



www.css-security.com • 425.216.0720

Deploying Smart Cards in Your Enterprise

The merging of *physical* access technology with public key-enabled smart card technology has been an emerging trend that has occurred in the security industry over the past few years.

While Public Key Infrastructure, smart cards, and physical security devices have all been around for many years, the convergence and overall maturity of these technologies is beginning to make their widespread use a real possibility for many corporate environments. In addition, the wide variety of feature sets and form factors can make the task of product selection quite difficult, but also makes it possible for an enterprise to find solutions that better suit their needs than in years past.

May 05

Introduction

An emerging trend that has occurred in the security industry over the past few years is the merging of *physical* access technology – such as magnetic stripe cards and readers or proximity readers – with public key-enabled smart card technology.

This convergence now allows the possibility for an enterprise to deploy a “single card” solution, where one card could serve as an employee ID badge and automated building access card, as well as a secure token which can provide a wide variety of public key functionality.

This document is intended to provide a brief introduction to smart card technology, as well as describe how a smart card deployment might be handled in an enterprise environment, and the impact and considerations necessary for such a deployment.

Background Information

Smart Card Basics

A smart card is a credit card-sized piece of plastic, with a small microchip embedded on the face of one side. The microchip is actually a very small computer – complete with an operating system, application software, permanent storage, and I/O communication facilities. Smart cards have been around since the mid-1980's, but to date have been far more prevalent in Europe than in the United States.

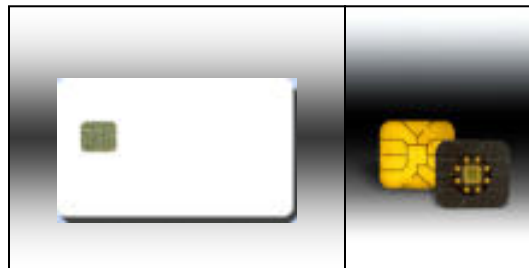


Figure 1: A Smart Card and close-up of the Embedded Chip

Unlike a normal computer, however, a smart card contains no batteries or power source of any kind. It therefore is only usable when inserted into a smart card *reader*. The word “reader” is actually a bit of an understatement in this case; a smart card reader is actually responsible for providing power to the chip, as well as communicating with the operating system and applications on the card. This communication amounts to sending commands to the card, and retrieving the results of those commands. There is no such thing as a smart card “writer” – all smart card readers are capable of sending information to a smart card, and receiving information from the card in return. What happens to the information sent to the smart card is entirely up to the operating system and applications on the card.



Figure 2: Smart Card Reader

Smart card readers come in many forms. Some smart card readers are intended to be “stand-alones” – battery powered devices which have their own displays and user input capabilities for allowing a person to interact with a smart card. However, most smart card readers are intended to be connected to a computer, and allow the computer and its user to interact with the card. The connection to the computer can take many forms as well – there are readers which connect via serial port, parallel port, USB, or laptop PCMCIA slots. A handful of companies now offer desktop computer keyboards with smart card readers built in. There are even smart card readers for PDA devices.

A series of International standards (ISO 7816) are intended to ensure that all smart cards are interoperable with all smart card readers. This is generally the case; however there are occasionally compatibility problems that crop up between certain cards and readers.

Smart Card Applications

Smart cards have been used in a variety of applications: cell phones, set-top boxes for cable and satellite television, loyalty programs, meal plans, cell phones, secure credit card payments, and much more. The types of smart card applications of interest to most corporate environments, however, are *PKI-enabled* cards, which allow the storage of digital certificates and their associated RSA keys, and can perform digital signatures and encrypt data with those keys.

These cards and their cryptographic keys are nearly always protected by a PIN or password, which the card owner must enter in order to use his card. This prevents someone other than the owner from making use of a lost or stolen card. Most cards also have some means of “locking” the card after a certain number of incorrect PINs are entered (generally between 3 and 10), to thwart PIN-guessing attacks. In addition, most cards have some means of unblocking a card once it has been locked, by entering a special unblocking PIN code. Usually these cards will permanently disable the card if too many incorrect unblocking codes have been entered.

