

---

## Implementing digital signatures for healthcare enterprises: the case of online disability evaluation reports

---

Bengisu Tulu\*, Haiqing Li, Samir Chatterjee,  
Brian Hilton and Thomas Horan

School of Information Science, Claremont Graduate University,  
130 East Ninth Street, Claremont, CA 91711, USA

E-mail: bengisu.tulu@cgu.edu E-mail: haiqing.li@cgu.edu

E-mail: samir.chatterjee@cgu.edu E-mail: brian.hilton@cgu.edu

E-mail: tom.horan@cgu.edu

\*Corresponding author

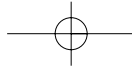
**Abstract:** This paper presents a conceptual security framework and a case study of a digital signature solution implementation for a healthcare organisation that provides disability evaluation services for various government agencies and private companies. One service the company provides for its 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 investigated a digital signature solution. A security framework previously proposed was utilised to guide the implementation of the digital signature solution. This security framework consists of eight sequential stages. An in-depth analysis of the first seven stages for this case is provided, including guidelines for choosing digital signature solutions, vendor analyses and implementation issues.

**Keywords:** case study; digital signatures; healthcare; public key infrastructure; security framework.

**Reference** to this paper should be made as follows: Tulu, B., Li, H., Chatterjee, S., Hilton, B. and Horan, T. (2005) 'Implementing digital signatures for healthcare enterprises: the case of online disability evaluation reports', *Int. J. Healthcare Technology Management*, Vol. 6, Nos. 4/5/6, pp.470–488.

**Biographical notes:** Bengisu Tulu is currently a Doctoral Student in management information systems at the School of Information Science at Claremont Graduate University, where she also presently works as a Research Associate in the Network Convergence Laboratory. Her research interests include voice/video over IP, security and medical informatics. She is currently working on quality of information required for telemedicine applications and digital signatures in the healthcare domain. Ms Tulu received her Masters degree in management information systems from Claremont Graduate University. Earlier she received a Masters degree in information systems and a Bachelors degree in mathematics from Middle East Technical University, Turkey.

Haiqing Li is a Doctoral Student in the School of Information Science at Claremont Graduate University and over the last three years has worked as a Research Assistant in Network Convergence Lab, CGU. He is also a Lecturer



at the University of La Verne. In addition to digital signature, his research interests include network convergence, VoIP security, network simulation and geographic information system.

Samir Chatterjee is an Associate Professor in the School of Information Science and Director of the Network Convergence Laboratory at Claremont Graduate University. Prior to that, he taught at the Robinson College of Business, Georgia State University, in Atlanta. He holds a PhD from the School of Computer Science, University of Central Florida. His research interests are in voice/video over IP, cyber-security, *ad hoc* collaboration and bioinformatics. He is a member of ACM, IEEE, and IEEE Communications Society. He has published over 50 articles in respected scholarly journals such as *Communication of the ACM*, *Computer Networks & ISDN Systems*, *Computer Communications*, *Communications of the AIS*, *Information System Frontiers*, *ACM Computer Communication Review*. He is principal investigator on several NSF grants.

Brian N. Hilton, PhD, is a Research Fellow at the Claremont Information and Technology Institute, School of Information Science, Claremont Graduate University. His research interests include geographic information systems, spatial decision support systems, open source software, and information system development. He received a PhD and a MS in management information systems from Claremont Graduate University and a BA in economics from the Richard Stockton College of New Jersey.

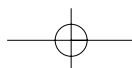
Thomas A. Horan, PhD, is Associate Professor in the School of Information Science and Director of the Claremont Information and Technology Institute (CITI) at the Claremont Graduate University (CGU). Dr. Horan's research addresses the planning and assessment of information technology systems, focusing on three substantive areas: healthcare informatics, community informatics and digital infrastructures. This research has been reported in a wide variety of journals, including the *Information Systems Frontiers*; *Communications of the ACM*; *Knowledge, Technology and Policy* and *Journal of Urban Technology*. His most recent book, *Digital Infrastructures* (edited with Rae Zimmerman) was published by Routledge Press (2004). Dr Horan has both his Master's and Doctorate degrees from CGU.

