Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Making Smart Cards Work In the Enterprise

Will smart cards improve security in the enterprise environment? Smart cards offer a secure and convenient form factor on which employees can carry digital credentials for accessing parking facilities, buildings, computers, and network resources. Indeed, the ability for an employee to carry both physical and logical access credentials can be provided on a single card. Adding to the significance of smart cards, that same card can also be used for employee photo identification, and potentially a multitude of other applic...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Making Smart Cards Work In the Enterprise

© SANS Institute 2002, Author retains full rights.

Security Essentials
GSEC Practical Assignment
Version 1.3

Brett Lewis

04-Apr-2002

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Summary

The time has come for enterprises to begin considering whether smart cards can be used to improve security in their environments. Smart cards offer a secure and convenient form factor on which employees can carry digital credentials for accessing parking facilities, buildings, computers, and network resources. Indeed, the ability for an employee to carry both physical and logical access credentials can be provided on a single card. Adding to the significance of smart cards, that same card can also be used for employee photo identification, and potentially a multitude of other applications, including encryption, digital signatures, secure storage of employee medical information, and electronic wallet for cafeterias and vending machines. Done right, a single-card solution can provide return on investment in the forms of vastly improved security, reduced need for certain security and IT personnel functions, and customer satisfaction.

This paper examines some of the key benefits that can be realized from employing smart cards, and it explains how smart cards can be used to significantly improve both physical and logical security. Additionally, it provides an overview of some strategic infrastructure elements needed to make smart cards work in an enterprise environment, including complimentary technologies, personnel, hardware, software, and perhaps most importantly, policies and procedures.

What Are Smart Cards?

A smart card is a plastic plate about the size of a credit card, with an embedded integrated circuit chip that provides either memory only, or memory along with a programmable microprocessor. Smart cards are designed to be tamper resistant; most – even the memory-only types – contain logic that specifies the rules for accessing the onboard read/write memory; thus the content of the memory is protected. Many microprocessor type chips are manufactured with special coprocessors and logic to perform cryptographic functions onboard the card. The amount of memory, which is EEPROM (Electrically Erasable Programmable Read-Only Memory), on both types of chips ranges from 8K to 256K bits, with the trend going toward higher amounts of memory.

Like any other computers, smart cards must interface with external systems to be of value; to accomplish the exchange of input/output, smart cards use either a contact or a contactless interface. Contact type cards must be inserted into a reader to make physical contact with it; the reader provides power to the card and exchanges input/output via the physical contacts. Standards for contact cards are defined in ISO 7816. The contactless type card exchanges input/output via induction, and typically is powered by that same inductive circuit. Essentially, this means that the card, which has an embedded wire antenna wound around its perimeter, is activated via radio frequency when it is placed near the reader. The operating distance for contactless cards is relatively short; some types work at up to 10 cm (4 inches), others at up to about one meter. Mifare®, an open technology developed by Philips Semiconductors, is fully

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

compliant with ISO 14443A, and seems to be the de facto industry standard for contactless smart cards. [i]

To help facilitate multiple applications on a single card, manufacturers commonly embed both contact and contactless type chips on the same card to create hybrid cards. Additionally, there are 'combi' cards on the market that provide both contact and contactless functionality via a single chip. Furthermore, other card features, such as bar codes and magnetic stripe, can be integrated into the same card as contact and contactless integrated circuit chips.

Further information about smart card technology is available from many resources on the Web. A nice multimedia tutorial is available on the US General Services Administration (GSA) eGovernment web site.[ii] For a more technical description of how smart card technology works, refer to Dr. David B. Everett's paper on the Smart Card Group web site. [iii] For an excellent overview of standards that apply to smart cards, refer to the US General Services Administration document entitled "Smart Card Policy and Administrative Guidelines". [iv]

Applications

For enterprises contemplating the use of smart cards, the following four primary applications should be considered. While each one of these applications is a compelling use for smart cards, the real beauty of an enterprise smart card program is that a single card issued to each employee can be used for all of them. RSA Security presented a web seminar on this topic (it is now available via the web on demand); their use of the term "smart badge" makes sense in referring to a single-card solution to multiple enterprise applications. [v]

- Employee ID badge – Many organizations already utilize employee badges as part of their physical security program. When smart cards become part of the plan, it makes perfect sense to customize the card with a photograph of the employee to whom the card is issued, along with the employee's signature, the organization's logo, the badge expiration date, and other features that pertain to the organization and/or the employee's department.

