Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise

Bengisu Tulu
Claremont Graduate University

Haiqing Li
Claremont Graduate University

Samir Chatterjee
Claremont Graduate University

Brian Hilton
Claremont Graduate University

Deborah Beranek-Lafky
Claremont Graduate University

See next page for additional authors

Authors
Bengisu Tulu, Haiqing Li, Samir Chatterjee, Brian Hilton, Deborah Beranek-Lafky, and Thomas Horan

Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise

Bengisu Tulu
Claremont Graduate University
bengisu.tulu@cgu.edu

Haiqing Li
Claremont Graduate University
haiqing.li@cgu.edu

Samir Chatterjee
Claremont Graduate University
samir.chatterjee@cgu.edu

Brian N. Hilton
Claremont Graduate University
brian.hilton @cgu.edu

Deborah Lafky
Claremont Graduate University
deborah.lafky@cgu.edu

Thomas A. Horan
Claremont Graduate University
tom.horan@cgu.edu

ABSTRACT

This paper presents a case study of a digital signature solution implementation for a healthcare organization that provides disability evaluation services for various government agencies and private companies. One service the company provides for its clients is online disability report generation and electronic report submission. When generating these disability reports, the signature of the examining physician is required for submission. The current process used by the company involves the manual collection of signatures. To streamline this process, and to meet legal and client requirements, the company was seeking a digital signature solution. A security framework previously proposed was utilized to guide the implementation of the digital signature solution. This security framework consists of eight sequential stages. An in-depth description of the first six stages for this case, including guidelines for choosing digital signature solutions, vendor analyses, and implementation issues, are provided.

Keywords

Healthcare, Digital Signatures, Public Key Infrastructure, Security Framework, Case Study

INTRODUCTION

Digital signatures are messages that identify and authenticate a particular person as the source of the electronic message; and indicate such person's approval of the information contained in the electronic message (Policy and Communications Staff, 2000). They help users to achieve basic security building blocks such as identification, authentication, and integrity. This paper presents a case study regarding the implementation of digital signatures within a healthcare organization that collaborates with various clients such as government agencies and private organizations. Providing timely and accurate medical disability evaluation information to these clients is an industry challenge. The company meets this challenge by using technology to continuously improve performance and functionality. They provide electronic medical services to healthcare practitioners for filing disability evaluation reports and sending them to clients. Regardless of the method used to generate binding disability reports, the examining physician must sign them. The signature process currently used requires the manual collection of signatures. The company was seeking a digital signature solution that would meet legal and client requirements and would streamline the current signature process. A security framework previously proposed (Tulu and Chatterjee, 2003) was utilized to guide the implementation of the digital signature solution. This security framework consists of eight sequential stages. However, the framework is flexible allowing the implementer to revert to a previous stage at any time during the implementation if needed.

The next section provides brief background information regarding the company and its processes as well as digital signature processes. It will continue with the analysis of the digital signature implementation by utilizing the aforementioned security framework. Each step will be explained in detail within the context of this case study. The paper will conclude with a discussion and areas for future research.

BACKGROUND

Company Background

The company provides an array of disability evaluations, management, and information services nationwide. They conduct disability evaluations for clients such as the Veterans Administration (VA), the Social Security Administration (SSA), and Worker's Compensation. Over the past 20 years, they conducted and produced over 2 million disability exams and ratable reports. They operate 26 medical evaluation facilities, and its nationwide provider network consists of 10,000 fully credentialed physicians and auxiliary providers.

Providing timely and accurate medical disability evaluation information to clients is an industry challenge. The lack of disability evaluation standards and a common terminology between various agencies also introduces a challenge for physicians. Each disability program has its own definitions and terminology. A physician that is dealing with a disability claim must learn the terminology related to that specific claim process and provide an evaluation report accordingly. The differences between terminologies of one organization to another may cause further confusion and result in a less accurate and/or poor quality assessment. The company meets these challenges by using technology to continuously improve performance and functionality. One of these technologies allows the examiner to manage the claim cases online and in real-time. Another one formats and presents the medical data gathered in the online report submission software in a narrative report with electronic signature capability.

