Case Study: Using Smart Cards with PKI to Implement Data Access Control for Health Information Systems

Jewel Watts and Huiming Yu

Department of Computer Science
North Carolina A&T State University

Abstract

Data access control is an important topic in Information Assurance (IA) curriculum. The data access control for health information system case study is developed to enhance IA education by providing conceptual information that is relevant and parallel the materials that are learned in the classroom. Students will be able read the case study materials and answer questions based on their reading. The learning goal of this case study is to help students understand the need for data access control, the technologies that are proposed, and how they protect the data's confidentiality, integrity, authentication and non-repudiation.

Keywords

Electronic Health Records (EHR), Smart Card, Public Key Infrastructure (PKI), authentication, integrity, confidentiality, access controls

1. Introduction

In many health systems today, paper-based records are being replaced by Electronic Health Records (EHR). EHRs allow records to be accessed, read, and transferred more efficiently than paper-based records. How to implement EHRs continues to be a topic with high interest. The goal of information technology professionals is to keep EHRs safe from threats. Keeping patient data private is one of the most important requirements in a health information system, and well defined access controls are needed. With laws in place provided by numerous governmental entities such as Health Insurance and Practice Accountability Act (HIPPA), we cannot afford to implement a nationwide EHR system without first guaranteeing data privacy. This legislation provides end-to-end ways to ensure that health records transactions are more secure, but it doesn't provide the functionality that most clinical systems need—which is a multi-user environment [1].

The information in a patient's record at a hospital usually has more data in one record than those in banks, schools, and even Human Resource departments [2]. So the need to make EHRs as secure as these organizations is a high priority. Unfortunately, privacy laws such as HIPPA cannot fully protect the patient's data from being misused. In one year from 2006-2007, more than 1.5 million names were exposed during data breaches that occurred in hospitals [2]. Even though regulations are in place to secure patient data, there seems to be loopholes that allow un-authorized access to patient data. Some of the laws contain vague language such as "reasonable efforts" and "acceptable measures".

To be able to implement and benefit from EHRs, there needs to be a solid platform that allows secure access to patient files that work in parallel to preserving the inter-operable workflow of the average hospital. Along with securing such a platform, the need to maintain a high availability of the records needs to also be preserved. This means that EHR data should be delivered in a timely manner in which the patient's health will not be compromised.

In this case study, we will discuss a business case that was done by a contractor of the Federal government in choosing whether Smart Cards/PKI is the solution to access control issues. The case study is entitled, “CIO PKI/Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications” [3].

2. Case Study: Using Smart Cards with PKI to Implement Data Access Control for Health Information Systems

2.1. Background

The General Services Administration contracted Booz-Allen & Hamilton to document a business case approach on the topic of Public Key Infrastructure (PKI) on Smart Cards to be used by Federal agencies. The CIO Enterprise Interoperability Emerging IT Committee is planning to use the presented methodology to figure out if using Smart Cards along with PKI is going to be able to provide authentication, access control, and electronic commerce. This case study was prepared to help Federal agencies to understand business case methodology, and also to figure out if Smart Card’s implementation’s benefits will outweigh the risks. The Government Paperwork Elimination Act has pushed Federal agencies into making e-commerce a reality. To support this move, Federal agencies are being required to increase overall network security providing information assurance, in which they have considered PKI/Smart Cards as a solution [3]. This report focuses on using Smart Cards along with PKI. The methodology that was used in this business case closely looks at the question, “Is this worthy enough to invest in?” It also finds the feasibility of its technical and programmatic implementations. This is the step-by-step business case methodology that was used [3].

