April 2002

PKI Note: Smart Cards

For many years, particularly in the United States, smart cards were considered a technology solution in search of a business problem. Recent trends, events and innovations with regard to smart cards and their use with digital certificates suggest that this is no longer the case. Smart cards are a "something you have" authentication factor, which can secure and enhance PKI technology and at the same time PKI technology can enhance the use of smart cards. Smart Card technology takes advantage of a ubiquitous form factor and the security of Integrated Circuit Chip technology to provide a degree of strong authentication. This PKI Note provides an overview of authentication tokens, discusses smart card technology, and presents the benefits of smart card technology.

Authentication

The ability to verify and validate that an individual is actually the person with whom one is intending to communicate or conduct a transaction is called authentication. There are only three ways to authenticate an individual: knowledge factor (something a person knows), possession factor (something a person has), or a biometric factor (something a person is). These factors can operate in any combination for increased security and provide "multifactor authentication" – refer to PKI Note **Biometrics** for a general discussion on authentication factors.

Possession factors are something an individual "has," such as a door key, an employee badge, or even a cryptographic key. Physical tokens offer a wide variety of authentication techniques, ranging from simple tokens (e.g., door key), to data readable tokens (e.g., magnetic stripe cards), to tokens with processing capabilities (e.g., smart cards) including cryptography. In general, the custody of a physical token provides assurance that the holder is the authorized individual. This custody is typically evidenced by data that can be validated to have originated from a particular token. The validation process has a higher level of assurance when cryptography, such as a digital signature, is used to provide integrity and authenticity of the token data.

The decision in the virtual world as to how authentication should be performed is quite similar to the way in which we understand it in the more commonplace physical world. As an example, most people have had to decide whether to lock their possessions through the use of a key lock versus a combination lock. In terms of authentication, the key lock is the possession factor whereas the combination lock correlates to the knowledge factor. The similarities, however, do not end there, as consideration of some of the difficulties includes: contingency (what if the key is lost or the combination number forgotten?), convenience (is it easier to simply remember a number or to have to carry a key?), effective security (safe crackers have their favorites!), and cost (the least analogous to the virtual world, because this is a primary consideration as possession significantly increases costs).

Acknowledgements

PKI Note: Smart Cards is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Authors:

Eric Longo
KPMG LLP

Jeff Stapleton
KPMG LLP

Table of Contents

Authentication 1

Smart Cards and PKI 2

Token Technologies 2

Smart Cards 3
- Smart Card Industry 3
- Smart Card Technology 4
- Industry Interoperability 5
- Dual Interface Card 6

There are numerous benefits to implementing PKI enabled smart cards as an identity management architecture. Non-repudiation, which can be achieved by using digital signatures, is a combination of integrity and authentication that can be proven to a third party. The relative strength of digital signatures, notwithstanding the strength of the underlying asymmetric cryptography, relies on the access control procedures established and enforced over the private key.

- Smart cards provide an easy-to-use, familiar, portable form factor to securely store an individual's private signature key. Security related to removable media protecting the location of the private key is increased. A significant benefit from this is the ability for an individual to utilize his/her smart card at various terminal locations (e.g., login to numerous PCs at various locations).
- Security related to removable media protecting the location of the private key is increased, as it is exceedingly difficult to borrow or steal something that isn't there.
- Smart cards provide a tamper resistant security module in which to generate asymmetric key pairs, securely store private signature keys, and generate digital signatures. Security related to physical access controls over the private key is increased.
- Smart cards can provide local authentication (e.g., PIN, biometric) of the individual to the card to activate the integrated circuit chip. Security related to logical access controls over the private key is increased.
- Smart cards provide multi-application capability coupled with a multi-function form factor that is virtually ubiquitous. Hence, digital signatures can be readily enabled for a multitude of applications that support smart cards.

Critics argue that smart cards are confounded by the same problems as PKI, such as interoperability, scalability, lack of widespread acceptance and support and, most importantly, no realistic business case. A compelling argument can be made for each of these positions as well as the merits (or demerits in this case) for using smart cards within a PKI environment, but the most compelling counterargument is the fact that PKI enabled smart cards currently offer the best combination of flexibility, security, and cost among token technologies, and smart cards will continue to offer more functionality at decreasing costs. To quote a recent Washington Post report, "smart cards have finally arrived in the U.S."

PKI enabled smart cards currently offer the best combination of flexibility, security, and cost among token technologies, and smart cards will continue to offer more functionality at decreasing costs. To quote a recent Washington Post report, "smart cards have finally arrived in the U.S."

Token Technologies

There are a number of considerations when making the decision on a particular authentication token technology. The decision should be based primarily on security requirements as well as financial considerations. The diagram[1] below illustrates various authentication token and hardware encryption technologies and their respective positions of cost relative to security.

