Smart Card-Based Identity and Access Management

Contributors:
Shahin Shadfar, Schlumberger Information Solutions

Introduction

Since the tragedy of September 11, 2001, security has gained a new connotation and evokes previously unthinkable images. Most of the hijackers used either false or stolen identification documents, a few used their real identities, and all of them managed to breach our borders. This massive security breach underscores the importance of Authentication as well as Authorization.

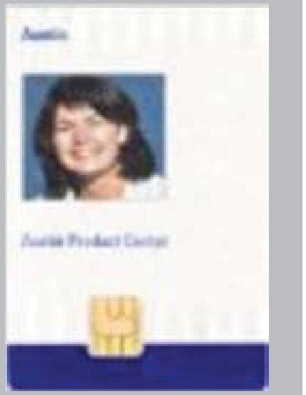
On a smaller scale, within an enterprise, securing physical premises, protecting information, and restricting access to critical applications has become a priority. The multiple network entries through Virtual Private Networks (VPNs), dial-ups, web portals for employees, partners and customers, wireless connections and more, make strong Authentication and Authorization all the more critical, since traditional password-based identification is no longer doing the job adequately. At the same time, managing employees' credentials for physical access to facilities, such as garages and office buildings, their logical access to PCs, corporate networks, critical applications and online accounts, and even resetting their passwords, can all be burdensome and expensive.

A new form of identification is necessary to secure both physical and logical access while combining other business benefits.

Smart card technology, although over twenty years old, has made some significant progress in recent years and, combined with the right software systems and appropriate policies, offers appealing solutions. These solutions allow organizations to deploy secure, portable and multi-purpose employee badges leading to an efficient and cost effective Identity Management system. A sound understanding of the business processes and goals within an enterprise is key to the most successful implementations. Securing a power utility company (generation plants, electricity grids, mobile employees) poses significantly different challenges from implementing security at a large hospital, for example, because each company's IT processes and business drivers are as vastly and distinctly different as their two industries.

This paper discusses the benefits of smart card-based identity and access management solutions and the different technical components of an enterprise-wide corporate badge deployment. This paper is geared toward people dealing with real business problems within organizations, as well as to technologists chartered to find viable technical solutions. Since all projects require financial justification, the Return On Investment (ROI) is also germane to the discussion. The scope of this paper is limited to the deployment of smart card-based identity and access management systems inside a public or private organization.

Java Card Specifications



- CPU: 8, 16 bit ‹Micro-controller
- Memory: EEPROM 32k, 64k and (soon) 128k
- External Clock Frequency: 1 to 7.5 MHz
- Operating Temperature: –25 to +75 C
- Data retention: 10 years
- Standards: ISO 7816, Java Card 2.1.1, Open Platform 2.0.1
- Security: DES, Triple DES, RSA 1024, SHA-1, X.509 certificates, On-Card key generation

How ‘smart’ is a Smart card?

Smart cards were invented in France in the late seventies and millions have been used over the past few years as pay phone cards, banking debit and credit cards and GSM mobile phone identifiers. The smart cards that are highlighted in this paper are, however, much more advanced than their predecessors from the seventies and eighties. Nevertheless, the concept remains simple: A credit card-sized piece of plastic with a fitted microchip or integrated circuit, with an input and an output channel, which can be used to store and/or manage the identity of its carrier. The chip includes memory, an operating system and a processor. Through a smart card reader, an information query is sent to the chip (for example, ‘who are you?’), and the chip processes your data and returns a response (such as ‘Adam Smith’). A smart card is, in many ways, a small computer you have in your wallet.

What changed over the years? The answer lies in the increased power, speed and capacity of the chip. In the late nineties, a team led by Bertrand Du Castel at Schlumberger marketed the first Java™ programmable smart card with a later addition of a crypto-processor. The current smart cards used for security applications derive from these early Java Cards. The advantage of this new edition is that you could add, update or remove ‘card applications’ called ‘cardlets’ or ‘card applets,’ similar to applications on your PC. The crypto-processor allows complex cryptographic functions to operate on the card, which becomes relevant to security.

In addition to offering cryptographic functions for security, the chip itself must be resilient to hacker attacks. If you have a powerful machine that can execute complex encryption functions, the security can still be greatly compromised if it was easy to steal the encryption key. Over the years, smart card chips have become more bullet proof and have earned FIPS Level 2 and Common Criteria certifications, and are commonly regarded as the most secure hardware tokens. For the technicians, a smart card is a sort of small ‘HSM’ (Hardware Security Module). In short, smart cards are portable, secure and multi-purpose tokens.