- Building access – Controlling physical access to buildings and other facilities such as parking garages can be accomplished in part via smart cards. As is the case when any security controls are put in place, designing this solution entails a balancing act between the level of security and the amount of convenience in using the system. Often contactless smart cards are used for physical access because they provide a good balance of security and convenience – users need only touch the card to the reader. In contrast, with other types of cards, including contact smart cards, magnetic stripe, and bar code, the user must insert or swipe the card in a certain way in order for it to be read.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- PC / network logon – There are two basic ways that smart cards can be used to authenticate users for PC and network access. The first way is to store passwords for multiple applications in the card's tamper-resistant memory. With this method, the system reads the password from the card when the user inserts it into a reader. Typically the user must also type a PIN (Personal Identification Number) to access to the secure storage on the card. This method is arguably a significant improvement over normal password systems, which suffer such abuses as users writing their passwords on sticky pads, and shoulder surfers attempting to glean passwords by watching the keystrokes of authorized users during the logon process. However, the second of the two ways offers an even stronger method of authentication via the use of digital certificates. More information about certificate-based logon is presented in the section on "Benefits" herein.

- Remote network access – Essentially, this is the same concept as the PC and network logon application (above). Many organizations still allow remote access user authentication via passwords. Again, the use of certificate-based authentication using smart cards can significantly improve security over password-based methods.

Besides the above four primary applications, smart cards can potentially be used for any number of additional applications. Below are some others for consideration.

- Digital signatures and secure e-mail – Employees can digitally sign e-mail, as well as decrypt secure electronic mail using their smart card. The card contains the employee's digital certificate, along with his/her public and private key pair.

- Secure storage – Employees gain access to secure storage areas on servers and laptop computers via certificates stored on their smart cards.

- Authentication for accessing web sites – Employees can be authenticated via smart cards to access secure applications and content on an organization's web sites – especially intranet and extranet web sites. In some cases, it may also be worth considering the issuance of smart cards to business partners and certain customers for accessing secure areas on the company web sites.

- Storage of sensitive data – Sensitive data can be stored securely on smart cards. For example, personal medical data can be stored on each employee's smart badge, which could then be read in the event of a medical emergency.

- Debit transactions – Smart cards can be used for cash payments at cafeterias and vending machines. Users would occasionally 'recharge' their card in exchange for cash; the card would then be used as if it were the equivalent of that cash. This can be more convenient for both consumers and vendors.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

To further consider the possibilities for applications, below are some ideas for how to integrate complimentary technologies into smart card-enabled systems.

- Biometrics – Biometric devices such as fingerprint readers can either replace or be combined with the use of PINs to access private data on smart cards, thus increasing security by introducing another factor of authentication. The factor of security introduced with biometrics is referred to as "something you are", or "something about you", which is some unique biological characteristic, such as a thumbprint. This measure will increase security by helping to ensure that a person in possession of a smart card is authorized to use the services of that card. The use of biometrics also makes it significantly more difficult to repudiate transactions (more on this topic herein).

- Electronic turnstiles – Facility access systems can be integrated with electronic turnstiles that are outfitted with either contact or contactless smart card readers. The turnstiles, which might be placed at office building entrances, allow the authorized smart badge holder to pass through a gate. These devices are often designed to prevent 'piggybacking', in which a person (who may or may not be authorized) attempts to pass through the turnstile on the heels of an authorized person who has just presented his or her card.