---

## 1 Introduction

Escalating healthcare costs and increasing demand for healthcare services, as a result of an aging population, instigated a search for innovative solutions that can improve quality of health services while reducing cost. As stated in a report addressed to the President of the USA (President's Information Technology Advisory Committee, 2004), the paper-based medical record is one of the most fundamental and pervasive problems of healthcare delivery. Hence, recommendations presented in this report focused on four core elements to revolutionise medical record systems:

- electronic medical records
- computer assisted clinical decision support systems
- computerised provider order entry
- secure, private, interoperable, electronic health information exchange.



472 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan*

Medical reports are one of the core components of the medical system. Difficulty in storing these paper-based reports, as well as the demand from patients for a more flexible report sharing between integrated institutions, is pushing healthcare organisations to develop electronic medical records. On the other hand, security and privacy rules and regulations are forcing organisations to take slow and secure steps in making this transition from paper-based to electronic record keeping. One of the major concerns in sharing electronic medical reports is authenticating the parties involved in generating these reports. At this point, a specific need arises for an authentication mechanism that can replace traditional handwritten signatures used in paper-based medical reports. The ultimate goal is to enable a smooth flow in record sharing between medical organisations in order to minimise cost and improve quality of service.

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 achieve basic security building blocks, such as identification, authentication, integrity and non-repudiation. This study presents a case study regarding the implementation of digital signatures to sign electronic medical reports for disability evaluations. In the disability evaluation industry, the need for independent evaluations introduces a significant organisational complexity as claimant reports travel from one organisation to another including government agencies, private organisations, physician clinics and hospitals.

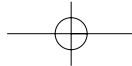
The company in the case study presented here meets this challenge by using technology to develop a seamless online record. They provide electronic medical services to healthcare practitioners for filing disability evaluation reports and transmitting them to clients. The company was seeking a digital signature solution that would meet legal and client requirements and would streamline the current signature process. Regardless of the method used to generate a legally binding disability report, the signature of the examining physician is required. The current signature process utilises the manual collection of signatures. A security framework previously proposed (Tulu and Chatterjee, 2003) was utilised 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 signatures overall. It continues with an analysis of the digital signature implementation by utilising the aforementioned security framework. Each step is explained in detail within the context of this case study. The paper concludes with a discussion and areas for future research. A glossary of commonly used terms is included as an appendix.

## **2 Background**

### *2.1 Company background*

The company provides an array of disability evaluation, 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 have conducted and produced over two million disability exams and rateable reports. They operate 26 medical evaluation facilities, and their nationwide provider network consists of 10,000 fully credentialed physicians and auxiliary providers.

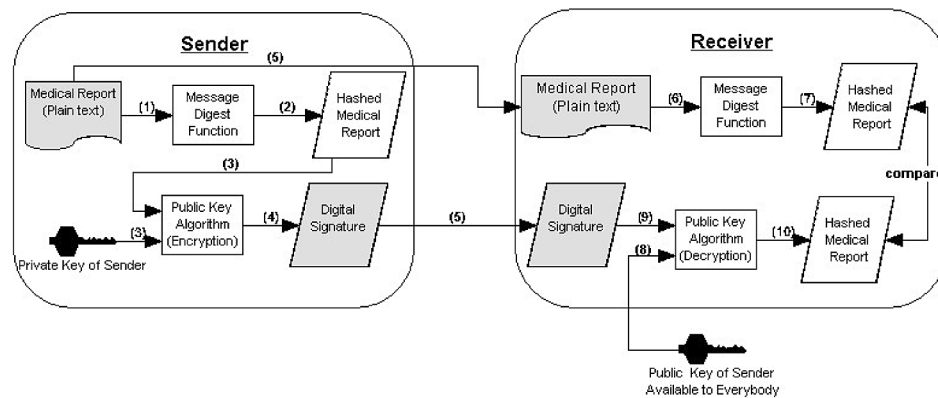
Providing timely and accurate medical disability evaluation information to clients is an industry challenge. The lack of disability evaluation standards and a common terminology between various agencies also introduces a challenge for physicians (Tulu et al., 2004). Each disability programme has its 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 organisation to another may cause further confusion and result in a less accurate and/or poor quality assessment. The company aims to meet 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 medical 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 utilises 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 physician finalises and ‘locks’<sup>1</sup> 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.