Smart card Usage

There are already examples of large deployments of smart cards as employee badges in the United States. The United States Department of Defense (DoD) has, at this time, the largest number of smart card users through its Common Access Card (CAC) program, with over two million cards currently deployed for physical and logical security of its worldwide employees. A non-negligible number of Fortune 100 companies have also embarked on large-scale smart card deployment projects. Based on these implementations and the latest developments in the technology, what are the applications that make the most business sense?

The smart card ‘vision’ is to provide a platform where all credentials of an employee are centralized. One common ID card becomes the employee badge that gives access to different ‘systems.’ Following is a list of its most common applications, which are typically the objectives of Phase One of a deployment project.

- Picture ID
  The smart card is used as the employee badge with company logo, name and picture of the card bearer.
- Physical Access
  The employee uses the smart card to gain access to parking lots, garages, buildings and rooms. The system would need to identify the employee and based on his or her profile grant access to authorized areas. The usage of biometric technology in addition to the card can reinforce security at more restricted premises. For instance, Joe is given access to the parking lot, the main entrance, building 1 and 3 but not to building 2. Also, once in building 3, he would need to further authenticate himself with his fingerprint to enter the server room.

  Since many employees have become more mobile and their office locations number more than one, and are located on different continents, it would be ideal if the same card could work in multiple locations without wasting any time at the front desk. However, convenience is not always the best friend of security. Therefore, the systems and, more importantly, the processes implemented, should increase convenience (and thus productivity) without compromising security.

  By standardizing physical access at different sites across the world, and reducing the number of required cards to only one, you are already simplifying user management, which leads to cost savings. Meanwhile, you are also increasing the security level since it is easier to keep track of one card instead of four separate badges per employee. Has your company disabled those cards every time an employee was terminated or relocated to another office location?
- Computer Logon and Network Access.
  Joe has entered building 3 with his badge and now sits at his desk. He inserts his smart card into his PC and is prompted for a card PIN (Personal Identification Number), which can and should be a ‘strong’ alphanumeric password. Once he ‘authenticates’ himself to the card, he is granted access to the PC as well as to the enterprise network for which he has permission. So why is a PIN more secure than the good old password?

  First of all, using a hard token such as a card, in addition to a PIN, elevates your authentication level to what is commonly called ‘Two-factor authentication.’ It is not only ‘something you know’ but also ‘something you have’ that identifies you - thus, two factors. Secondly, a card PIN has 3 major advantages over a simple password:

  - While your password travels through the network, your PIN is sent locally only to the card itself. If the PIN is correct, the card then uses a digital certificate to allow your PC to handshake with the server and hence authenticate you to the network.

- If you enter a wrong PIN more than, say, four times (or ‘n’ times based on your security policies), your card gets ‘blocked.’ Consequently, you do not have to impose c@mP1#x passwords usually resulting in sticky notes on screens of employees who have trouble remembering such complex passwords, and exposing the password to the entire office. Nor will you have to process such a high number of helpdesk calls for password resets due to employees forgetting or losing their complex passwords.
- All passwords are kept in a centralized file that, though encrypted, could still be hacked. PINs are not kept anywhere other than individually on each Smart card. Each employee carries his or her own PIN on his or her smart card badge.

Many industry studies demonstrate that network attacks mostly originate from internal sources, such as recently terminated employees who haven’t been deleted from the company directory or systems in place, rather than from external hackers.

Joe is working on some confidential document but needs a break for lunch. As he removes the card from his PC it automatically locks the screen. Why would Joe remove the card? The answer is because he needs the badge to access the cafeteria and to pay for his lunch. In a single action, Joe has secured his PC and can use his Smart card for other applications, such as debit for his lunch. Now we are starting to see the advantages of tying everything together.

Below are some secondary applications we often see in projects. Based on your business drivers, you might consider these functions with differing priorities.

- Health Record storage

  The Smart card being also a storage device (with up to 64k of memory), it can contain some personal information such as healthcare data. Beyond simple storage the card can be programmed to grant access to, say, physicians to view and update some data while the insurance company would have permission to view a subset only. Healthcare organizations in the U.S are seriously considering following their European counterparts in using Smart cards to comply with HIPAA (Health Insurance Portability and Accountability Act) regulations and attain other business benefits.