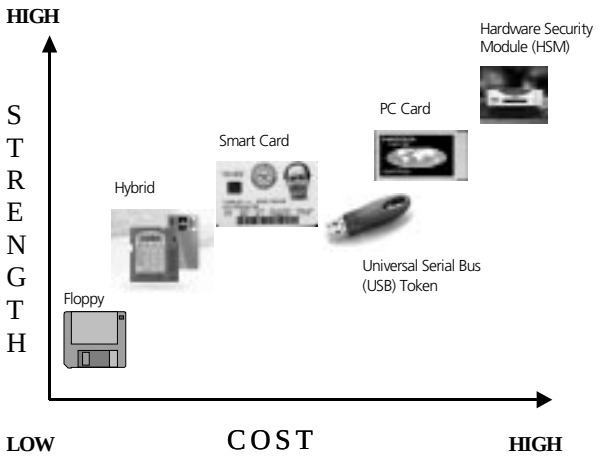

Figure 1 - Authentication Tokens

[1] In November 1999, the Department of Defense commissioned a study examining and comparing the various authentication token technologies. The basic categorization of the diagram is taken from this study.

Hardware Security Modules and PC Cards have the highest security, but also entail the highest costs. Their major disadvantage is their bulky form factors, which tend to make them unsuitable for personal use. Even PC Cards are not wallet size.

USB Tokens have moderate costs and their major advantage is their ubiquity, as most desktops and laptops now have USB ports. Their major disadvantages are the physical wear on the plug-in interface, the fact that USB is only supported by the Microsoft operating systems and the inability to include multifunction capability (i.e., photo, magnetic stripe, bar code, etc.).

Smart cards are the only token technology that provides multi-application capability coupled with a multi-function form factor that is virtually ubiquitous.

Smart cards are the only token technology that provides multi-application capability coupled with a multi-function form factor that is virtually ubiquitous. The form factor benefits are difficult to argue against. No other token can function easily for both physical and logical access and at the same time fit into standard wallets. The ability to have magnetic stripe, bar code, contact and contactless chips and photo on one form factor is perhaps its greatest benefit. Also, smart cards are slightly more evolved technologically than USB tokens, so many vendors provide applications residing on the chip for various purposes (e.g., e-purse functionality, loyalty programs, cryptographic operations).

Other form factors such as read-only magnetic stripe cards and software tokens have the lowest security, but typically with lower costs. Read-only tokens are often susceptible to replay attacks and must rely on application software; however software and software tokens are vulnerable to viruses and Trojan attacks, such as capturing keyboard strokes to determine passwords.

In general, token technology satisfies requirements for portable authentication and is becoming increasingly prominent as the need to authenticate and identify the individual (not solely the PC) grows in the marketplace. However, a crypto-coprocessor will be necessary (and is becoming standard) to provide satisfactory response times when using smart cards with PKI. Furthermore, standards are necessary to facilitate and promote interoperability.

Smart Cards

The global smart card market is difficult to assess in quantitative terms and is fraught with conflicting data.

This section discusses industry and technology trends, and issues regarding interoperability.

Smart Card Industry

Smart card technology is not nearly as "new" as many people might think. The technology has been in existence for almost 30 years (original patents were filed in France in the early 1970s). Europeans continue to use the cards regularly for a wide variety of applications including stored value (pay phones, vending machines, parking, etc.) as well as health data storage and electronic purse applications. The global smart card market is difficult to assess in quantitative terms and is fraught with conflicting data. One report claims that the total smart card market consists of approximately 320 million units sold in Europe accounting for about 26% of the total worldwide microprocessor smart card market.[2] At the same time the Gemplus annual report states that Gemplus alone sold more than 200 million units in 2000 alone, and, according to some sources, it is unlikely that Gemplus accounted for 63% of the total European market for smart cards in 2000.

The results from a comprehensive survey of the smart card manufacturers on behalf of the Smart Card Alliance yielded a somewhat surprising reality check.[3] In 2001 more than 41 million smart cards were manufactured for use in the United States and Canada. This is more than twice the number reported for 1999. The vertical market category with the largest share was the Wireless/Telephony segment with 37% of the total. This is primarily due to the

[2] Please refer to the following URLs for additional information: http://www.epaynews.com/statistics/scardstats.html#1 and http://www.idc.com/getdoc.jhtml?containerId=pr2002_03_12_133258.

[3] The more recent KPMG study can be interpolated with the previous (1998) study by the Tower Group to demonstrate the shift in vertical market breakdown for smart card use in the United States (for more information please refer to: http://egov.gov/smartgov/tutorial/html).

smart card chip's increased use within cellular phones. The astounding number that came out of this survey was the increased use for the government vertical market. The rate of growth within this segment was a purported 1,500% and it is likely that much of this increase is connected to the U.S. Government's commitment to PKI. What this study demonstrates most clearly, however, is that there is tremendous room for growth. The health care vertical market accounted for less than 1% of the total, and the number of smart cards manufactured for use in the rest of the world is more than twenty times the total for North America.