Online report submission software, developed in-house, is used to submit medical claim reports to the company where these reports are reviewed for quality assurance and submitted to the clients. The electronic signature used in this software currently utilizes a login username and password. However, according to the legal and client requirements, this type of electronic signature is not accepted as a proof of signature. Therefore, after the doctor finalizes and "locks" the report, an HTML page must be generated for the physician to print and sign after submitting the final report. This manually signed page is then faxed back to the company where it will be scanned and kept with the electronic report as a proof of signature.

Digital Signature Technology

Digital signatures enable people to sign digital documents by providing the properties of a handwritten signature. They must fulfill the five compelling attributes of handwritten signatures as listed by (Schneier, 1996). He stated that the handwritten signatures are authentic, unforgeable, not reusable, unalterable, and cannot be repudiated. In the case of handwritten signatures, both the signature and the document are physical things, which makes it difficult for the "signer" to claim the signature is not their own. In order to provide a secure electronic signature scheme, these attributes must be satisfied. Electronic signature technologies include PINs, user identifications and passwords, digital signatures, digitized signatures, and hardware and biometric tokens (Policy and Communications Staff, 2000). Therefore, it is important to distinguish between electronic and digital signatures. Digital signatures are a subset of electronic signature technologies that utilize keys and cryptographic algorithms for signing documents.

Digital signatures can be generated using various techniques; however, the only digital signature standard approved by National Institute for Standards and Technology (NIST) employs public key cryptography combined with a one-way hash function. This infrastructure, commonly referred to as the Public Key Infrastructure (PKI), requires each user to have a public-private key pair where the public key is available to the world while the private key is only known by the user. Figure 1 illustrates the use of PKI for generating digital signatures.

The following is an example of a digital signature scenario. Bob (sender) wants to send Alice (receiver) a text message with a digital signature. First, Bob creates the text message to be signed and generates a hashed message using a message digest function (e.g., MD5, SHA1, etc.). A message digest function is a mathematical function that generates a 162-bit hash of the original message; this hash cannot be used to regenerate the original message. Therefore, the hashed message is secure and unique. Once Bob has the hashed message, he uses the public key digital signature algorithm and his private key to sign the hash to generate a digital signature for the specific document. Once Alice receives the digital signature, and the corresponding text message, she will need to calculate two separate values. First the hashed message of the received text is calculated using the same hashing algorithm. Then, once she has the hash value, she can now use the decryption algorithm with Bob's public key and digital signature to retrieve the signed hash. If she can decrypt the digital signature, this implies that Bob's private key was used to encrypt the hashed message. The final step for Alice is to compare the hash she calculated with the hash she retrieved from the decryption process. If these two hashed messages match, this implies that she received the original message Bob signed (thus preserving message integrity).