- Surveillance cameras – Cameras could be integrated with facility access systems to increase the level of security. For example, a surveillance system could be triggered to record the video of any person entering particular areas off-hours. Another example is that the surveillance system could record the video of any person attempting to enter a facility using a badge that was reported as lost or stolen. In some situations, it may be desirable to have security personnel monitor the video for certain areas. Regardless of whether any live video is monitored or not, it probably always makes sense to record that video, so that evidence of security breaches, when they occur, can be maintained.

- Alarm systems – Alarm systems could also be integrated with facility access systems similarly to surveillance systems. In this scenario, certain events – such as off-hours access or attempts to use a stolen card – would trigger an alarm, which would in turn alert security personnel to respond.

- DSRC (Dedicated Short Range Communication) – Where greater operating distances are needed for convenience and/or speed of ingress/egress – for example, in parking facilities – complimentary technologies can achieve that distance. For example, infrared DSRC (Dedicated Short Range Communication) technology can be used to communicate between a device and the reader at distances of more than several meters. One way that DSRC is employed is for a contactless card (i.e. an employee's smart badge) to be inserted into a small device in a vehicle; the device reads the employee's card and acts as a proxy in sending the credentials to the reader. [vi]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Benefits

As with anything else, the benefits realized from smart cards depends on how they are used. For the sake of discussion, let's assume that an organization is planning to employ smart cards for the four primary applications suggested above – employee ID badge, building access, certificate-based PC / network logon, and certificate-based remote access authentication – all through a single-card solution. Under this scenario, benefits should be realized in the forms of improved security via strong authentication, accountability (non-repudiation), facilitation of PKI (Public Key Infrastructure), positive return on investment, and convenience.

Multi-factor authentication

It is commonly accepted by information security people that there are three factors of authentication: 1) something you have, for example a token; 2) something you know, for example a password; and 3) something about you, for example a fingerprint. It is probably safe to say that most organizations still use single factor authentication, in the form of a password system, to authenticate users for access to most computer and network resources. However, requiring two factors significantly enhances security because either one factor by itself is not sufficient to perform the authentication.

Smart cards introduce a multiple factor security scheme, which enhances overall security. Typically, the way smart cards are used for accessing computer and network resources is that a user inserts the smart card into a reader and then enters the PIN (personal identification number) associated with that card in order to unlock the services of the card. In such a scenario, the first factor of security is providing something you have – a smart card. The second factor of security in this case is providing something you know – the PIN. If there is a need, a third factor of authentication could be integrated as well; for example, part of the authentication could include the user's fingerprint being verified by the system.

Multi-factor authentication can also be used for physical access. For example, to access a secure room such as a server farm or a research lab, users could be required to present their smart badge and then enter their PIN into a keypad mounted at the entrance of the secure area.

Facilitation of PKI

Enabling computer applications with smart cards also provides greater security by enhancing an organization's public key infrastructure to a level where it becomes easy to use, thus eliminating the need for passwords. Passwords are seen as a weakness in security systems because they are often easy for potential intruders to steal or guess. Public key infrastructures solve this problem by providing a method of authentication that helps ensure a user's private key remains a secret. When smart cards are made an integral part of an organization's public key infrastructure, they enhance PKI by providing a secure and convenient form factor to carry and use digital certificates for multiple applications.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In an environment without smart cards, private keys are typically stored on a user's PC and accessed by the computer when needed. Though usually stored in a secure area on the PC, these private keys are still vulnerable to potential intruders; crackers could potentially extract or intercept them. Smart cards greatly reduce this vulnerability by storing private keys in a secure, tamper-resistant storage area on the card. Additionally, smart cards are capable of performing cryptographic functions on board the card, thereby isolating critical security-related computations and eliminating the need for the private key to ever leave the card at all.

Because certificates are stored on the card instead of on the PC, this makes digital certificates portable as well. Provided they have the proper permissions, employees can potentially use their smart cards from any computer in the organization. This portability also plays a significant role in providing a strong authentication mechanism for remote users. Telecommuters and users who travel with laptop computers can use their smart badge to authenticate themselves for access to the enterprise computer and network resources in much the same way they would from the office. The issues involved with remote access authentication are important ones with many organizations, and smart cards address these issues very nicely, particularly when used for certificate-base authentication.

