent for providing technologies to secure electronic business of many corporations around the world. RSA SecurID solution

is used to protect network devices, applications, web pages and local and remote networks, among others.

RSA SecurID authenticator generates a one-time passcode every sixty seconds. The combination of user PIN and current authenticator code is valid only for that particular user at that moment in time. This solution is currently being integrated with smart card. This again, eliminates the need for multiple devices, therefore providing ROI, by lowering the cost of administration and support of enterprise security.

Time-synchronous authentication, both the token and RSA ACE/Server have internal clocks that are synchronized.

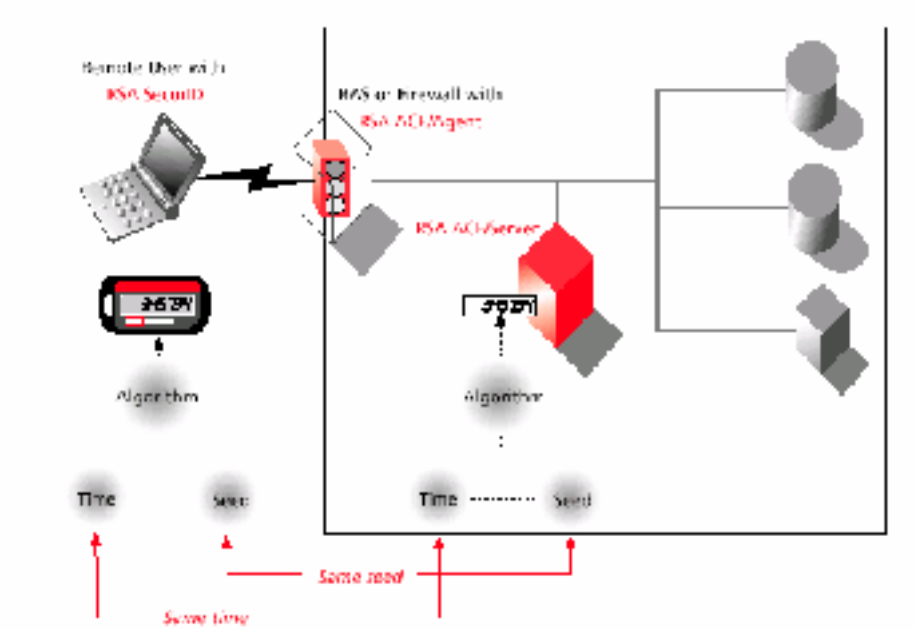

Figure 7: Time Synchronized Authentication. (16)

"Securely integrating several applications onto one platform is one of the most promising functions of the smart card. With RSA Security's established market position in two-factor authentication and e-business security and SchlumbergerSema leadership in providing secure smart card-based solutions, our strategic relationship is a win-win situation. The RSA Security and SchlumbergerSema solution helps protect valuable enterprise network resources, providing strong assurance that only authorized users can access corporate e-mail, intranets, extranets and other critical online resources," said Paul Beverly, vice president, Cards and eTransactions, North America, SchlumbergerSema. (16)

"We believe this relationship brings together complementary security expertise and technologies that provide our customers with multi-application smart cards to reduce

losses and liability, lower administrative costs and increase user convenience," said John Worrall, vice president of product marketing at RSA Security. (17)

E. **Conclusion**

As business, government agencies and healthcare organizations continue to move towards storing and releasing information via network, good security is of paramount importance. Smart cards provide powerful security, it is cost effective and convenient. In addition, smart cards offer Return On Investment (ROI) - fully integrating physical and digital security into one single platform will eliminate redundant administration, deployment and support costs. Last but not least, smart card solutions will economically manage today's security challenges while providing a flexible technology for future security scalabilities.

F. References:

(1) SchlumbergerSema. "Press Release: Gartner DataQuest names SchlumbergerSema as world's leading smart card provider"
URL: http://www1.slb.com/smartcards/news/02/sct_gartner2805.html

(2) Entrust. "Trusted Public Key Infrastructure"
URL: http://www.entrust.com/resources/pdf/pki.pdf

(3) HID. "Contactless Smart Card Reader"
URL: http://www.hidcorp.com/products/smart/mifare_reader.html

(4) HID. "HID Mifare Reader"
URL: http://www.hidcorp.com/pdfs/smart/mifare_reader.pdf

(5) Transponder News. "A news service reporting on developments regarding the use of radio based transponder systems for commerce and scientific applications. Covering the RFID technologies, EAS technologies and magnetic coupled techniques."
URL: http://rapidttp.com/transponder/presre22.html

(6) Entrust. "Enhanced Internet Security"
URL: http://www.entrust.com/products/index.htm

(7) Gartner. "Entrust Authority PKI Product"
URL: http://www.gartner.com/reprints/entrust/90697.html

(8) Citrix. "What's New. Citrix Metaframe XP for Windows, Feature Release 2"
URL:
http://download2.citrix.com/ctxlibrary/products/pdf/Whats_New_in_MF_XP_FR2.pdf

(9) Wyse. “Secure, Managed Winterm Thin Clients”
URL: http://www.wyse.com/products/winterm/index.htm

(10) Wyse. “Winterm Smart Card Solution”
URL: http://www.wyse.com/products/accessories/smartcard.htm

(11) SchlumbergerSema. “Smart cards”
URL: http://www1.slb.com/smartcards/products/smartcards.html

(12) SchlumbergerSema. “Reflex USB V.2 Readers”
URL: http://www.reflexreaders.com/Products/Reflex_USB/reflex_usb.html

(13) SchlumbergerSema. “Reflex 20 Readers”
URL: http://www.reflexreaders.com/Products/Reflex_20/reflex_20.html

(14) Microsoft. “Microsoft Windows Hardware Compatibility List”
URL: http://www.microsoft.com/hcl/

(15) SchlumbergerSema. “SchlumbergerSema and Precise Biometrics integrate smart card authentication technology”
URL: http://www1.slb.com/smartcards/news/02/sct_precisebio1902.html

(16) RSA. “RSA SecurID Authentication. A Better Value for a Better ROI”
URL: http://www.rsasecurity.com/products/securid/whitepapers/BVBROI_WP_1201.pdf

(17) Citrix. “Product Brief: Feature Release 2 for Citrix Metaframe XP for Windows”
URL:
http://download2.citrix.com/ctxlibrary/products/pdf/MetaFrame_FR2_Product_Brief.pdf

(18) RSA. “The Smart Badge: Securing PCs, Networks and Buildings”
URL:
http://www.rsasecurity.com/products/securid/whitepapers/SDSB_WP_0302.pdf

(19) Entrust. “An Introduction to Cryptography and Digital Signatures”
URL: http://www.entrust.com/resources/pdf/cryptointro.pdf