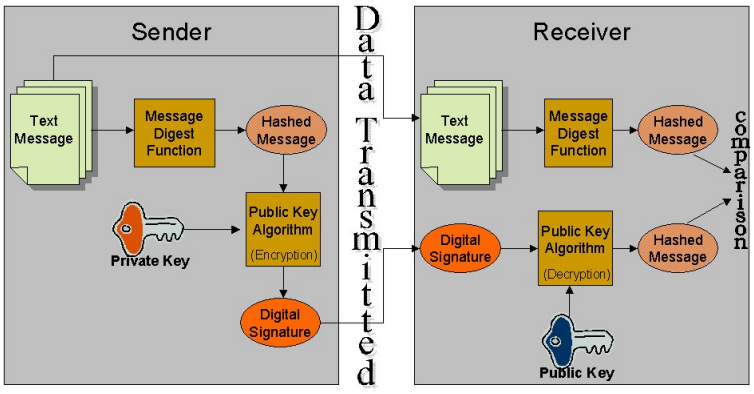

Figure 1. Digital Signatures Using PKI

Key generation and distribution are the biggest challenges in deploying PKI. The solution is to use a trusted central authority – called a Certification Authority (CA) in PKI. CA is a trusted entity that accepts certificate applications from entities, authenticates applications, issues certificates to users and devices in a PKI, and maintains and provides status information about the certificates. If a CA is managing a large, geographically dispersed population, it may use Local Registration Authorities (LRAs), who provide direct physical contacts with subjects. These LRAs are especially required if the CA is issuing a high level of assurance for its certificates. Currently, there are four levels of assurance defined in the evolving government standard (PEC Solutions, 2000): Rudimentary; Basic; Medium; and High.

Traditionally, PKI architectures fall into one of three configurations: a single CA, a hierarchy of CAs, or a mesh of CAs. Each of the configurations is determined by the fundamental attributes of the PKI: the number of CAs in the PKI, where users of the PKI place their trust (known as a user's trust point), and the trust relationships between CAs within a multi-CA PKI (Polk and Hastings, 2000). The most basic PKI architecture is one that contains a single CA, which provides the PKI services (certificates, certificate status information, etc.) for all the users of the PKI. All the users of the PKI place their trust in the sole CA of the architecture. Isolated CAs can be combined to form larger PKIs in two basic ways: using superior-subordinate relationships, or peer-to-peer relationships. In the former, which is called a hierarchical PKI, all users trust a "root" CA. There is single point of trust. The latter, a mesh PKI, connects CAs with a peer-to-peer relationship. A PKI constructed of peer-to-peer CA relationships is called a "web of trust". The Bridge Certification Authority (BCA) architecture was designed to address the shortcomings of the two basic PKI architectures, and to link PKIs that implement different architectures. Unlike a mesh PKI CA, the BCA does not issue certificates directly to users. In addition, the BCA is not intended to be used as a trust point by the users of the PKI, unlike the "root" CA in a hierarchy.

IMPLEMENTATION OF A SECURITY FRAMEWORK

OASIS PKI Technical Committee, which was formed in January 2003, conducted a survey and a follow-up survey in June and August 2003 respectively, with the goal of identifying primary obstacles to PKI deployment and usage (Hanna, 2003). A major finding of this recent study shows that the PKI is a truly horizontal, enabling technology with many applications. Nevertheless, 92% of the respondents noted that they would use PKI more if obstacles were removed. The top two obstacles reported were: (1) Software Applications do not support PKI, and (2) Cost is too high. Respondents of this study also agreed that the one critical application that needs improvements in PKI support is "document signing"; the problem examined in this study.

Keeping these drawbacks of PKI deployment in mind, a framework was selected to guide the PKI implementation process. A security framework (Tulu and Chatterjee, 2003), which was proposed to help management decide how to make their organization compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), was utilized to decide on how to implement the PKI at this company. The framework, illustrated in Figure 2, consists of eight sequential stages and allows implementers to revert to a previous stage any time during the implementation. The following subsections describe each step within the context of this specific case.