  Why not leave all the information on a server instead? This is the eternal question about the usage of Smart cards. The business driver for those who select the Smart card storage path lies in the fact that connections sometimes go down and that not all clinics, hospitals or offices have access to the same databases. Using Smart cards allows you to access the healthcare data off-line, which guarantees access at all times and reduces the cost.

  What if the employee loses his or her Smart card? This is another great question about Smart cards. The system should be able to backup the information once in a while to a centralized database. The point is you do not need a connection to that database every time you need the employee’s information. Think about emergencies!

- Electronic Payment

  An entire book could be dedicated to payment with smart cards. Since the introduction of Smart cards in the French banking industry in the late eighties (leading to fraud reduction by a factor of 10) many standards or proprietary systems have been created mostly by the large financial institutions such as Visa. Applying this concept in organizations is simple however. The employee uses the Smart card to buy soda at vending machines and pays his or her lunch at the cafeteria. There are different ways of achieving this from a technical standpoint. You could have an electronic purse programmed on the chip on which you deposit a certain amount of money using ATM-type kiosks. Alternatively you can read an employee’s identifier off the card and a back-end system bills you at the end of the month. More advanced solutions integrate with the enterprise payroll systems and do automated deductions.

  Studies show tangible productivity increase mostly from the time saved at the register. Also employees do not have to go find an ATM every once in a while

- Remote Access

  VPNs (Virtual Private Networks) and other solutions used for remote access create secure channels between a remote user and a private network. Yet username and password based Identification does not provide a strong authentication mechanism and when a link remains weak in your security chain, your overall security suffers.

  Smart card solutions also bring a strong two-factor authentication mechanism for remote access users.

- Thin-Client Authentication

  Thin client devices provide remote access to applications that are installed and stored on centralized, secure servers with the obvious advantage of reducing the cost of applications maintenance across multiple PCs (fat clients), for example, and easing user access management.

  In a distributed computing environment such as the thin client model, critical data and applications reside on a centralized server, which lowers risk on the client machines on the one hand but meanwhile creates new security threats. A malicious employee, who manages to impersonate a manager with access to confidential information, can cause a great deal of damage if he or she can gain access to the server. Once again, dual-factor authentication with smart cards can address these issues and can prevent such intents from becoming realities.

In certain environments, such as hospitals, multiple users (for example, nurses) use the same thin client or terminal. Using a smart card ID badge, nurse A can close his or her session by removing the card and resume it by reinserting it after nurse B finishes his or her work on the same terminal using his or her smart card identity badge, and so on.

- Single Sign On (SSO)
  If all systems inside your organization based their user identification on digital certificates, you would not need usernames and passwords anymore. You would need to present your smart card and type the PIN only once.
  For the specialists, mechanisms such as Kerberos use this model. The reality is that we still are far from having all systems use digital certificates. Many legacy applications rely on username and password sets. Examples include your email application, your internal web portal, your CRM (Customer Relationship Management) system, your personal Internet email web site; even your stock broker web site.

Smart cards can help. Imagine a system that stores all these usernames and passwords on your employee badge and every time you are prompted for logon, it first recognizes the application or web site and then automatically furnishes the required credentials. The portability of smart cards makes this feature especially compelling since your card and your PIN makes life easier for you at the office, at the home PC or at any other company machine. Moreover, you could configure some of the current systems to set random passwords. Think about the security benefits of giving your contractors a badge, which lets them work with different applications without even knowing their account passwords. Once their time is up, all you need to do is disable their smart card.

Significant helpdesk cost reductions are associated with these solutions. One employee helpdesk call costs a company an average of $30 in the United States. Over 30% of helpdesk calls deal with password resets.

- Web Access
  As with remote access authentication, smart cards are used to authenticate your employees to confidential internal or external web sites such as payroll and benefits' site. If you employ a policy server you could also authorize employees to different sections of a site based on their privileges.

- Email, document signing and encryption
  Another useful application of smart cards is in document signing and encrypting. Although a do smart card is not absolutely de rigueur for these purposes, it renders the operations more secure and more practical in many ways. Digital encryption and signing are enabled by PKI (Public Key Infrastructure) discussed below. For the sake of simplicity, imagine you need a digital certificate to encrypt and sign a document such as a Purchase Order (PO). This certificate might typically be stored on your work PC's hard drive. However, by storing it on the smart card itself, you have two advantages:

  - The digital certificate (signature) is again more secure, thanks to the dual-factor authentication feature discussed earlier. An important benefit of digital signing is its 'non-repudiation' factor. When you sign a PO, no one should be able to deny it a month later.
  - It is portable. You could encrypt and sign emails at work as well as at home. Similarly you can decrypt and verify the signature of an email you receive from anywhere.