The number of smart cards manufactured for use in the rest of the world is more than twenty times the total for North America.

The value chain within the smart card industry is quite complex. Participants include semiconductor manufacturers, card manufacturers, reader and host device manufacturers, software and related services providers (including applications, card management system and key management), personalization providers and issuers. Examples of silicon providers include Infineon and Phillips. The primary smart card technology (e.g., common operating system) platform providers are Microsoft (Smart Cards for Windows), Sun Microsystems (Java Card platform) and Mondex (Multos OS platform). The top five smart card manufacturers, with approximately 90% market share, are Gemplus, Schlumberger, Oberthur, G&D and Orga. In addition to the smart card manufacturers there are a large number of smaller peripheral smart card software and other related smart card services providers such as CardBASE, ActivCard, Datakey and Rainbow.

Smart Card Technology

A number of events and trends have occurred technologically in the last few years to propel smart cards from being perceived as a "bleeding edge" technology to more appropriate monikers such as "cutting edge" or "disruptive" (and perhaps in Europe simply 'smart'). The following are some of the smart card industry and technology trends that are currently being evidenced in the marketplace:

- Memory requirements are increasing as applications mature; "Entry Level" today is at least 4K and commonly 16-32K Byte, "Entry Level" tomorrow will be at least 64K Bytes[4] (Infineon Technologies state of the art chip, the SLE 88CX642S, is a 32-Bit RISC processor with 72K of EEPROM).
- Crypto processing will be more important, as will processing larger key-lengths (and factoring prime numbers for asymmetric algorithms). Until recently, it took a painfully long time to generate asymmetric keys on the card and while standard practices do not necessarily warrant this, the capability is there and certain government entities demand it.
- Shorter lead-times and delivery turn-around will be expected. One simply needs to ask the U.S. Department of Defense how long it took to place an order for and receive a large number of cards two years ago and then compare that process to today to discover that the manufacturers (and silicon providers) have come a long way.
- Full duplex, higher I/O speeds are now available and will soon be advanced through ISO and ANSI. The baud rate bottleneck (9600 as defined by ISO) is always being challenged and improved. USB interfaces dramatically improve data transfer rates.
- Dual interface as an alternative to combi-card is being offered (see "proximity" discussion below).
- Faster processor speeds and increased battery capabilities will be an important feature. Industry power requirements are already at "3 volts V_{cc}" and moving to even lower voltages.
- Price competitiveness is the overriding driving factor for the card industry and will continue to commoditize the cards and components. Customers demanding the "open" architecture card platforms for their infrastructures create a more level playing field and drive the components themselves to become more commoditized.
- Multiple application capability is becoming "preferred" in next generation card solutions, and highly complex "Crypto" applications for Inter/intra-net access control/payment are emerging.
- Java Cards are now achieving FIPS 140-1 level 3 certification.

Price competitiveness is the overriding driving factor for the card industry and will continue to commoditize the cards and components.

[4] Smart cards are typically characterized by the amount of non-volatile program and data memory, which usually is in the form of Electrically Erasable Programmable Read-Only Memory (EEPROM).

- New specifications including: PC/SC, Java 2.1, EMV, ETSI, GSM, Proton, Mondex, CEPS, IATA 791(B), etc. are becoming "standard" and threshold requirements (see "Industry Interoperability" discussion below).
- Increasing support for smart cards in Windows platforms, specifically Windows 2000 and XP. Both from a reader and application standpoint, Microsoft has made it much easier for the installation, use and deployment of smart card technology.
- Smart card readers are becoming more commonly available as standard equipment on laptops (e.g., Acer) and PCs (e.g., Compaq's built-in smart card reader keyboard).

Multiple application capability is becoming "preferred" in next generation card solutions, and highly complex "Crypto" applications for Inter/intra-net access control/ payment are emerging.