Non-repudiation

Accountability (non-repudiation) is a key concern for enterprises. It is important – in and many cases critical – to ensure that employees are accountable for the electronic transactions they perform. Smart cards help ensure this accountability because each employee is expected to be in physical possession of his own smart card, and each should be the only person to know the PIN for accessing the services on that card. This is to a great extent a policy issue, but smart cards help enforce that policy. Because the employee's digital certificate and private key exists only on the smart card and not on any computer (where it could potentially be intercepted), any transactions – such as system logon and digital signatures – performed with that certificate are reasonably certain to have been performed by the person to whom the card was issued. Smart cards may not make it impossible for employees to repudiate, but they certainly make it more difficult.

Positive ROI

Conventional wisdom would indicate that the more applications a smart card is used for, the greater the ROI (return on investment). Nevertheless, every implementation is different, and organizations should perform a thorough cost benefit analysis before proceeding with the deployment of smart cards. Again, organizations migrating from a multiple-card to a single-card solution may realize a cost savings. Use of the smart badge for building access – particularly if other complimentary security technologies are integrated with the solution – could potentially result in the need for fewer security guards, and thus, significant cost savings. On the IT front, certificate-based logon will, for the most part, replace passwords; therefore, help desk calls for password-related problems would become virtually nonexistent.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

On the other hand, there are many trade-offs involved, and there would be many new costs associated with the deployment and management of smart cards. For an outline of what should be included in a cost benefit analysis, refer to John Abbott's paper, "Smart Cards: How Secure Are They?". [vii]

Convenience

Although there may be certain aspects of the solution that are not convenient (see the section on Challenges herein), a single-card solution offers some attractive benefits. First, carrying and using a single card is easier than multiple cards. Many organizations already issue employee ID badges; therefore employees of those organizations are already accustomed to carrying a badge. For organizations that currently issue more than one card – for example an employee badge, and a separate card for building access – migrating to a single-card solution certainly provides a level of convenience for card carriers. This solution is also convenient for employees, because they are no longer required to remember passwords. And it provides a greater convenience for building access over other types of cards, such as bar code or magnetic stripe cards, which must be swiped or inserted into a reader in a certain way.

Challenges

Although some of the benefits of smart cards are indeed attractive, there are also challenges and obstacles. In his March 2002 Information Security Magazine article, "A Smart Card for Everyone?", Andy Briney outlines some of these key obstacles. [viii] The article refers to getting smart cards in the hands of the masses, but many of the obstacles still apply to business environments. Some of those challenges enterprises will face include technical, security, cultural, and cost issues.

Technical

Among the technical challenges enterprises will face in deploying a smart card program are interoperability issues and, if the company doesn't already have one, the design and implementation of a public key infrastructure. There may also be some challenges with integrating different systems. Migrating from different card systems might be a challenge, but there are actually some simple solutions that can be explored to ease the pain of migrating.

Interoperability has been addressed by various standards, but not all have gone far enough to completely address all the issues. For contact cards, ISO 7816 addresses the physical and electrical characteristics of the card, how the card interfaces with external systems, and the command set of the chip operating system. The PC/SC Specifications builds on the ISO 7816 standard to provide a platform independent architecture that addresses interoperability of smart cards and smart card devices for computing environments. [ix] Although a standard for the chip operating system is still not available, help is on the way.

ISO 7816 part 4 addresses commands for chip operating systems, but it leaves room for interpretation; therefore, products from different vendors are not necessarily

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

interoperable. To address this shortcoming, a consortium comprised of the US General Services Administration (GSA), NIST, and other federal agencies, as well as organizations from the private sector, has developed the Government Smart Card Interoperability Specification (GSC-IS), which is expected to be released in a document by NIST in April 2002. [x] Essentially, the specification addresses various operational issues in regard to interoperability, including a way to map different vendors' products to a common set of chip operating system (COS) commands. This specification should prove invaluable for enterprises to ensure the smart cards and smart card readers they procure – potentially from different vendors – are interoperable.