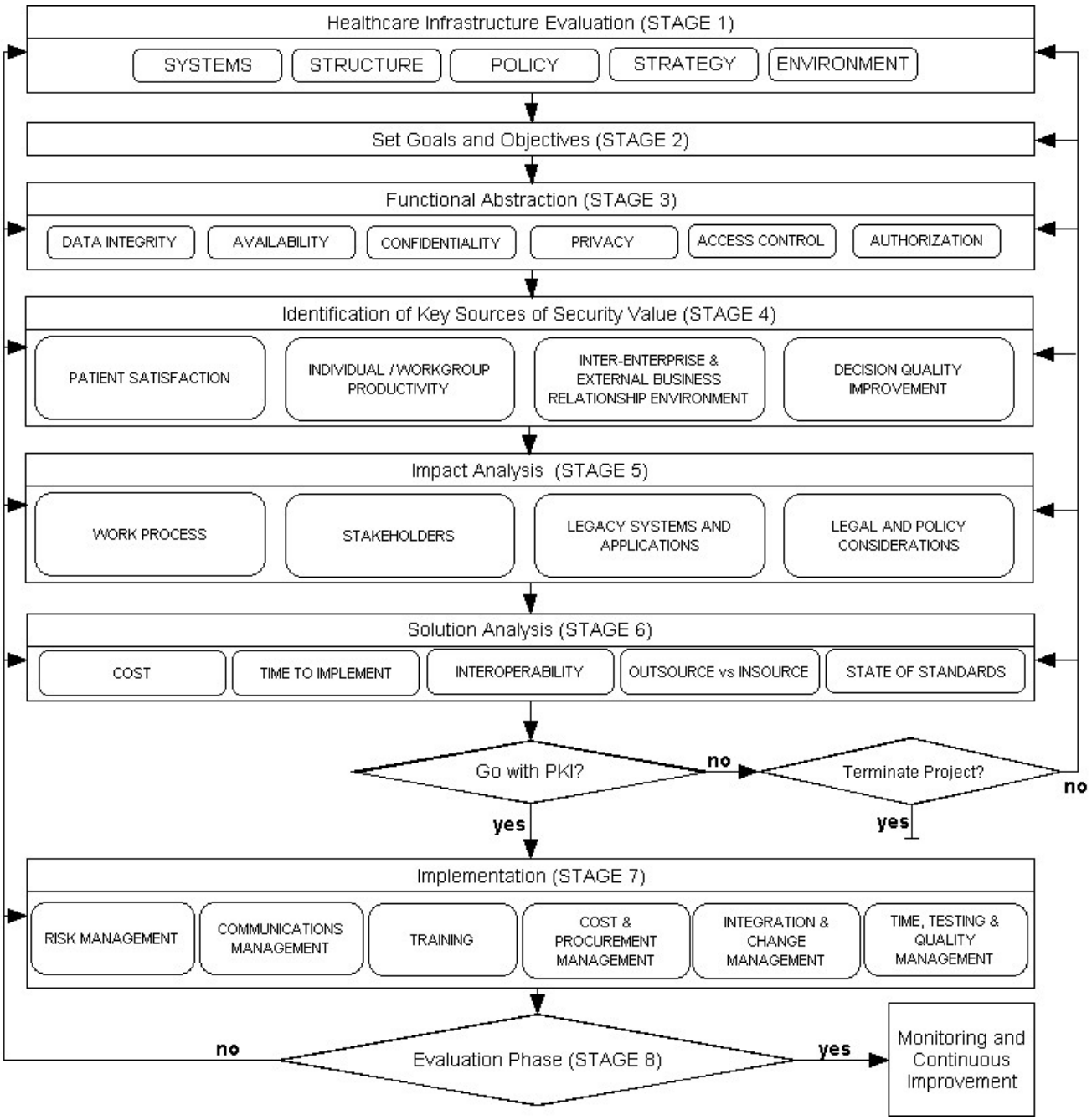

Figure 2. Security Management Framework (modified from Tulu and Chatterjee, 2003)

Stage 1: Infrastructure Evaluation

The infrastructure evaluation is intended to provide a diagnostic of the current state of the company information systems infrastructure. Table 1 below presents a brief summary of the diagnostics.

Stage 2: Set Goals and Objectives

The main goal of the PKI implementation is to eliminate the manual signature collection from physicians in the company provider network and streamline the online medical report collection process. Meanwhile, this will enable the company to implement a technology solution consistent with current and emerging standards and practices while satisfying the digital

signature requirements enforced by HIPAA rules and NIST standards. It will also establish a trust relationship between physicians and clients without requiring the company's approval for a personal signature.