## 2.2 *Digital signature technology*

Digital signatures enable people to sign digital documents by providing the properties of a handwritten signature. They must fulfil 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, digitised 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 utilise 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 (Kammer, 2000). 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.

**Figure 1** Digital signatures using PKI

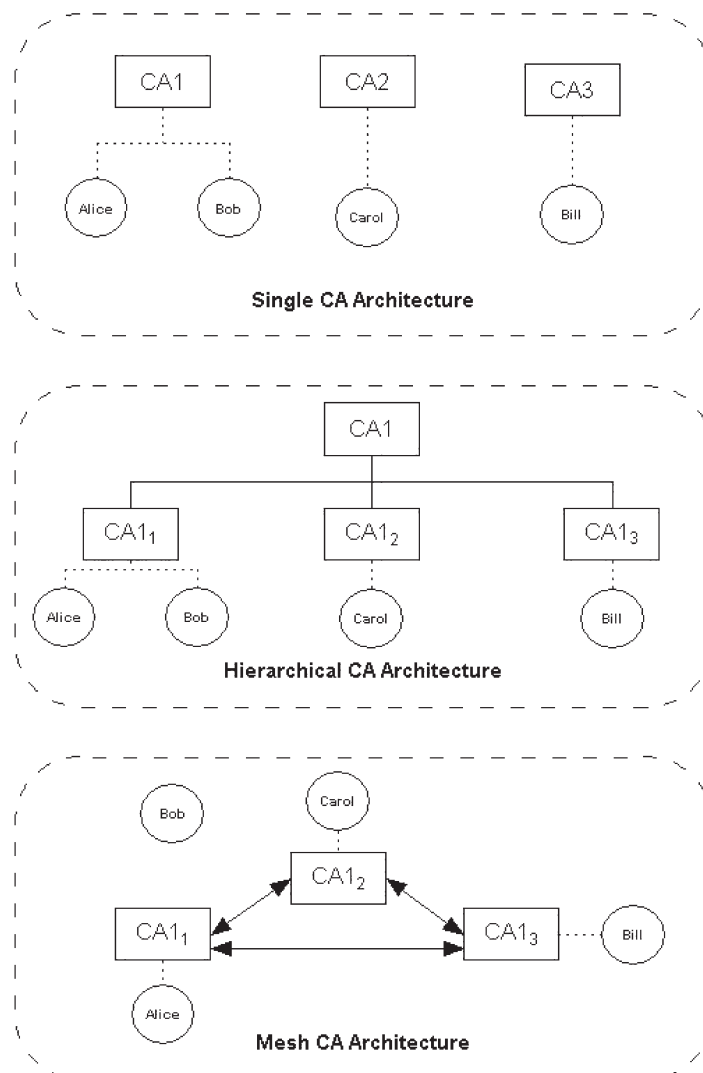
The following is an illustration of the digital signature scenario presented in Figure 1. Bob (sender) wants to send Alice (receiver) a text message with a digital signature. First, Bob creates the text message to be signed and generates a hashed message using a message digest function (e.g., MD5, SHA-1, etc.). A message digest function is a mathematical function that converts the original message to a unique, fixed length value, which is called 'hash'. For example, SHA-1 algorithm generates a 160 bits hash and MD5 Digest algorithm generates 128 bits 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).

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 (Polk et al., 2003): a single CA, a hierarchy of CAs, or a mesh of CAs. Each of the configurations, illustrated

in Figure 2, 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' (Polk and Hastings, 2000).