PKI-enabled smart cards can be used for an ever-widening variety of applications, such as:

- ♦ **Network Login.** Microsoft’s smart card login capability comes standard with all versions of Windows from Windows 2000 and above.
- ♦ **Remote Access.** Smart cards could be used for employee authentication when establishing a VPN connection to the client over the Internet.
- ♦ **Wireless Networking Authentication.** Wireless access points and authentication providers could be configured such that access to the client wireless networks would require a smart card – a dramatic improvement over traditional wireless authentication methods.
- ♦ **Secure Email.** Lotus Notes includes smart card capabilities via PKCS#11 starting with version 6.02. This would allow users to sign and encrypt email with their smart card.
- ♦ **PGP.** PGP has included PKCS#11 functionality in corporate versions of the software since version 7.0.
- ♦ **SSL.** Smart cards and their digital certificates could be used to authenticate users and secure communications to both internal and external websites.

Each of these usage scenarios carries a different set of concerns and considerations which must be addressed before deployment. These will be touched on later in this document.

Smart Cards in the Windows Environment

While most smart cards and readers are interoperable, the cards themselves are not: one vendor’s card may work completely differently than another’s, and provide drastically different functionality. To allow easier integration with software applications, standard interfaces have been created which abstract the card-specific elements to a well-defined set of APIs.

Deploying Smart Cards in Your Enterprise

The two primary ways for applications to communicate with smart cards or other cryptographic tokens are via a PKCS#11 interface, or by a Cryptographic Service Provider (CSP). PKCS#11 is an industry standard programming interface for dealing with cryptographic tokens, on a variety of computing platforms, including both Windows and Unix-based operating systems. The CSP interface is a Microsoft creation which allows applications to use Microsoft's CryptoAPI to communicate with cryptographic devices.

A diagram of how these components integrate with various applications is given below:

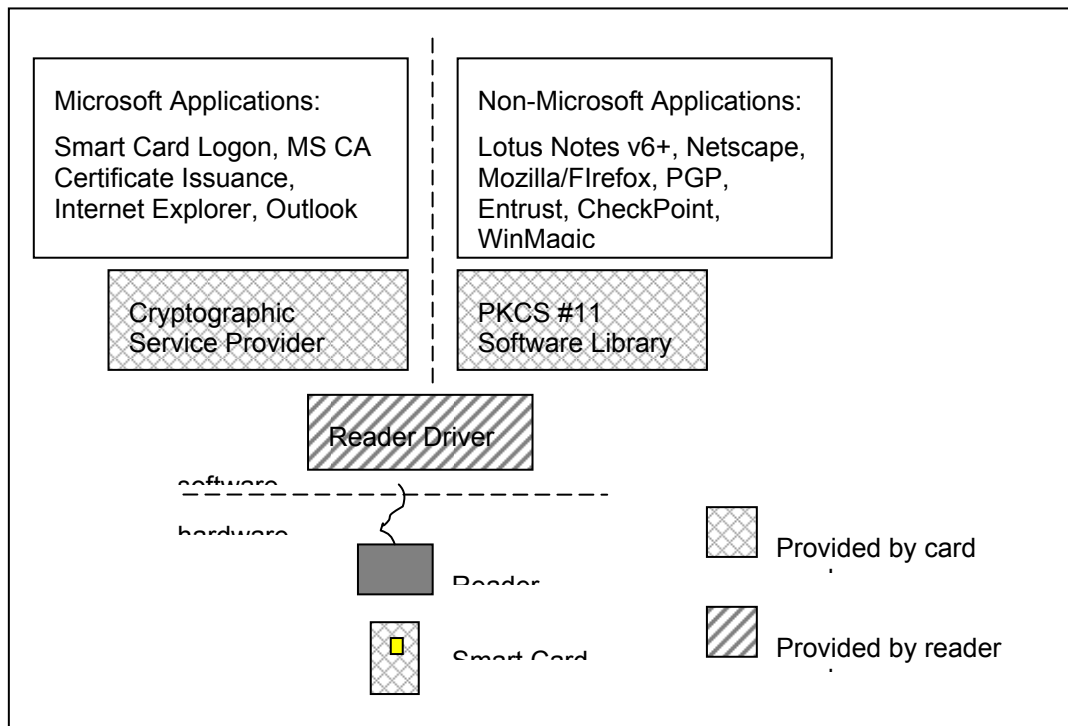


Figure 3: Smart Cards and Associated Software

Smart Card Benefits

The cost of a smart card deployment can vary greatly depending on volume, but often ranges from \$50 to \$80 per user, including the card, reader, and associated software. Given this additional cost, it is reasonable to ask what benefits may be derived from using smart cards in an enterprise environment. Some potential benefits are given below:

- Two-factor authentication. Most IT environments require users to authenticate via username and password – “something you know”. Requiring a PIN-protected smart card for authentication leverages an additional factor: “something you have” (the card), plus “something you know” (your PIN). This higher degree of assurance can help increase the security posture of a network environment.
- Non-Repudiation. Most PKI-enabled smart cards are capable of generating RSA public and private key pairs on the card, where the private key cannot be extracted from the card under any circumstances. Therefore, any digitally signed email or documents created using these keys must have come from someone who had access to the card and knew its PIN code.