SYSTEM	HW: Servers, client machines SW: MS Windows 2000 OS, IE Explorer 5.5 or better Applications: MS SQL Server, Oracle, MS File System, IIS 5.0 Web Server Network Security: HTTPS and SSL using Verisign Server side certificates.
STRUCTURE	Work Process: Described in the background section Organizational Structure: The company has contracts with various federal agencies, state agencies, and private companies. Based on these contracts, the company is responsible of providing a medical report, generated by a physician after examining a claimant, for these clients. The company's nationwide provider network involves 10,000 physician offices. The company operates 26 clinics. Roles and Responsibilities: Physicians are responsible for providing an accurate medical exam report to the company in a timely manner. The company is responsible for the completeness of the medical report as well as the format and timeliness to its clients. Geographic Spread: The company operates in 50 states.
POLICY	Organizational Security Policy: The company's security policy is strictly controlled by various rules and regulations and is enforced by governmental healthcare organizations. The company is under pressure to meet the specific security requirements of its clients. To deal with these various governmental agencies and private organizations, the company requires a security policy that could help to meet these requirements. Current security policy is to become HIPAA compliant and follow the VA PKI policy (Department of Veterans Affairs, 2003) very closely as the VA is the largest client of the company. Management Support: The company's upper management is very supportive of technology use and aware of the security issues involved. Their mission is to be a pioneer in developing and implementing information technology to improve the effectiveness of conducting and managing disability evaluations. Therefore, they are very responsive to problems that occur while implementing new technologies. Government Policy on Security: Explained in Section 2.
STRATEGY	A core competency of the company is bringing new technology to the field of disability evaluations. They have positioned themselves as pioneers and innovators in this field. In the case of this digital signature project, the company is ahead of its clients which is introducing some new problems into their strategic decision making process. That is, they need to predict the behavior of their clients in order to implement a technology that will be compatible with future implementations.

Table 1. Infrastructure Diagnosis

Stage 3: Functional Abstraction

This stage recommends an appraisal of the specific security requirements by rating them in importance of the operation for the enterprise. The basic security blocks are included in Table 2, which illustrates the results of this analysis specific to the company. The values were derived from interviews with key company personnel and security standards imposed by the healthcare industry (e.g., HIPAA).

	Authentication	Authorization	Access Control	Integrity	Confidentiality	Privacy	Availability
Importance	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM

Table 2. Functional Abstraction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authorization is the process of deciding if someone or something is allowed to have access to a service or a resource. Access control is a much more general way of talking about controlling access to a resource. It is analogous to controlling entrance by some arbitrary condition which may or may not have anything to do with the attributes of the particular user (The Apache Software Foundation, 2003). Integrity is the process of preventing, deterring, and detecting improper modification of

information during or after transit (Kleinsteiber, 2002). Confidentiality is the process of protecting against the disclosure of information to parties other than the intended recipient(s). Privacy is the ability and/or right to protect your personal secrets, privacy cannot extend to legal persons such as corporations (Anderson, 2001).

Stage 4: Identification of Key Sources of Security Value

Patient satisfaction is always a key issue for healthcare providers. In the case of disability evaluations, rather than use the term "patient", "claimant" is used since each patient evaluated by a physician has filled-in a claim form and submitted it to their healthcare provider (client). The medical examination conducted by the physician is directly related to this process and it is necessary for the claimant to be reimbursed by the client. By utilizing a digital signature solution for electronic reports, the company will provide faster service to its clients, which directly effects the response time of the client to the claimant. Moreover, the PKI enables the company to encrypt all documents in a secure manner. This will help the company to ensure the privacy of claimant information.

Another key source of security value relates to the physician productivity. Eliminating the manual print-and-fax process and replacing it with a "single-click" will increase physician productivity. For the company, manual scanning of signatures will no longer be required. External business relationships with clients will be enhanced as a result of providing a trust relationship directly between providers and clients and also by eliminating the dependency on the company for signature verification. The new digital signature system will improve the decision-making process for both clients and the company where the accuracy of a medical report is of concern.