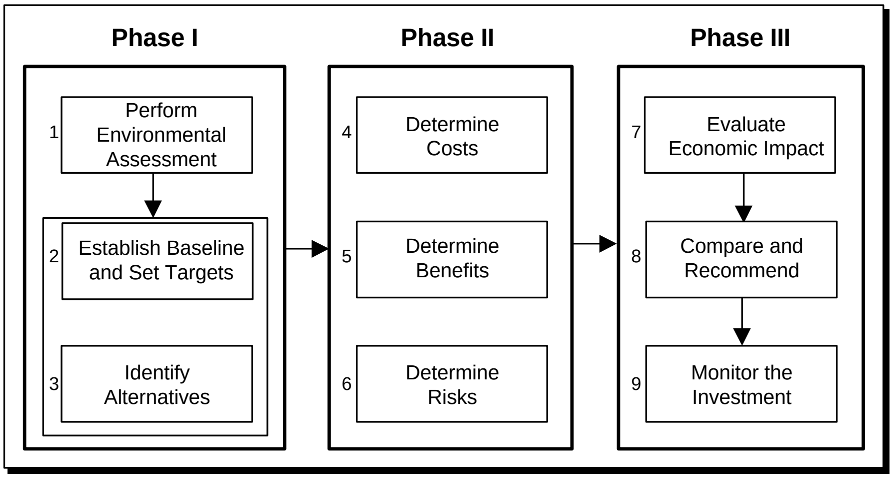
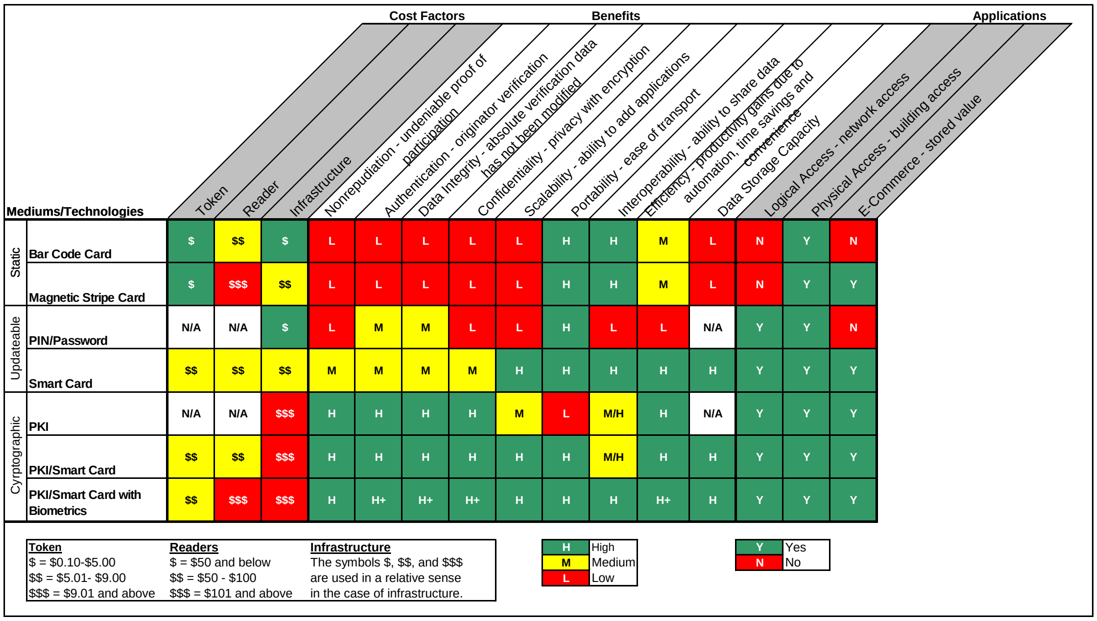


Figure 1. Business Case Analysis Methodology for PKI/Smart Cards

The article has provided supporting data that shows various technologies that have been developed for information assurance. Since there is not only one best way to provide information assurance to all agencies, the agency has to choose which technology to implement based on their individual benefit-cost analysis. PKI/smart cards are useful to agencies that have a mobile workforce with access to card readers (taking advantage of the portability of smart cards), agencies placing a high value on building access, and those that conduct business electronically outside of their agency. Here are the technology solutions that have been weighed, based on cost of tokens, readers, and infrastructure [3].



	Mediums/Technologies	Cost Factors			Benefits									Applications		
		Token	Reader	Infrastructure	Nonrepudiation - undeniable proof of participation	Authentication - originator verification	Data Integrity - absolute verification data has not been modified	Confidentiality - privacy with encryption	Scalability - ability to add applications	Portability - ease of transport	Interoperability - ability to share data	Efficiency - productivity gains due to automation, time savings and convenience	Data Storage Capacity	Logical Access - network access	Physical Access - building access	E-Commerce - stored value
Static	Bar Code Card	$	$$	$	L	L	L	L	L	H	H	M	L	N	Y	N
	Magnetic Stripe Card	$	$$$	$$	L	L	L	L	L	H	H	M	L	N	Y	Y
Updateable	PIN/Password	N/A	N/A	$	L	M	M	L	L	H	L	L	N/A	Y	Y	N
	Smart Card	$$	$$	$$	M	M	M	M	H	H	H	H	H	Y	Y	Y
Cyrptographic	PKI	N/A	N/A	$$$	H	H	H	H	M	L	M/H	H	N/A	Y	Y	Y
	PKI/Smart Card	$$	$$	$$$	H	H	H	H	H	H	M/H	H	H	Y	Y	Y
	PKI/Smart Card with Biometrics	$$	$$$	$$$	H	H+	H+	H+	H	H	H	H+	H	Y	Y	Y