The design and integration of a PKI, if the organization doesn't already have one in place, is sure to be another challenge. Designing a PKI requires a great deal of planning to do it right. Some organizations may wish to choose from several vendors who sell PKI solutions; others may wish to design and implement their own PKI. Windows 2000 comes out of the box with PKI elements, including directory services (Active Directory) and certificate services. This makes the home-grown solution attractive to some of the many Windows shops. Whether home-grown or not, though, PKI will require a significant effort to plan and to develop the policies.

In regard to facilitating the migration of older card technologies to smart card technologies, it is recommended that the old card features be integrated into the smart badge – at least until all of the older technology components have been replaced with new ones. For example, an organization replacing a large number of magnetic stripe readers with Mifare readers may decide to include a magnetic stripe on its new Mifare cards, thus ensuring its employees can continue to gain access to all authorized areas. Once all the readers have been replaced, any new and replacement cards issued will no longer need the magnetic stripe feature, and it can be eliminated from the design.

Security

One of the primary security risks pertaining to an enterprise smart card program stems from lost cards. If a card is lost and not reported as such immediately, there is potential for an unscrupulous person to find that card and use it to gain unauthorized access to enterprise physical or digital resources. There are measures that can be taken to mitigate this risk, though. First, cards that have a PIN require that the cardholder enter the correct PIN to gain access to the services on that card. Additionally, some cards can be set to self-destruct if the user makes a certain number of failed attempts to enter the correct PIN. There must also be policies and procedures in place that address how to handle the situation when a card is lost. For example, administrators should modify accounts to block access from cards that have been reported as missing or stolen.

Cultural

The use of a smart badge in the enterprise will cause some major changes, and many of these won't come easy. Employees will need to get accustomed to having their cards in their possession at all times, because the cards will be the employees' keys for both physical access and access to digital resources. For organizations that already utilize employee IDs, this aspect may be insignificant, but for other companies, there will likely

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

be growing pains as employees forget their badge at home and temporary badges need to be issued.

A major cultural challenge will occur because employees will need to insert their card into a PC smart card reader to logon, and then remove the card whenever they walk away from their workstations for any length of time. Additionally, based on the author's personal experience in testing certificate-based smart card logon, the logon process may take somewhat longer than with passwords. While these tradeoffs can be easily justified for the purpose of improving overall enterprise security, they will take some getting used to.

Cost

Smart cards and related infrastructure components are expensive in comparison with some other authentication systems. The cost of the cards can vary greatly, depending on what features are integrated into them (i.e. contact chip, contactless chip, magnetic stripe, etc.), and what sort of customization (i.e. graphics) must be done. Besides the cost of the cards themselves, smart card readers will be needed for each PC and for entrances and exits connected to the building access system. Other components of the card management system also increase the overall cost. And there will be a significant cost to implement a PKI, if one doesn't already exist.

To help keep costs down, it is important to ensure that the products selected are interoperable with other manufacturers' products. There should be the freedom to select products from different manufacturers – if only as a backup plan. If, for whatever reason, it becomes necessary to switch to a different product, the change will likely be very costly if the products aren't compatible. The establishment of contracts with one or more vendors to supply smart card products and services is also essential for any significant deployment effort. And as with most products, costs can be reduced when buying in bulk.

Costs also will come down as more organizations begin to deploy smart cards. With the US government planning to purchase millions of cards over the next few years, this should help drive costs down. And some experts believe that smart card readers will be standard equipment in all new PCs – perhaps built into keyboards – within the next couple of years.

Infrastructure

Once it has been decided to proceed with a smart card program, an organization must deploy the infrastructure to support the program. Essential components of that infrastructure include a contract or set of contracts for procuring the other infrastructure components, a card management system, a public key infrastructure, a facility access control system, and a comprehensive set of policies.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Procurement and inventory control

A contract or, more likely, a set of contracts should be established for the procurement of the components needed to implement smart cards. Components to consider including in the contract consist of smart cards, PC smart card readers, readers for facility access, digital cameras, smart card printers and other devices for card customization, certificate authority servers, card issuance workstations, and services to assist with the implementation. Care should be taken to ensure that the smart cards and smart card readers included in the contract are interoperable with each other, as well as with similar products from other manufacturers.