Stage 5: Impact Analysis

The digital signature standards that are accepted as HIPAA compliant are Public Key Cryptography and the One-Way Hash function. Therefore, the company should benefit from these digital signature standards. Preliminary analysis has indicated that the proposed solution would streamline the workflow process and eliminate the overhead on both physicians and the company. Impact analysis of the workflow process was mentioned in the previous subsection. When stakeholders are considered, the main concern is the impact on the physicians that will lead to a specific implementation requirement for a simple, client side signature tool. Physician satisfaction is very critical concern in implementing a PKI-based digital signature solution for the company. Based on a study (Horan, Tulu, Hilton and Burton, 2004) conducted among providers, it was reported that work practice compatibility is very important in determining physicians' behavioral intent to accept and use a new system. Therefore, it is important to ensure that the new system will not introduce dramatic changes into current work practice processes. For example, if signing a report becomes a complicated process, it is expected that physicians would be less willing to use the system themselves and would eventually engage their assistants in the process of signature collection.

PKI implementation may have a significant impact on the existing legacy systems within the company. The implementation of a digital signature solution for signing medical reports, will significantly impact the two applications used for online report submission and generation. The implementation of the PKI will necessarily be highly integrated with these two applications and significant programming changes and additional hardware may be required. Currently, the online submission software does not allow physicians to view the Word document after they lock it. To generate a digital signature, the physician must to view the Word document to be signed and click on the "lock and sign" button to generate a digital signature.

Legislative initiatives surrounding digital signatures began in the states with the first digital signature law that was enacted by Utah in 1996. This law was based on work done by the Information Security Committee of the American Bar Association's Section of Science and Technology (Garfinkel, 2002). As more states began to enact various similar laws, two models – the Utah Model and the Massachusetts Model – emerged to become templates for others. The Utah model "envisioned a public key infrastructure supported by state-licensed certification authorities" (Garfinkel, 2002) whereas the Massachusetts model was more technology-neutral (i.e. not mandating PKI), including both digital signatures and other forms of electronic authentication in its list of accepted technologies.

While state legislative activities were on the increase, the federal government tried to close the debate in 1999 and passed the Uniform Electronic Transactions Act (UETA), which does not enforce PKI. In 2000, former President Clinton signed the Electronic Signatures in Global and National Commerce Act (E-SIGN), which added federal consumer protection elements absent from UETA. E-SIGN "pre-empted all state laws except state laws that conform to the official text of UETA"(Garfinkel, 2002). E-SIGN and UETA gave digital signatures the same legal validity as traditional paper-based handwritten signatures. This implies that any standard electronic signature technology accepted by federal standards is a legally valid proof of signature.

UETA and E-SIGN do not impose the use of digital signatures at the federal level; in fact, each federal agency and organization has the right to require higher security levels for electronic signatures. These legal considerations are very important for electronic signature implementations. Since the subject company operates in different states, and deals with state and federal agencies as well as with private organizations, the company must implement a solution that is at the intersection of all the proposed solution sets; which eliminates all but PKI. While PKI will adequately address the legal requirements, there are other considerations that must be factored in to the final implementation. These revolve around the selection of a certification authority. The key considerations are: certificate reliability; authority reliability; CA architecture and its impact on the clients' existing systems; and cost. Since the subject company has no experience in functioning as a CA, outsourcing this service is the only available option. A vendor must be selected that optimizes the cited factors. It should be noted that the cost factor is closely tied to level of assurance. The estimates for this phase of the project were based on the lowest level of assurance. A higher level of assurance would incur additional charges as well as complicate the certificate management process, due to the additional proof required for authentication.

Stage 6: Solution Analysis

A complete requirements analysis will be necessary to formulate a solution. A digital signature solution, intended for internal use only, will mostly depend on the availability of technology and the preferences of internal users. In this case, however, the company and its clients will use the digital signature solution for authentication and verification. To evaluate the existing solutions, meta-requirements were first identified. Then, these meta-requirements were expanded to specify implementation requirements and standards. Finally, the evaluation criteria for each requirement were specified according to the implementation requirements. Table 3 illustrates the requirements and the evaluation criteria.