Token	Readers	Infrastructure
$ = $0.10-$5.00	$ = $50 and below	The symbols $, $$, and $$$
$$ = $5.01- $9.00	$$ = $50 - $100	are used in a relative sense
$$$ = $9.01 and above	$$$ = $101 and above	in the case of infrastructure.

H	High
M	Medium
L	Low

Y	Yes
N	No

Figure 2. Three types of technology: Static, Updateable and Cryptographic

Figure 2 shows three types of technology that are Static, meaning it can't be changed, Updateable, meaning it can be changed, and Cryptographic, meaning it can be changed and programmed. These are listed from least secure to more secure (from bar code cards to PKI/Smart Cards with Biometrics). Each technology is scored in the areas of the relative cost, the reader, and the infrastructure. Those in green are the lowest cost technologies, yellow for moderate costs, and red for highest costs. The matrix also measures the benefits of each technology.

2.2. PKI

PKI uses public key cryptography. An algorithm is created and produces two mathematically computed keys that are related. Using PKI enforces authentication, confidentiality, data integrity, and also non-repudiation. The way that PKI works is by using a public key along with a private key to mathematically scramble data. Both keys consist of a series of numbers or bit strings. The private key, which is maintained by the user, cannot be found by using the public key, which is openly available to a trading partner. Data encryption is done by one key, and decryption done by the other.

PKI is able to have the functionality of authentication by consulting Certificate Authorities (CA), Registration Authorities (RA), and other authorities that provide a variety of security features. These features include message integrity, key recovery, data privacy, signature verification, and user authentication. The public key is made public and formed into a digital certificate when the trusted authority cryptographically signs the certificate. The digital signature is created from the data and the sender's private key. The signer first hashes the data to a fixed size value. They then encrypt the hashed value with their private key. This final piece of data is then appended to the data that is digitally signed. To verify the signature, three pieces of information are examined, including the value of the hash, the transmitted signature, and the signer's public key. The signature is verified when the signature matches the hash value as well as the key.

Using PKI, data alternations can be detected. Importantly, it is the Certificate Authorities responsibility to manage three main functions. The first is to manage the certificate life cycles, which include issuing the keys. The second is to manage key revocation when a private key is lost, stolen, or made public. And the third is to give notice as to which key pairs have been revoked.

2.3. Smart Cards

Smart Cards, which are the same size as a credit card, are more secure than magnetic stripe cards. Smart Cards are embedded with a microprocessor which processes information, and memory which can store information. The card works in unison with a card reader, which transfers information to and from applications. Smart cards have a wide range of applications including electronic purse, logical and physical access control, health care, telecommunications, and transportation. To date, approximately 700,000 smart cards have been issued within the Federal Government [3].

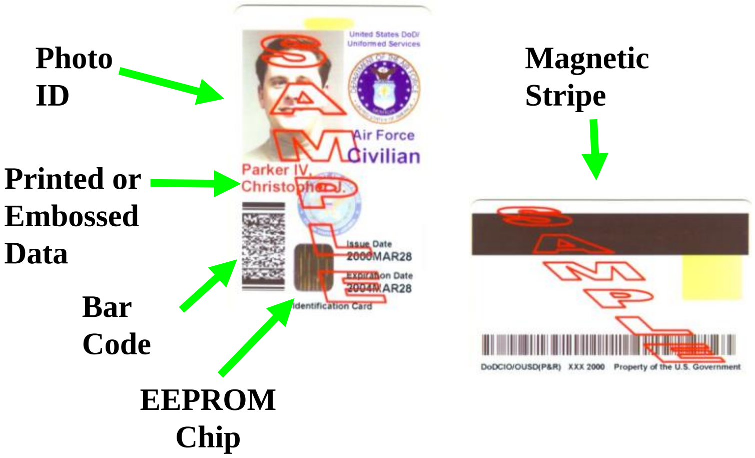


Photo ID
Printed or Embossed Data
Bar Code
EEPROM Chip
Magnetic Stripe
United States DoD/ Uniformed Services
Air Force
Civilian
Parker IV, Christopher J.
Issue Date 2000MAR28
Expiration Date 2004MAR28
Identification Card
SAMPLE
DoDCIO/OUSD(P&R) XXX 2000 Property of the U.S. Government