Document signing is a perfect example of security augmenting the realization of business goals. Many organizations are moving toward 'paperless' transactions with their suppliers and partners. For instance, a major pharmaceutical firm is now developing an industry standard mechanism to finalize contracts with their suppliers in a paperless fashion. Cost savings in the millions of dollars motivates their interest, if they can reduce the time it takes to close contracts by 25%. Securing all links of this chain then becomes a 'business enabler' with obvious Return On Investment.

- Wireless Authentication
  The future is wireless! This is a true statement especially for client machines employees will deal with. Although the technology is already there, many organizations such as U.S government agencies hesitate in deploying W-LAN (Wireless LAN) or simply PDAs (Personal Digital Assistants) mainly due to the lack of security. Although the technical problems go beyond authentication issues, Smart cards can play a key role in identifying the devices and their users. The employee would use the badge to authenticate to a wireless LAN (Local Area Network) gateway and also would insert the card to his or her PDA in order to read an email.

- Other Proprietary applications
  The beauty of smart cards resides in the fact that they are programmable and subsequently flexible and scalable to new applications. You could develop a specific card 'applet' for your needs and deploy it 'on the fly.' The capability to update cards with new data and applications after the initial deployment heavily depends on your Card Management System (CMS) capabilities, which we will discuss in the next section.

  As an example, a large automobile manufacturer has added a proprietary program to the card to track different parts as the vehicle is being assembled. This was developed for quality measurement purposes.

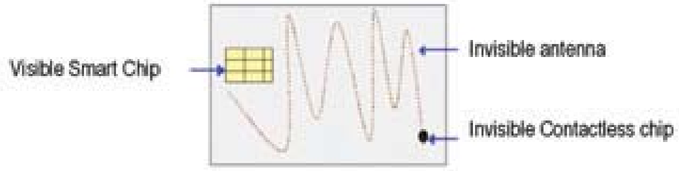
Components of the Corporate Badge

In the previous section, we described the main functions and benefits of a smart card-based ‘Identity Management’ solution from a user perspective. In this section, we will visit different front- and back-end components that constitute this solution. We have described the specifications of an ideal system. Now we must examine what’s under the hood. The intention is to provide a big picture rather than bury you under too many technical details.

- Smart Card – Badge

  Although not the only alternative, the Java Card (version 2.1) has become the de facto standard for security projects. When also used for physical access, usually the visible smart chip is embedded to a card that contains another chip as well as a small antenna. These two components are placed inside the plastic and remain invisible from the surface and are used for contactless access. When the antenna is placed in a magnetic field created by a proximity door reader, sufficient power is generated (for physicists, due to the Foucault current) for the contactless chip to function and send a signal to the door reader carrying the badge number. This accounts for the absence of battery inside the badge. A few different standards have been established in the industry. Note that currently these two chips do not communicate with each other and are only placed on the same token. There are however prototypes of Smart cards where the same chip works in contact and contactless fashion.

  Other than the area containing the electronic smart chip, the entire card is usually printable. You can print a color picture of the card bearer, name, title, as well as a company logo. Color codes could be used to distinguish full-time employees from part-timers or contractors. A magnetic stripe and/or a bar code could also be added to the card for compliance with other legacy systems.



- Smart Card Readers

  Physical access door readers propagate magnetic waves, as explained above, and read the card number from a distance of up to six inches. A few door readers are usually connected to a ‘panel’ that communicates with the Physical Access server. A biometric reader and/or a PIN pad could be added to the card reader for access to more restricted areas.

  Logical access card readers come in various formats and connect the machine to the Smart card. There are serial port, USB and PC Card readers that follow PC/SC standards. Note that these readers are also ‘writers’ and can update the information on the card if the program handing the card has the required privileges.

USB Token with Smart Chip

  An innovative USB connector that fits in your key chain is now available using a particular Smart card chip where the USB protocol has been programmed. This means that you do not need to have a Smart card reader installed on your machine as a USB port is sufficient leading to greater portability.