Once the cards have been procured and delivery is taken, they must be inventoried and tracked in accordance with stringent policies and practices.

Card Management System

A card management system is comprised of various components that deal with managing the life cycle of employee smart badges, from customization to replacement, as well as with the provisioning of temporary cards. Below are some of the essential components of the card management system.

- Customization – Customization is the process of printing the enterprise name and logo on the card, as well as personalizing the card for the person to whom it will be issued. This personalization typically includes the person's photograph and hand-written signature. It also includes encoding the contactless chip with information needed for building access, and requesting and downloading a digital certificate on behalf of the user to whom the card will be issued. It might also include printing a bar code or encoding a magnetic stripe with information that is unique for the person.

  Part of this process will include taking official photographs and capturing employee's handwritten signatures for printing on the card. Many organizations have special stations set up with digital cameras, etc. to handle this. Also, there are products available – from simple to elaborate – to enable in-house customization of smart cards. Alternatively, this process can be contracted out to a trusted third party.

- Issuance – Issuance is the process of distributing cards to the employees, contractors, temp workers, and possibly visitors. It is imperative that the person to whom the card is issued proves his or her identity to the issuer. Additionally, all cards issued must be tracked.

- Revocation – There must be a process to revoke smart badges from people as dictated by the organization's policy. The most common scenario will probably be for employees leaving the organization. Additionally, there must be mechanisms and procedures in place for blocking access to physical and digital systems when a card is reported lost or stolen.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Replacement – There must be a mechanism in place to systematically replace cards. Reasons for replacing cards might include preventative maintenance (providing a new card before the old one fails), as well as ensuring that the employees photograph is current. All cards should have an expiration date clearly indicated.

PKI (Public Key Infrastructure)

A public key infrastructure is a collection of technologies, policies and practices that facilitate the use of applications that rely on public key cryptography. Such applications include file and e-mail encryption, digital signatures, and certificate-based logons to computer and network resources. Essentially, a PKI enables users of such applications to create digital certificates and public/private key pairs, exchange digital certificates and public keys, verify the authenticity and validity of certificates, and establish or reject trust relationships between certificate issuers. Much of what a PKI does can be done manually – for example, users can e-mail their certificates and public keys to each other, and they can manually check with certificate issuers to make sure another person's certificate is valid. However, for anything other than very small scale operations or performing such functions with extremely limited frequency, manual operations of this nature are impractical.

The technology components of a PKI include certificate authorities, which are special servers used to issue digital certificates; an enterprise directory service, which provides a mechanism for publishing certificates and for applications to find certificates in a fashion that is transparent to the user; and applications that are enabled for public key cryptography. In a Microsoft shop, examples of these components include Windows 2000 Servers configured as certificate authorities, Active Directory for the enterprise directory services, and MS Outlook for one of the applications.

Although PKI is being portrayed in this section as a component of an enterprise smart card program, smart cards can also be considered a component of PKI. The reasons for this are described in the section on, "Benefits", herein.

PKI is an essential part of a smart card infrastructure because it significantly enhances the security of computer and network resources by providing the means to eliminate user passwords and allow for stronger certificate-based access authentication.

Further details of public key infrastructure are beyond the scope of this paper, but information is plentiful on the web.

Facility access control system

Many organizations already have systems to control physical access to their buildings and other facilities. Essentially, these systems are comprised of a central database, controllers, card readers, management terminals, and a mechanism to push database changes out to the controllers and readers.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The central database contains a list of employees (and possibly trusted consultants and other third parties), the locations that those people are authorized to access, and the hours that access is permitted. The management terminals facilitate maintenance of the database – adding, changing, and deleting employees, and modifying the areas and hours of authorized access. In some systems, there is a mechanism that copies portions of the central database to the appropriate controllers. Controllers are devices that provide instructions to the card readers for a local geographic area. And card readers are connected directly to the controller.