Figure 3. A Typical Smart Card

Smart cards can be used in both logical access control systems and physical access control systems. A physical access control system is an automated system that controls an individual's ability to access a physical location. A logical access control system, like an EHR access system, is an automated system that controls an individual's ability to access one or more computer system resources. These resources include workstations, networks, applications, or databases. Smart cards may use three levels of logical access control. The first is file access security. The second is the ability to detect and respond to a sequence of invalid access attempts with a self-locking mechanism. And the third is the "logical channel", which is a logical link between the host system and a file on the smart card.

The use of smart cards for logical access augments the traditional PIN/password logon process, which was described by Microsoft Chairman and Chief Software Architect Bill Gates in the following manner: "Passwords are the weak link in Internet security. The use of smart cards will become the major way for corporate users to authenticate themselves to the network." [3].

2.4. Governmental "Large Agency" - Applications of Smart Card/PKI

The agency has three administrations which serve approximately 240,000 employees and a large external population. They use internal smart cards to be the standard identification card when

interacting with various administrations and offices. They are conducting PKI projects that support secure email and Web enabled applications for external customers, as well as with staff. Their PKI operations are verified through VeriSign. They have issued 100,000 certificates that are in use.
The agency missions that are promoted by the implementation of PKI/smart cards are [3]:

- Ensuring the confidentiality of highly sensitive information is maintained, especially with regard to medical data
- Providing a means for the constituents to transport core registration data, thus enabling a higher level of service by improving processing time and data accuracy
- Providing strong authentication and digital signature capability to ensure secure data transmission.

The Smart Cards were issued to its employees as well as its counterparts. The agency prepared specifications for the Smart Card and also finalized the way that they were going to obtain the necessary software, hardware, and firmware. They have organized a Smart Card management team that guides the development of the project and makes sure that the implementation goals are met and are consistent with stated requirements.

The following are the goals of the Smart Cards [3]:

- Promote health care versus hospital care
- Seamlessly improve services to constituents
- Reduce data entry errors on records
- Encourage use of electronic business methods
- Implement only one card across the entire agency
- Be honored by all facilities, and all employees
- Will be a scalable card
- Enhance business services and bring inherent value to the mission
- Be network-centric and not card-centric
- Be interoperable across the Federal government and have digital certificate for e-commerce and e-government participation
- Store clinical and administrative data on one card, and be able to change information with ease.
- As the card matures, it will be capable of more applications such as:
- Interaction with kiosks
- Prescription refills

A proof of concept demonstration was performed on August 31, 2000. It showed that Smart Card technology would be a practical approach to improving the systems, processes, and data management abilities of supporting delivery of care to citizens. The agency continued with full implementation of the Smart Card because of the successful demonstration. It is expected that business processes, technology configuration, training and communications activities, and support infrastructure will be developed and deployed during the initial implementation phase [3].

It is the goal of the agency to make sure that citizens can obtain services, and the following factors should be considered to evaluate the initial implantation [3]:

- Constituent and staff satisfaction with the administrative and emergency data set
- The card's success in enabling electronic service delivery using public/private key technology
- The success of initial interfaces with existing systems
- Card issuance stations.

The PKI certificate policy has been published. Though this policy will change over time, it is the cornerstone of PKI that will enable orderly expansion, migration to new technologies, and interoperability inside and outside the agency [3]. They are using PKI to secure electronic mail and to also provide secure socket layer (SSL) services for some Web servers. PKI will be used by personnel, contractors, and business partners. The on-site CA, VeriSign, issues individual certificates. These certificates are stored in each individual user's e-mail contact list. To prove one's identity, it is done centrally and then passes through Cygnacom Solutions, Inc, which serves as the PKI national registration authority. They also provide documentation and help desk services for those subscribed to PKI.

Two types of certificates are issued [3]:

- User certificates are attributed to individuals and can be used for secure electronic mail, Web-based applications and remote access services.
- Server certificates are attributed to web servers to provide server authentication and encrypted sessions.

Each certificate is intended for use by employees or contractors and provides secure communication and transactions for internal business processes [3].