Deploying Smart Cards in Your Enterprise

- ♦ **Less Dependence on Passwords.** Since they are never sent over the network, card PIN values generally do not need to be changed as frequently as network passwords do. Windows systems can be configured to allow users to log in to their computers using only their card and their PIN, rather than a network password. This would even enable a scenario in which users did not even know their network password.
- ♦ **Automatic Screen Locking.** Systems can be configured in such a way that the user's screen is automatically locked when their smart card is removed from the reader; the user would then be required to re-insert the card and enter their PIN to regain access to his computer. If implemented properly, this can help reduce the security threat of an unattended logged-in workstation more effectively than inactivity timeouts.
- ♦ **Improves the Security of Kerberos.** Microsoft's implementation of Smart Card Login uses the proposed PKINIT standard for Kerberos-based login. In short, a user still receives a Kerberos Ticket-Granting Ticket (TGT) as a result of a successful login to their domain via smart card login – just as they would if they had used their password. In addition, unlike the standard password-based Kerberos login, the initial response packet from the Domain Controller is not subject to offline password-guessing attacks.

Need More Information?

The References section at the end of this document contains some references and web site links for obtaining more information about smart cards, security tokens, and the deployment of these technologies in an enterprise environment.

Usage Considerations

There are a variety of areas that must be addressed when considering an enterprise smart card deployment. Some of these will be addressed in the following sections.

Issuance / Card Personalization

For a user to be able to use his smart card, a number of things must happen:

- ♦ Many smart cards must be initialized in some way before their first use.
- ♦ The user PIN and card unblocking PIN must be set. The user's PIN should be known only to the user; the unblocking PIN should be archived in a secure location for later use.
- ♦ A certificate (or certificates) and the associated private key(s) must be stored on the card.

The manner by which these things happen is entirely up to the enterprise. There are two primary schools of thought:

- ♦ **Auto-Enrollment:** Users are allowed to request and install their certificates directly from the Certificate Authority, using their standard network credentials. This approach puts the user in control of setting his own PIN, archiving his unblocking PIN, and managing his certificate. In this scenario, the user could receive his ID card with an un-personalized smart card chip on it, and then personalize his own card at a time of his choosing.
- ♦ **Enrollment Authority:** In this scenario, the enterprise would designate a certain number of personnel as "enrollment authorities", who would be responsible for setting up a user's card on their behalf. The user would then need to change their PIN, either as a part of the initialization process, or at a later time. The enrollment authorities could either be associated with the group that prints the badges and enrolls the ID cards into the building access system, or an entirely separate group. This approach gives the enterprise a much higher degree of control over the process, but also requires more administrative overhead.

These two approaches need not be mutually exclusive – for example, in some deployments, it may be sensible to allow users to enroll their cards for *some* purposes, but require centralized control over enrollment for other purposes. In either case, it is **highly** recommended, regardless of the process chosen, that once the personalization process is complete, *only* the user knows the user PIN for their card, otherwise non-repudiation will be weakened.

Certificate Authority

A PKI smart card deployment at any organization will often require a new PKI (Public Key Infrastructure), or a new CA (Certificate Authority) to be created for the purpose of issuing certificates to smart card users. As with any certificate authority deployment, there are a number of facets to consider, including:

- ♦ **Certificate Templates:** What kinds of certificates will the CA issue? What will the certificates be used for? (Smart card login, secure email, client authentication?)
- ♦ **Certificate Revocation:** If a CA issues certificates for smart card login or remote access, it may be advisable for the CA to issue Certificate Revocation Lists (CRLs) with a relatively short validity period. For example, a CRL validity period of 24 hours will ensure that no user will be able to login to the network within 24 hours of his certificate being revoked. (Disabling the account would of course have the same effect). **Note:** there are two factors that may put a lower bound on this time period – domain replication speed, and disaster recovery time. If a CRL is not replicated through a domain or forest before it expires, major problems could result. And an enterprise must ensure that a new CRL can be published even under a disaster recovery scenario, or no users will be able to log in to the network with their certificates.
- ♦ **Certificate Usage:** Will users be using their certificates to authenticate themselves outside of the company? For example, if an employee uses his certificate to sign an email message sent to a 3rd party, the signature will be reported as invalid, unless the 3rd party user has access to the issuing CA certificate hierarchy, and has trusted them. This means that the CA certificate chain and CRLs must be made available outside the company – generally via an HTTP-based URL. Inter-organizational use of certificates may also require the use of a Certificate Policy (CP) and/or Certificate Practices Statement (CPS).