Having local copies of the appropriate portions of the central database helps increase security and performance. For example, one controller might be dedicated to a small, remote building with a dozen card readers. Instead of the user's credentials, which are read from the smart badge, being sent all the way back to the central system for validation, the controller, or in some cases the card reader, can perform that validation locally. For security as well as performance reasons, only the appropriate portions of the central database should be copied to the local controller; for example, only the list of persons authorized to access the particular geographic areas served by that controller.

Policies

Several policies will be essential to the success of an enterprise smart card program. Below are some of the ones that stand out.

- Card usage – Once smart cards are fully deployed in an enterprise, a policy should be immediately implemented that all employees will be issued a single smart badge that functions as a photo ID and a smart card. The policy should indicate the applications for which employees must utilize their smart badge. The policy should also state what exceptions may be necessary; for example, whether system administrators still need to use passwords to perform certain administrative functions.

- Card issuing and revocation – Enterprises must decide which department is responsible for managing the card issuance process and performing the role of certificate registration authority. Once the card is customized with the employee's photograph and other features, that department would request a certificate on behalf of the employee and install that certificate on the employee's smart card. Likewise, that department would manage card changes and revocation when employees change positions or leave the enterprise. The policy should also convey that employees must prove their identity before their cards will be issued.

- Temporary cards – Another necessary policy is one that describes how to handle situations where employees forget their smart badge on any particular day. If employees are required to use their smart badge for computer / network logon, the organization will most likely need to issue a temporary badge to the user. Temporary cards will need to be tracked; therefore, they should be signed out and then signed back in the same day. As with the normal issuance of smart

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

badges, employees should be required to prove their identity before a temporary badge is issued.

- Lost cards – The organization also needs to set a policy requiring employees to immediately report lost cards, and requiring smart card program administrators to immediately revoke the privileges associated with lost cards.

- Replacement cards – Additionally, the policy should indicate how replacement cards will be handled. For example, an organization may decide that employees who lose their smart badge will be issued one replacement free of charge in a two-year period, and that for subsequent losses the employee will be held personally responsible for the cost of replacing the card. Also, the policy should separately indicate how the replacement of temporary cards will be handled. For example, it may be decided that employees who lose temporary smart badges will be held personally responsible for the cost of replacing the card (even the first time).

- Visitor badges – It needs to be decided whether badges will be issued to visitors. Issuing smart badges to visitors may help keep better track of those visitors, assuming other controls are put in place.

- PKI-related policies – A public key infrastructure must not be put in place without a comprehensive set of policies. These policies must address the operation of certificate authorities (CA's), the trust relationships between CA's operated by the enterprise and those operated by other entities, and issues particular to certificates issued by the CAs.

Conclusions

Although there are obstacles in the way of many organizations implementing smart cards today, these obstacles are becoming easier to overcome. There are some technical hurdles to overcome, but the more difficult hurdles are in the areas of procurement, as well as policies and procedures. Enterprises contemplating the implementation of smart cards should carefully consider their needs, and then the detailed requirements for fulfilling those needs. Also, those enterprises should perform a thorough cost benefit analysis to determine whether smart cards truly make sense for their environment. If it makes sense to proceed, some good first steps are to implement a small pilot program, and to implement one application – for example, just building access, or just computer / network logon – at a time. Once the project gains momentum, additional applications could be added, and the pilot program can be expanded. For most organizations, the success of each small step will help move the project forward, whereas if too much is taken on up front, a failure could be catastrophic to the entire project.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Suggestions for Further Research

Although there are certainly many opportunities for further research in regard to smart cards, two topics come to mind in regard to assisting enterprises utilize these technologies. They are: 1) a framework for enterprise smart card programs, and 2) an open method for contactless smart card logon to computer and network resources.

Framework for enterprise smart card programs

If a usable, well-documented framework were to be developed, perhaps it would spur the deployment of smart cards in enterprises. Ultimately, it would be most beneficial if the framework consisted of a package of instructions, surveys, policy templates, schematics, and lists of cards and equipment that are interoperable.