Industry Interoperability

CEN (Comit Eurpen de Normalisation) and ISO 7816 Information Technology – Identification Cards – Integrated Circuit Cards with Contacts is a multipart international standard defining smart card specifications. This standard defines the physical and electrical characteristics as well as transmission protocols. It is not a perfect standard in that adherence to its requirements does not in and of itself produce interoperability. It does, however, enable interoperability and serves as a starting point for the manufacturers and smart card software companies. When combined with certain specifications, this standard actuates a sufficient degree of interoperability. The following table depicts some of the most commonly accepted specifications as they relate to both physical and logical authentication of smart cards to systems and a URL for obtaining more information about them:

Standard or Specification	Primary Sponsoring Organization(s) or Company (Companies)	Purpose and Informative URLs and links[5]
ISO 7810 ISO 7816	CEN/ISO	Defining smart card standard. Creates standards for Integrated Circuit Cards and interindustry use of plastic cards. http://www.iso.org/iso/en/ISOOnline.frontpage http://www.scia.org/knowledgebase/default.htm http://cuba.xs4all.nl/~hip/iso7816.txt
ISO 14443	ISO	Defining RFID proximity smart card standard (2 types with different modulation specs) http://www.iso.org/iso/en/ISOOnline.frontpage
PC/SC	Microsoft	Smart card reader architecture specification for PCs. http://www.pcscworkgroup.com/ www.microsoft.com
OCF	Sun Microsystems	Smart card reader / CAD (Card Access Device) specification. www.opencard.org
EMV	EuroPay/Mastercard/Visa consortium	Develops industry-wide chip card specifications to ensure interoperability of smart cards and card terminals for financial industry cards. http://www.emvco.com/
JavaCard 2.1	Sun Microsystems	Java-based smart card specification. http://java.sun.com/
PKCS	RSA	API specifications (PKCS #11 and 15 apply to cryptographic smart card functions). http://www.rsasecurity.com/rsalabs/pkcs/index.html
Global Platform (formerly Open Platform)	Visa	Comprehensive smart card and terminal specifications for application loading and management. http://www.visa.com/openplatform/ http://international.visa.com/fb/paytech/productsplatforms/globalplatform.jsp
GSA Interoperability Specification	General Services Administration	www.gsa.gov

Figure 2 - Industry Interoperability

PKI enabled smart cards currently offer the best combination of flexibility, security, and cost among token technologies, and smart cards will continue to offer more functionality at decreasing costs.

[5] These reference URLs are not intended to be representative of official sites but rather a collection of useful references that years of research have turned up.

In addition to the previously noted standards and specifications, a number of organizations (e.g., NIST, Visa, etc.) have developed "Protection Profiles" for smart cards which have been adopted by the Common Criteria guidelines and certification.

The major smart card manufacturers include Gemplus, Schlumberger, Oberthur, G&D, and Orga. These companies along with some other niche PKI smart card software providers such as ActivCard, Datakey, Litronic, OpenCARD, and now RSA provide the cards and/or the requisite software for implementing a smart card solution.

Easy subsequent (dynamic) addition of applications/software is a direction that many large organizations (e.g., Visa, American Express, Department of Defense) are migrating toward. The consensus in the industry is that for this to happen effectively, Sun's Java Card specification, including the technical requirements for developing and presenting dynamic loading of applets, should be utilized. The "buzz" in the smart card industry these days is that after many years of Sun Microsystems' Java card platform competing aggressively with Microsoft, the platform of choice for issuers is and will be Java based.

Dual Interface Cards

Many organizations are beginning to issue and utilize smart cards internally in order to combine physical and logical (e.g., PKI) access controls with the multifunction form factor. Unfortunately, many companies have made the decision to issue smart cards within a corporate environment and failed to keep in mind the potential control related issues between the physical security personnel / management and the network access or information technology (IT) department personnel / management. For logical and physical access projects, someone should be appointed to oversee the two groups or, at the very least, obtain the support of the person who has oversight of both groups (if it's a single individual) or the buy-in of both departments if they are separated organizationally. If neither department relinquishes control then it is possible to use a combi (2 chip contact and contactless) card product maintaining separate databases and data flows. If they can work together, a dual interface card is probably the right solution. The difference is primarily related to the processing of "real estate" and memory allocation on the chip.

Regarding the use of a dual interface card, it is important to note that the popular (at least internationally) Mifare product and an ISO Type 14443A compliant product are not identical. Even though 14443A products are based on Mifare they are not upward compatible from the security system POV. 14443A has the card act like a microprocessor card contactlessly, versus Mifare, which is really a memory product. If an existing Mifare system is in place, then a combi card is probably more economical, versus having to upgrade the firmware at the physical reader locations to accommodate the 14443A product.

Also, there have been a number of vendors, such as Cubic, Sony and ERG, trying to push other types of ISO 14443 products as a part of the standard; however, there is an approved Type A-Mifare-Philips-Hitachi-Infineon and Type B-NEC-ST-MOT. This would have been akin to not having a standard at all but rather a large number of vendors' proprietary specifications. The bottom line with regard to smart card proximity devices and integration is that it should be carefully planned to avoid the pitfalls of becoming dependent on a single vendor's solution that may not be able to sustain itself in the marketplace.

Another physical access solution is the HID 125khz proximity card, which can be used on its own or in combination with a contactless smart chip (i.e. MIFARE) along with the contact smart chip.

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to under-stand and exploit the value of PKI in their e-business applications.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810