Encryption and Key Archival

If users are allowed to *encrypt* data with their certificates, rather than just sign it, key archival becomes a must, in the event of a lost card or fired employee. Of course, key archival dramatically weakens non-repudiation, since more than one person in the organization has legitimate access to the keys.

The standard solution to this dilemma is to issue each user **two** certificates – one for signatures and one for encryption. The private key for the signature certificate is created on the smart card, and is never allowed to leave the card, while the encryption certificate is generated off-card, loaded onto the card for use, and then archived in a secure location. Usage attributes on these two certificates would need to be set to enforce this distinction.

User Issues

In addition to the infrastructure issues mentioned above, there are a number of other process and procedural considerations that must be addressed for a smart card deployment. The following is a sampling of the kinds of things that will need to be discussed:

What Will Users Be Allowed to Do?

Some card management software allows users to do more than others. In general, users may be allowed to *view* their certificates, and change their PIN if desired. Other functions, such as adding or deleting certificates may need to be restricted.

Physical Badge Considerations

Will badges be removable from the badge holder for insertion into the reader? If not, the reader(s) selected must potentially be able to accept the card with the badge holder still attached.

If the users remove their badge for insertion into the reader, this may result in users accidentally leaving their workstations logged in with their cards still inserted in the reader. Some employees may resist the idea of keeping their badge on a retractable badge holder, as inserting their card/badge in the reader would essentially physically tether themselves to their computer. Another option would be to force employees to use their badges to *leave* the building, as well as *enter*, which would at least keep an employee from heading for home with his badge still plugged in to his computer.

Forgotten Badges

The physical access group will almost certainly develop some sort of provision for a user to gain access to their building in the event that their badge has been accidentally left at home. Unfortunately, if a user *needs* the digital certificates on their badge to perform his duties, the standard “temporary badge” solution will not suffice – as the only place the user’s signature key exists will be on their badge. Passwords, therefore, will often remain as a fallback authentication mechanism.

Windows 2000 and Windows Server 2003 machines have security policy settings that could disable password logon, and *force* the user to login via smart card. However, unless management is willing to force a user to return home for their badge, it is advisable *not* to use this option, and allow password-based login to the network.

Locked Cards

Most smart cards will automatically “lock” the card after some number of successive invalid PIN entries – generally 3, 5, or 10. Most cards have some sort of “Security Officer” (SO) role, with a completely separate PIN, which can be used to unblock the card. Nonetheless, some sort of enterprise procedure will need to be developed for this situation. Some possible options are:

- ♦ **Centralized Unblock:** The SO PIN is set for each card before being given to the user, and is archived securely for use in unblocking. The user will need to return to the issuing station (or person) and ask the card admin to unblock their card for them.
- ♦ **Remote Unblock:** Like the remote unblock scenario, the SO PIN is set for each card before being given to the user. Some card management systems have some sort of provision for allowing a user to unblock their card over the phone, by contacting a card administrator, and entering some information given to their during the process – in a method similar to the backup Windows XP license activation process.
- ♦ **User Unblock:** The user is ultimately responsible for unblocking their *own* card. When the card is initialized, the unblocking PIN is presented to the user, who is responsible for storing the information in a secure location. They can then retrieve this information and use it to unblock their card at a later date.
- ♦ **Re-Issuance:** When a card becomes blocked, the situation is essentially treated as if the card was lost – except that a new card would not need to be purchased. The card is “re-initialized”, and all information on the card is erased and then re-personalized from scratch.

Forgotten PINs

The forgotten PIN scenario is very similar in nature to the locked card situation. Clearly, one possible response is to simply let the user *lock* their card while attempting to guess his PIN, and then treat the resulting locked card. (Many cards will not allow an unblock to occur unless the card is actually blocked). Other alternatives would be archiving the user PINs in some location, but this has undesired effects on non-repudiation.

Lost or Damaged Cards

From time to time, it can be assumed that users will lose their cards, or damage them to a point where they are no longer usable. Procedures will need to be developed for timely re-issuance. In addition, these procedures may need to integrate with the badge printing and building access procedures.

The lost or damaged card scenario is yet another reason *not* to disable passwords for network access. Some sort of backup authentication mechanism will be needed.