Open method of contactless smart card logon

Ultimately, many companies would probably find it desirable to implement contactless logon to computer and network resources. The functionality might work something like this: Computers would recognize when users are in the vicinity – say, within two meters – by sensing their smart badges, and then challenging the user by requesting their PIN and/or some biometric input. If multiple users with smart badges are in the vicinity, the computer would display a list of those users, and allow for one to be selected. Once authenticated, the user would be logged on, and the session would remain active for as long as the user stays within the operating distance. When the user moves outside the bounds of that operating distance, either the computer is locked, or the session is terminated. This functionality would help enforce security policies that require users to lock their workstations or logoff when they step away. It might also reduce the amount of wear and tear on the smart card, increasing the life span and the return on investment of cards and readers. The functionality would also make the use of smart cards more convenient for computer users, because it would eliminate the need for users to insert and remove their cards from readers multiple times per day.

There are existing solutions for contactless logon; some even work as described above. The problem is that there are currently no open standards that make this functionality possible via certificate-based authentication. It would seem that organizations could benefit from understanding where the smart card industry is in regard to making contactless computer logon a reality, as well as what the hurdles are.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

1. Philips Semiconductors. Information about Mifare® contactless smart card chips. URL: http://www.semiconductors.philips.com/markets/identification/products/mifare (01-Apr-2002).

2. US General Services Administration (GSA). "Smart Card Tutorial". URL: http://egov.gov/smartgov/tutorial/smartcard_foyer.htm (31-Mar-2002). Note: Requires Macromedia Flash 4.

3. Everett, Dr. David B. "Smart Card Technology: Introduction to Smart Cards". URL: http://www.smartcard.co.uk/resources/articles/intro2sc.html (31-Mar-2002)

4. U.S. General Services Administration (GSA). "Smart Card Policy and Administrative Guidelines". URL: http://egov.gov/smartgov/101800_policy_handbook.pdf (29-Mar-2002).

5. RSA Security web seminar presented by Roland Fournier. "IT and Facilities – Leveraging Smart Badges for PC, Network, VPN and Building Access". 27-Mar-2002. URL: http://www.placewareforum.com/rsasecurity/page.cfm?p=event&eventid=12957&subcatid=11728 (01-Apr-2002).

6. EFKON Parking and Access Control Brochure. URL: http://www.efkon.com/efkon/dlds/parking.pdf (02-Apr-2002).

7. Abbott, John. "Smart Cards: How Secure Are They?". 01-Mar-2002. URL: http://rr.sans.org/authentic/smartcards.php (29-Mar-2002).

8. Briney, Andy. "A Smart Card for Everyone?". Information Security Magazine. Mar 2002. URL: http://www.infosecuritymag.com/2002/mar/cover.shtml (29-Mar-2002).

9. PC/SC Workgroup. "PC/SC Workgroup Specifications Overview". URL: http://www.pcscworkgroup.com/Specifications/SpecificationsOverview.html (28-Mar-2002).

10. Digital Security Initiative Workgroup. "Executive Summary of Government Smart Card Interoperability Specification (GSC-IS)". URL: http://egov.gov/smartgov/information/exec_summary.pdf (03-Apr-2002).

Cagliostro, Charles. "Smart Cards Primer". URL: http://www.smartcardalliance.org/industry_info/smart_cards_primer.htm (28-Mar-2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Fancher, Carol H. “Smart Cards”. Scientific American. August 1996. URL: http://www.sciam.com/0896issue/0896fancher.html (28-Mar-2002)

Gilhooly, Kym. “Smart Cards: Smart Move?“. Computerworld. 21-May-2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO60688,00.html (03-Apr-2002).

Microsoft Corporation. “Smart Card Logon”. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/security/sclogonwp.asp (04-Apr-2002).

Microsoft Corporation. “The Smart Card Deployment Cookbook”. URL: http://www.microsoft.com/technet/security/prodtech/smrtcard/smrtcdcb/smartc00.asp?frame=true (03-Apr-2002).

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**