2.5. Benefits

2.5.1 PKI Benefits

PKI allows users to communicate securely by offering them controlled access to the intranet for all corporate information, such as human resource data, secure e-mail, and various applications [3]. PKI secures the actual transaction through encryption, not the network or communication link. PKI facilitates the exchange of confidential data with business partners by enabling the creation of secure extranets and virtual private networks (VPN) that give select partners easy access to business-critical information stored on internal networks [3].

A list of benefits that PKI provides:

- PKI provides a secure transaction. It makes sure that the exchange of confidential data is done via secure extranets and virtual private networks (VPN). When using VPN, there is easy access to business-critical data that is stored in internal networks.
- PKI provides authentication, which determines a reliable 2nd party, by only allowing single sign-on and by using electronic signatures.
- PKI provides data integrity, which protects the system against unauthorized data. Modification by assuring that the received data is accurate and complete, and has not been altered or modified.

- PKI provides non-repudiation, which verifies the origin of a transaction, by giving the sender proof of delivery, and giving the recipient proof of the sender's identity. After a transaction between the two parties, neither can deny that data was sent/received.
- PKI provides confidentiality, which protects information from being seen by unauthorized entities, by encrypting confidential data.
- PKI provides interoperability, which is a "chain of trust" between all active parties, by using a single certificate that is trusted by all parties. This allows all trusted parties to securely interact with each other.
- PKI provides Bridge Certification Authorities, which allows different PKIs to be linked. This allows technical and policy interoperability. Agencies also have the choice to exclude certain sub-trees that they do not want to interact with.
- PKI provides scalability by allowing many-to-many relationships.

2.5.2. Smart Card Benefits

PKI certificates are stored on Smart Card tokens. Smart cards have become widely accepted due to the high level of security the card provides compared with PKI certificates stored on a hard drive [3]. Smart Card technology offers benefits such as providing interoperability and scalability, and unlike PKI, it also provides portability.

A list of Smart Card benefits:

- Smart Cards are portable, which means the card-holders have freedom and access to their cards immediately.
- Smart Cards offer interoperability, which means that they can gain access to multiple networks, services, and the Internet.
- Smart cards can scale applications by defining the number of users, number of applications, and number of certificates. This helps to expand Smart Card usage and cut unnecessary costs
- Smart Cards allow an organization to add new users quickly by ordering a new card. This is only a small monetary investment.
- Smart Cards permit an organization to not only have two factors in authorization, but three forms, such as with the use of biometrics. Using biometrics with the Smart Card provides an extra measure of verification. Biometrics can be the use of facial recognition, voice pattern recognition, iris scan, hand geometry, and fingerprint recognition.
- Smart Cards have a high efficiency, which make them able to complete digital forms.
- Smart Cards have a much higher data storage capacity than magnetic stripe cards. Most Smart Cards have a 32 Kbyte chip on which data can be stored, which is 100 times greater than magnetic stripe cards.

2.5.3 Benefits of Implementing PKI-Enabled Smart Cards

Some may argue that Smart Cards aren't needed to implement PKI, but there are many advantages to using PKI-enabled Smart Cards. When both technologies join, increased benefits are:

- The private key is generated and stored on the Smart Card. The operating system on the Smart Card prevents key exposure outside the card.
- Digital certificate is stored on the Smart Card itself, rather than have it on a hard drive or disk. This makes authentication and non-repudiation possible because the user of the card has a PIN that accesses the signature.

- Information on the Smart Card is encrypted, which means secure data retrieval, transfer, and storage.

3. Conclusion

PKI/smart cards are a sound business investment when they are used to satisfy security and business needs as they provide the means for secure online transactions [3]. PKI enabled Smart Cards give a great measure of security benefits because it encrypts transactions, offers non-repudiation, authentication, data integrity, and confidentiality. By placing PKI certificates on a smart card, scalability, portability, interoperability (via the Federal Bridge), efficiency, and data storage capacity are possible [3]. They are also able to be used for logical access to computer networks and physical access to buildings. This case study provides the materials to help students understand how to implement data access control by using Smart card with PKI.

References

[1] Unites States Department of Health & Human Services, "Administrative Simplification under HIPAA: National Standards for Transactions, Privacy, and Security [Online]", *http://www.dhhs.gov/news/press/2002pres/hipaa.html*

[2] Kroll Fraud Solutions, "2008 HIMSS Analytics Report: Security of Patient Data [Online], *http://www.mmc.com/views/Kroll_HIMSS_Study_April2008.pdf*

[3] "CIO PKI/Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications". *http://smart.gov/library.cfm#category_d9c8062b-62b7-11d6-bcd1-8aa2af114fbf*