Support

While a migration to smart cards for enterprise network access may well result in a dramatic decrease in password-related calls to the support desk, there is increased potential for card- or reader- related support questions and problems to arise. Support staff will need to be educated and equipped to handle the problems users may encounter in this area. In addition, they may become the first people contacted in some of the above scenarios as well – lost badges, locked cards, etc.

Smart Card Deployment Software

Many companies now offer software which can assist in managing an enterprise-wide smart card deployment. Such software can assist with card and certificate inventory, and can integrate directly with a corporate certificate authority to issue certificates to the smart cards.

Most of these products provide web portal environments for enrollment or administration, help desk support, and end-user roles. In addition, it may be useful to look for products which can support both a *centralized* and a *self-service* issuance model; with centralized issuance, an enrollment administrator enrolls a user's card and certificates on their behalf, so the user receives their card in a fully personalized state. In self-service issuance, a user receives their card in an un-personalized state, and must visit a user portal in order to personalize their own card.

Other PKI-Enabled Form Factors

In addition to smart cards, there are a wide variety of other PKI-enabled security devices. USB tokens, for example, offer all of the same cryptographic functionality as a smart card, in a form factor which resembles a USB flash memory drive. These tokens are made by a large number of vendors – many of which are also smart card vendors – and do not require the use of a separate smart card reader. Some vendors have even released tokens which combine a visual one-time password (OTP) display, and a PKI-enabled USB device.

Like smart cards, they can be integrated with physical access control systems such as proximity devices; however, due to their size, they cannot be used as a replacement for corporate identity badges. In many corporate environments, however, this is not a concern.

Such devices are mentioned here because many of the same applications and deployment issues that apply to smart cards also apply to USB PKI tokens.

For the Future

Smart card technology, and the variety of smart card and card-enabled applications available, continues to increase on a daily basis. An enterprise smart card deployment opens up a wide variety of additional options which could be leveraged at a later date. Some future options or uses of smart cards will be presented for consideration here. These are not necessarily recommended for an initial roll-out, but could be added at a later date if deemed worthwhile.

Java Card Applets

Many card vendors offer Java-based cards, which run a special card operating system that is extendable by loading new applications onto the card. For example, a Java card with a PKI applet capable of meeting an enterprise's needs could be extended with new applications such as loyalty programs, secure payments, or additional identification information. Many new smart cards are following this model. For example, the Department of Defense Common Access Card program, in which every member of the Armed Services and civilian employees of the DoD will be issued a smart card, employs Java card technology from a variety of vendors.

PKCS#11 and CSP development

The PKCS#11 and CSP provide standardized APIs for communicating with smart cards and other cryptographic devices. This allows for the possibility of an organization to develop their own smart card-enabled applications, which would make use of their cards in unique ways and can be specifically customized to each corporate environment.

Biometrics

Many companies now offer integrated smart card/biometrics products, such as combination fingerprint and smart card readers. Biometric templates can be stored on smart cards for safekeeping, and matched against a live scan for authenticated access.

In addition, biometric match-on-card is also available as a Java card applet, which would allow users to authenticate to their smart cards via fingerprint scan – without entering a PIN. This and related technologies may become avenues worth exploring as biometrics technology continues to mature.

Summary

While Public Key Infrastructure, smart cards, and physical security devices have all been around for many years, the convergence and overall maturity of these technologies is beginning to make their widespread use a real possibility for many corporate environments. In addition, the wide variety of feature sets and form factors can make the task of product selection quite difficult, but also makes it possible for an enterprise to find solutions that better suit their needs than in years past.

Due to these factors, CSS believes that corporate PKI and security token deployments will accelerate rapidly over the next few years.

References

1. Smart Card Alliance: Nonprofit smart card advocacy group: <http://www.smartcardalliance.org/>
2. International Standards Organization (ISO): Electronic copies of the ISO 7816 smart card set of standards: <http://www.iso.org>
3. Smart Card Deployment at Microsoft: Article about Microsoft's use of smart cards for remote access: <http://www.microsoft.com/downloads/details.aspx?FamilyID=fc694186-ce2b-4e01-b80d-35847c47303b&DisplayLang=en>
4. Microsoft Technet Article on smart card deployments:
<http://www.microsoft.com/technet/security/topics/smrtcard/smrtcdb/default.mspx>
5. EMV: Secure credit card payments via smart cards: <http://www.emvco.com/>
6. M.U.S.C.L.E: Smart card effort for Linux platforms: <http://www.linuxnet.com/>