Meta Requirements	Implementation Requirements	Evaluation criteria
Legal compliance – This solution should be able to provide legal binding signatures.	E-SIGN / UTEA / 21 CFR 11	Match the requirements of E-SIGN and/or UTEA
	State laws	Match the state requirements
Client Requirements – The signature generated should be compatible with client requirements.	PKI based digital signature solution	Use one of the three algorithms provided by the Digital Signature Standard (DSS)
Special Industry Requirement – This solution should match the healthcare industry standard.	HIPAA security matrix	Message integrity
		Non-repudiation
		User authentication
		Other Option Requirements
End user requirements – This solution should match the user requirements. The users include providers, clients, and the company.	Platform compatible	Web based solutions
	Integrated with current reporting system	Support Microsoft Windows Operating system, and Internet Information Server 5
		Support Microsoft Word Documentation format
		Provide online signing and verification
	CA solution	No lock with single CA provider
	Manageability	Provide management interface; audit trials; data storage solution for digitally signed documents.
	Customizable	Vendor provides standard APIs
	Easy to use for physicians	No special hardware and software requirements
	Cost	The cost for physicians should be minimum
		The implementation cost should be reasonable based on the fair market price

Table 3. Requirement Analysis

Table 4 illustrates the comparison of digital signature application solutions based on the five items listed in the framework as well as additional items that were identified during the requirements analysis phase. Pricing for a Signature/Certificate

solutions analyzed for 100 users ranged from $2,695 to $33,000. The reason for the wide range in pricing was due to the one-time server fee requested by Provider2, which is $24,500 regardless of the number of users. However, if the number of users increases to 10,000, this solution becomes more cost effective whereas the suggested solution from Provider1 becomes less cost effective. The price range for 10,000 users is $178,900 to $393,000. Here, the certificate cost is a higher proportion of the total annual cost, however, it is important to keep in mind that the examining physician rather than the company could absorb the cost of the certificates.

Evaluation Criteria	Provider 1	Provider 2	Provider 3
Match the requirements of E-SIGN and/or UTEA Success case that work with government agents	Yes	Yes	Yes
Use one of the three algorithms in DSS	Yes	Yes	Yes
Message integrity	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes
User authentication	Yes	Yes	Yes
Web based solutions	Yes	Yes	Custom
Support Windows-based application (IIS5, IE)	Yes	Yes	Yes
Support Microsoft Word format	Yes	Planned	Custom
Provide online signing and verification	Yes	Yes	Yes
No lock with signal CA provider	Yes	Yes	Yes
Friendly Management interface Audit trials Data storage solution for digital signed documents	Yes (1) transaction receipt (2) file management system	Yes	No demo for evaluation
Vendor provides standard API or library	Yes	Yes	Yes
No special hardware and software requirements	Yes	Yes	Yes
The cost for physician should be minimum	No cost for physician, except the cost of certificate	No cost for physician, except the cost of certificate	No cost for physician, except the cost of certificate
The implementation cost should be reasonable based on the fair market price	N/A	N/A	N/A

Table 4. Solution Comparison

The study also compared different CA solutions based on the requirements and proposed three CA providers who are capable of satisfying all the requirements. The implementation strategy proposed was outsourcing the CA to a third-party CA provider so that the company can focus on the application side of the implementation. The company identified as a critical requirement that the application fits the physician office workflow as already defined. Pilot tests can help to reveal any issues related to the CA. Once the digital signature application is adopted, it will be easier for the company to identify any issues regarding the CA. After this experience, the company may decide to operate as their own CA. The size and geographic dispersion of the physician provider network will challenge the CA implementation. The number of CAs, how they will be placed, and what performance bottlenecks can appear are questions that should be addressed.