- Physical Access System

  There exist many different systems in the market that connect to doors and panels, cameras, alarm systems, and which manage users from a central database. Various systems are generally used within the same organization at different sites and countries. Selecting one vendor across the company often poses serious challenges. The good news is that you do not have to do so, although reducing the number of systems helps. As long as you employ the same standard for the Smart card and door readers, and your back-end system support that standard you could have a heterogeneous server farm. The addition of a common interface to the different physical access greatly simplifies user management across geographic areas. Please refer to the ‘Automated Provisioning’ sub-section later in this paper.

- Public Key Infrastructure (PKI)

  PKI is a fairly complex topic that goes beyond the scope of this paper. For the sake of simplicity, let us say that PKI is responsible for attributing digital certificates to entities (such as employees, servers), and that each entity holds private and public keys. While public keys are published in company directories (such as LDAP or Active Directory), private keys are ‘securely’ kept by the entities themselves. Using PKI functions, the entities can transact securely (authenticate, authorize, encrypt, decrypt, sign, verify signatures). A central Certification Authority (CA) manages certificates.

  You do not necessarily need smart cards for PKI and, symmetrically, you could have a smart card deployment within an organization without PKI. Yet the combination is powerful for some of the applications mentioned earlier.

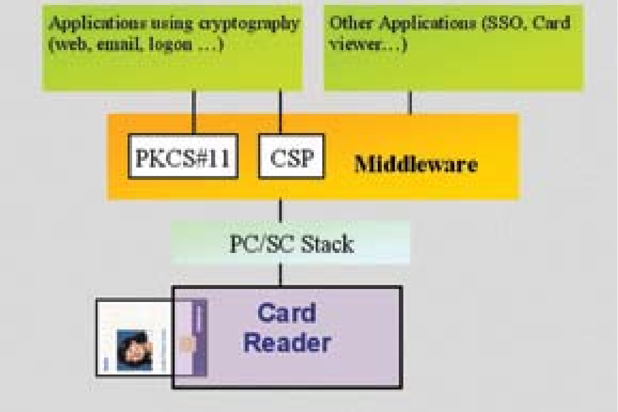
  The smart card used in today’s security projects can perform advanced cryptographic functions and even generate required keys. The users’ private keys can be created and securely stored on the card itself.

Scalability and efficient certificate management have been major challenges for PKI systems. Today, a few vendors offer solid solutions for corporate deployments. Although their solutions comply with X.509 certificates standards, interoperability still remains a challenge. If you intend to use the PKI for external communication, then you should develop a solid Certification Process (CP) and Certificate Policy Statement (CPS) that both deal with the critical legal aspects of your transactions with third parties.

For separate PKIs in different organizations to work efficiently together, they need to 'cross-certify' against one another, which can become quite cumbersome and difficult to manage. New mechanisms, such as Federated Identity Management, that offer a more holistic model for inter-organizational cross-identification are emerging.

- ## Smart Card Middleware

The middleware is a set of software modules that allow applications such as your web browser to see the smart card and to communicate with it. The comparison to device 'drivers' as used in some literature, is misleading since the middleware contains some sophisticated cryptographic functions that can work hand in hand with those on the card.


Applications using cryptography (web, email, logon …)
Other Applications (SSO, Card viewer…)
PKCS#11
CSP
Middleware
PC/SC Stack
Card Reader

Today the middleware comes part of a larger 'user kit' that installs, besides the middleware, card Readers drivers, tools to view the card content, a module to communicate with a Card Management System (CMS – discussed further), a Thin Client Authentication module, etc.

Although different vendors' middleware follow some industry standards, these widely vary in their quality. The problem is that Microsoft applications use a Cryptographic Service Provider (CSP) while other applications usually use another standard called Cryptoki or PKCS#11. A 'good' middleware is fast, interoperates seamlessly with Microsoft applications (Internet Explorer for instance) and others (such as Netscape Navigator) and efficiently handles digital key recoveries and rollovers (when there is no more room on the card).

The U.S Department Of Defense has played a significant role in defining some interoperability standards for smart cards in recent years. Following the initial Common Access Card (CAC) program, a new standard known as the Government Smart Card-Interoperability Specification (GSC-IS) has been developed around the card and the middleware.