Figure 2 PKI architectures (modified from Polk et al., 2003)



476 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan*

PKI implementation can use any of the architectures illustrated in Figure 2. This introduces a challenge for integrating the existing PKI implementations with various architectures under a single umbrella. The Bridge Certification Authority (BCA) architecture was designed to address the shortcomings of the basic PKI architectures, and to link PKIs that implement different architectures (Polk and Hastings, 2000). Unlike a mesh PKI CA, the BCA does not issue certificates directly to users. In addition, the BCA is not intended for use as a trust point by the users of the PKI, unlike the 'root' CA in a hierarchy. With an effort to connect existing federal agency PKIs, the Federal PKI Steering Committee established the Federal Bridge Certificate Authority (FBCA) in support of a broader, government-wide PKI network (USA General Accounting Office, 2003). Currently there are four agencies that are participating in the FBCA and additional organisations are planning to participate in the future. FBCA was designed to be able to accommodate not only federal CAs but also CAs of nonfederal, state and local government agencies as well as private sector.

### 3 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 the follow-up study was that 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:

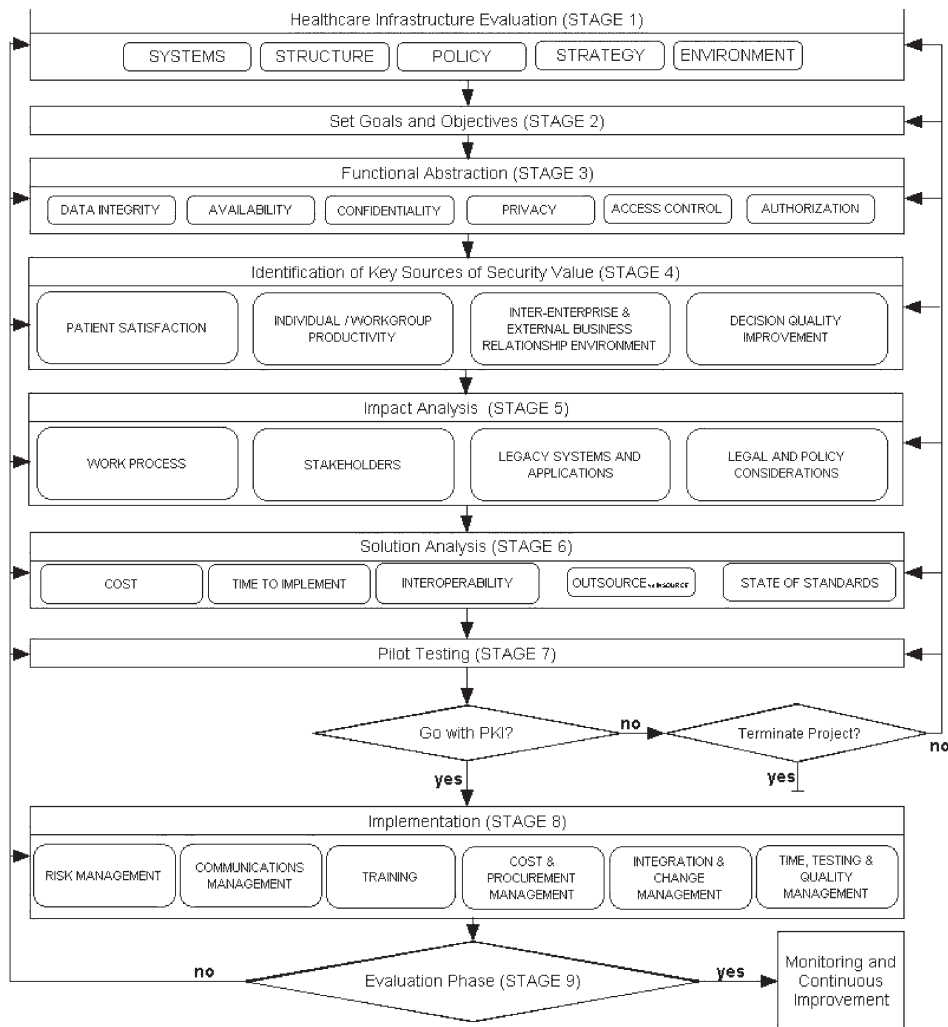
- software applications do not support PKI
- the cost is too high.