CONCLUSION

Based on analysis conducted during stage one through six of the security framework, recommendations for the company were generated. First, the company must meet client requirements by following current standards and by analyzing the enterprise architecture of the client organizations. Within this context, the most important decision is the selection of a Certificate Authority (CA). Our analysis indicated that selecting a third party CA would be more appropriate for the company, since their technical team has no experience in digital signatures, or PKI implementation, and it is therefore not a core competency of the company to provide a CA solution in-house. However, as the company's experience develops, it may reassess the idea

of deploying an in-house CA solution should it become a client requirement. Secondly, while selecting an application vendor, the company must find a vendor that can easily integrate a solution within the company's information systems and workflow processes. We evaluated several vendors and recommended one to take into a pilot-testing phase. A formal pilot test was the third of our major recommendations. We proposed a multi-step pilot-testing phase. First, we proposed an initial lab-based test in which potential software solutions can be evaluated prior to testing with actual users. If the lab test succeeds, then 10 physicians are to be selected from the physician provider network. These physicians will be equipped with certificates and instructed in system use. While the lab testing is underway, the company's technical team will be working to integrate the selected software solution with their existing software and workflow. When this effort is completed, the pilot phase users will be brought online. We then propose to evaluate the user response, using methodology to be described in a follow-up study to the present one, and including examinations of migration strategies, physician acceptance, system adoption, and inter-organizational impact. The final two stages of the security framework, implementation and evaluation, have not yet been addressed in the course of this project. It is expected that the pilot-testing phase will commence as recommended, and the results of these two security framework steps will be reported in the future.

Future studies could draw on this case to address the inability of the healthcare industry to use a common digital signature solution. The research presented here expands the knowledgebase regarding implementation of PKI based digital signature solutions. Follow on studies should expand the knowledgebase of user acceptance of digital signatures in the medical field by examining online systems and public/private key management challenges.

REFERENCES

1. Anderson, R. (2001) *Security Engineering: A guide to building dependable distributed systems,* Wiley Computer Publishing, New York, NY.
2. Department of Veterans Affairs (2003) Public Key Infrastructure Project, *Department of Veterans Affairs*, (Accessed 2004: February, 21), http://www.va.gov/proj/vapki/default.htm.
3. Garfinkel, S. (2002) *Web Security, Privacy and Commerce,* O'Reilly & Associates, Sebastopol, CA, USA.
4. Hanna, S. (2003) Obstacles to PKI Deployment and Usage - Survey Results and Draft Action Plan, *Proceedings of Proceedings of Fifty-Eighth Internet Engineering Task Force*, Minneapolis, MN, USA.
5. Horan, T. A., Tulu, B., Hilton, B. and Burton, J. (2004) Use of Online Systems in Clinical Medical Assessments: An Analysis of Physician Acceptance of Online Disability Evaluation Systems, *Proceedings of 37th Hawaii International Conference on System Sciences*, Hawaii.
6. Kleinsteiber, J. (2002) Storage Networking Industry Association Technology Center, http://www.snia.org/apps/group_public/download.php/1634/Authenicated_Infrastructures.pdf.
7. PEC Solutions (2000) (Ed, Administration, U. S. D. o. J. D. E.) http://www.deadiversion.usdoj.gov/ecomm/csos/cert_req/section2/2_2.htm.
8. Policy and Communications Staff (2000) National Archives and Records Administration, Washington, DC.
9. Polk, W. T. and Hastings, N. E. (2000) National Institute of Standards and Technology, Gaithersburg, MD, pp. http://csrc.nist.gov/pki/documents/B2B-article.pdf.
10. Schneier, B. (1996) *Applied Cryptography,* John Wiley & Sons.
11. The Apache Software Foundation (2003) Authentication, Authorization, and Access Control, *http://httpd.apache.org/docs/howto/auth.html*, (Accessed December),
12. Tulu, B. and Chatterjee, S. (2003) A New Security Framework for HIPAA-Compliant Health Information Systems, *Proceedings of Ninth Americas Conference on Information Systems*, Tampa, FL.