- ## Card Issuance System (CIS)

The CIS is a centralized system that creates cards for employees, personalizes them to a certain extent and updates the physical access system with the employee's credentials. It should perform the following tasks:

  - Interface with a central directory to retrieve employee information
  - Interface with a digital camera and Smart card printer to prepare physical cards
  - Potentially read and update the Smart card chip with some initial personalization
  - Read the Contactless chip number
  - Communicate with the Physical Access system to create or update an employee entry with associated Contactless card number
  - Track card stock
  - Provide an interface for administrative purposes

A Card Issuance System must be able to support several 'Printer Stations' in different locations. Scalability and flexibility to adapt to various workflows are critical.

There have been many attempts to merge the CIS and the Card Management System (CMS - presented below). Many have failed since they overlooked the business processes complexity behind the administration of these tasks. The group in charge of the facilities, who have different priorities and a different mindset from the IT people running the logical access, typically manages the physical access. The physical access administrator or officer rightfully wants to have a say in granting access to employees and will not accept the IT Security guy setting the access rights. There are a few systems that have taken into account these considerations and have created a unified system.

For the sake of simplicity, we consider the CIS apart from the CMS. In any case, these systems need to communicate with each other. They are typically bridged by the Smart card itself and a central corporate directory (such as an LDAP or Active Directory) in which they share common information.

- ## Card Management System (CMS)

Managing the card life cycle is the greatest challenge in any deployment. Before you select any technological solution in the market, you should spend enough time to draft a workflow of the processes that would best fit your organization taking into account security and user-friendliness. It is recommended that you seek help from expert IT security consultants with experience in designing and implementing security policies and processes. All possible incidents and scenarios, including the most out-of-the-ordinary ones, should be considered.

Who requests a badge for a new employee? How and where does the card get printed? Who requests a digital certificate? How to securely personalize (write to) the chip? What happens when an employee forgets his or her badge? What about lost cards (say during a business trip)? How do you unblock a card (when a user enters a wrong PIN a certain number of times, the card gets deactivated or blocked)? How do you recover encrypted emails if you lose your card? The challenge is to reach the necessary level of security without disrupting the business.

Until a few years ago, Card Management Systems were designed with 'theoretical' requirements that a few engineers thought to be relevant. Needless to say, the implementation to the field led to disastrous smart card deployments, tarnishing the smart card's reputation for solid identity and access management as a whole. Yet feedback from the real world and the incorporation of real business processes into these systems has resulted in a new breed of CMS that is very strong and adaptable to many different situations.

Below are some of the characteristics a sound CMS should feature:

- Communicate with directories such as LDAP or Active Directory to retrieve employee information and update certain fields
- Support the major Certification Authorities on the market
- Support OP secure channel between the server all the way down to the Smart card
- Make use of an HSM (Hardware Security Module) to store critical keys
- Provide a user-friendly employee portal (preferably web based)
- Provide an efficient Administration console with log audits
- Support card Java Applet management: loading and updating
- Allow centralized and 'self-service' enrollment
- Provide an effective way of recovering the content of a lost card

In short, the CMS is the most important module in your solution and hence, special effort should be made to evaluate and select the right system.

- **Electronic Payment System**
  Many different types of Smart card-based solutions for campus payment exist in the marketplace. A few can even be part of a larger external payment system (where your employee badge is also your credit card). As previously mentioned you could deposit an amount on the card itself or it could be managed on the back-end system in which case the card is only an identifier. In any case, the Smart card needs to a have a special applet for e-payment talking to whatever system you have installed. The other components are electronic devices that integrate to registers and vending machines with Smart card readers and that also communicate to a central server.

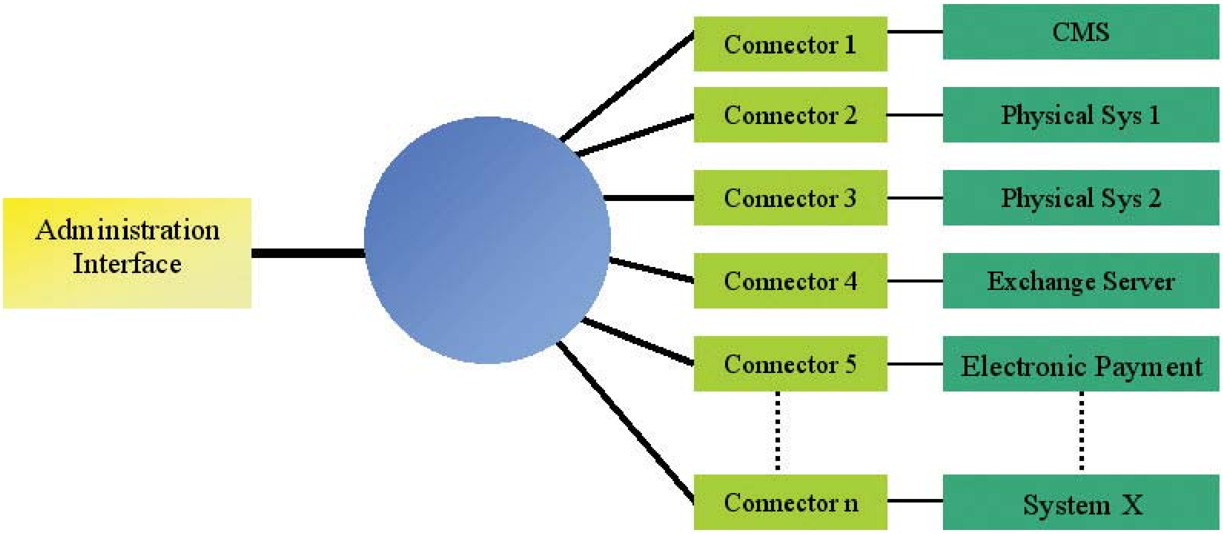
- **Password Wallet**
  Smart card based Single Sign On (SSO) software has matured in the last few years and now provide a reliable solution that stores username and passwords on the Smart card and automatically fills in the fields whenever the applications or web sites requiring those credentials pop up. Some of these solutions even recognize password fields on Java based windows, in Unix simulators and MS-DOS windows.

What happens if you lose your smart card? The usernames and passwords can be backed up in encrypted form in a database or enterprise directory and could be recovered through the CMS.

- **Automated Provisioning**
  Electronic Provisioning is on the rise these days. Let us assume you have a new employee (Joe) starting in your department. He will need a work space, a phone line, an email account, a Smart card badge, a certificate on his badge, an SAP account, a dial-up account and so forth and so on. An Electronic Provisioning engine will create a list of tasks and will automatically or semi-automatically request these services and will follow up until they are complete. For instance through an automated 'connector' to the Card Issuance System, it will request a new Badge for Joe. However, it will only send an email to the facilities department to request for an office space.

Similarly, when Joe moves to a new position or location, his accounts are deleted or updated and new ones, if needed are created. Perhaps more importantly from a security angle, all accounts are immediately disabled when Joe quits or is terminated. There are many 'nightmare' accounts of terminated employees seeking revenge on their ex-employer.

Using these systems, you could preserve distinct physical access systems in different locations and build connectors for them. This way you have one common interface, the Electronic Provisioning Administration console, talking to them and updating them. For instance, if Joe, based in Houston is going to London for a two-week mission, his manager could put a request for Joe's Badge to be enabled at the London office for that period of time although the two locations might have completely heterogeneous physical access systems.



These systems make your Smart card deployments more practical and help in the overall employee Identity Management leading to a better ROI.

- Biometrics

  As mentioned previously, biometric technologies add an additional (third) authentication factor (something I am). There are advantages in using biometrics in conjunction with Smart cards where the biometric information, for example the fingerprint, is stored on the card:

  - The authentication is local and could be performed off-line which has security benefits and cost implications
  - The matching is '1-to-1' instead of '1-to-n,' which reduces the 'false positives' and enhances security.

  The most advanced combination of Smart card technology and biometric authentication offer 'match on card' options. This means that the Smart card itself compares the fingerprint coming from the reader to the one it stores for its bearer, and returns a positive or negative response. This way, the stored fingerprint always remains on the card and cannot be stolen by a rogue application (and sent by email to the hacker!). Note that some Contactless chips have ample memory to store biometrics images and therefore allow biometric verification for physical access.

  Biometric applications have their own servers and administrative consoles allowing user enrollment for instance and the management of users. The integration of these systems with Card Management Systems are still evolving and have not reached, in my opinion, the level you would expect in a large deployment. In general, although the cost of biometric readers has decreased and the technology has gained an acceptable reliability level, enrolling and managing users still remain costly.

  There has also been an eternal philosophical discussion on the public acceptance of biometrics. Some also question the security of these devices, arguing that the credential used for authentication is 'public data.' We will leave these debates to the experts.

Implementation and Deployment

It is important to stress again that, at least as important as the technical components of the Smart card-based security solution, developing the right processes and policies and then enforcing them across your organization. Hardware and software pieces presented above are only tools helping you in your journey. Equally important is managing culture change and training your employees into a security-aware population. Indeed, the entire Smart card-based badge solution can be regarded as critical 'infrastructure,' much as electrical power into your organization. Many different groups and various categories of employees will have to deal with this solution on a daily basis. The overall system (in this case meaning the combination of technology and the processes) must work 99.99% of the time in all possible situations. At 97% success rate, you are making your employees angry and losing business. A solution dealing with security also needs to be as seamless as possible since in a large deployment of say, 20,000 users, you cannot expect everyone to make unreasonable efforts.

Below are some of the stages in a successful Smart card deployment project. As expected these steps are similar to any enterprise wide project but have some peculiarities.

- Lab Installation
  We assume that you have some ideas about your environment and requirements. Getting acquainted with the technology from the beginning is beneficial. Therefore it is recommend you have some lab installs probably with a few different vendors to evaluate the solutions. You should consider few key applications only and not set up the entire system which would complicate the project. The idea is to evaluate the user experience at this stage.
- Business Requirement Gathering
  Take sufficient time to gather the business requirements for all different departments involved. IT guys making unfounded assumptions have made many mistakes in the past in this part of the project.
- Processes and Policy definitions
  Based on your business requirements, you should define the processes around Smart card deployment and its life cycle management. It is recommended you seek assistance from experienced professionals. As stated previously balancing security, convenience and business benefits is critical.
- System Design and Architecture
  You should now have an internal or external team dedicated to this project that will design the overall system. Some customizations to existing solution in the market might be necessary since each environment is unique. Designing the PKI and the optimal CMS is crucial for the rest of the project.
- Training
  Administrators and helpdesk agents as well as employees need to learn how to use the system. In general you need to have a communication plan for all parties involved including the stakeholders of this project. Some systems integrators have rightfully included this step in their offerings.
- Pilot
  A pilot program for a manageable group of employees of different background is always valuable. I would recommend the scope of the pilot to be comprehensive enough without however over-loading it. Some organizations set up pilot projects with production systems since they perceive this step as a ‘pre-production’ phase. I would disagree with this approach for, on the one hand it leads to excessive costs (setting up a complete CMS, for instance is expensive) and on the other hand you might lose your focus. Testing and improving your processes and policies is a key task during the trial period. You should also survey the user population and not overlook the culture change factor.
- Large deployment
  You should start your production deployment with simplicity in mind. You can start with a few relevant applications on the Smart card and have a roadmap to add new functions in the future. Smart cards adapt themselves well to this approach, as long as you have the ‘right’ CMS allowing you to enable more applications on the fly without having to re-deploy cards. Obtaining executive sponsorship and hence the buy-in from various business units will facilitate your project.Problems will occur and it is easy to blame the new technology for any trouble. I have heard too many of “since you installed the smart card stuff, I can’t dial-up from home” or other unrelated issues. Your success lies in the way you handle people’s expectations.

What about Return on Investment?

Building a business case for any project, including those security related, is extremely important. There are different ROI models for security and especially Identity Management projects.
There is no obvious ‘Return’ in pure security except for potential cost savings. Cost If Not Invested (CINI) is a more appropriate term. However, if you approach security as a business enabler, then its return can be better defined and calculated. An example is using smart cards for digital signing, leading to paperless transactions. In general, the more applications you enable on the smart card, the better the ROI. Indeed, deploying Smart cards for remote access alone would have too high a cost to justify the solution, whereas using the card for physical and network (logical) access, in addition to Single Sign On and remote access, coupled with the proper processes, could bring tangible cost savings and increased returns.

Conclusion

Despite the security threats that come mainly from internal breaches, we want our employees to have access ‘from anywhere to anywhere’ which requires an ‘enabling’ type of security. This could only be achieved through an efficient Identity Management system that provides secure Authentication and the right level of Authorization. Although still evolving at a fast pace, smart card-based technologies for security and other site applications have matured radically over the years and offer an appealing employee badge solution for improved identity and access management.

Author Biography

Shahin Shadfar is currently the Program Manager in the Information Security group at Schlumberger, a group he helped start in 1999. He previously worked in the R&D team at Schlumberger that invented the Java Card technology used in the Security, Telecom and Banking industries.

Mr. Shadfar holds a Master of Science degree in Electrical Engineering from Georgia Tech, Atlanta as well as a Master of Science diploma in Computer Science from Ecole Superieure D’Electricite in Paris, France.