Respondents of this study also agreed that the one critical application that needs improvements in PKI support is 'document signing'. Document signing is 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 slightly modified version of the security framework (Tulu and Chatterjee, 2003), which was proposed to help management decide how to make their organisation compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), was utilised to investigate the possible PKI implementation at this company. The framework, illustrated in Figure 3, consists of nine sequential stages and allows implementers to revert to a previous stage any time during the implementation. The modification of the framework was necessary since the original version was designed to manage a transition that is required for the organisation where, as in this case study, the transition is not mandatory. Step 7 was added to the original framework since the solutions evaluated need to be pilot tested before reaching a decision. Also a decision point was added to terminate the project since this implementation is not a mandatory requirement for an organisation like the HIPAA. The following subsections describe each step within the context of this specific case study.

*Implementing digital signatures for healthcare enterprises*

**Figure 3** Security management framework (adapted from (Tulu and Chatterjee, 2003))



**3.1 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 presents a brief summary of the company’s information systems, organisational structure, security and related policy, and information technology (IT) strategy.

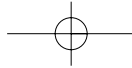
478 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan*

**Table 1** Infrastructure diagnosis

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 Organisational Structure: the company has contracts with various federal agencies, state agencies, and private companies. Based on these contracts, the company is responsible for 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	Organisational Security Policy: The company's security policy is strictly controlled by various rules and regulations and is enforced by governmental healthcare organisations. The company is under pressure to meet the specific security requirements of its clients. To deal with these various governmental agencies and private organisations, 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 3.
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 behaviour of their clients in order to implement a technology that will be compatible with future implementations.

### 3.2 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.



### 3.3 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 summarised in Table 2 and include authentication, authorisation, access control, integrity, confidentiality, privacy and availability. The table also 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).

**Table 2** Functional abstraction

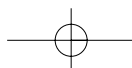
	<i>Authentication</i>	<i>Authorisation</i>	<i>Access control</i>	<i>Integrity</i>	<i>Confidentiality</i>	<i>Privacy</i>	<i>Availability</i>
Importance	High	High	High	High	Medium	Medium	Medium

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authorisation 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).

The company rated the importance level for authentication, authorisation, access control and integrity as high. The rationale for this is that the company must ensure that authorisation and access control levels are set high enough to prevent any unauthorised and/or unwanted access to their system. Furthermore, the company would prefer that clients authenticate and verify the integrity of the information contained in completed disability reports on their own (i.e., without assistance from the company). This preference is met through the high importance level.

### 3.4 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 completed a 'claim' form and submitted it to his or her healthcare provider (client) for reimbursement. By utilising a digital signature solution for electronic reporting, the company can provide a faster service to its clients directly affecting the response time needed to process a claim. Utilising a PKI-based solution would enable the company to encrypt all documents in a secure manner ensuring the privacy of claimant information.



480 B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan

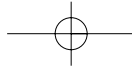
Another key source of security 'value' is related to productivity. For example, eliminating the manual print-and-fax submission process and replacing it with a 'single-click' submission process can only increase physician productivity. For the company, the manual scanning of signatures will no longer be required. It is expected that 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 should also enhance the decision-making process for both clients and the company where the accuracy of a medical report is of concern. Finally, future business relationships between the company and its clients (mostly government agencies) should strengthen as they align their business processes with newly emerging government PKI initiatives.

### 3.5 Stage 5: impact analysis

Preliminary analysis indicates that the proposed solution will 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 digital signature tool. A related study by the authors (Horan et al., 2004) found that work practice compatibility was very important in determining a physician's behavioural intent to accept and use a new system. Consequently, it is important to ensure that any new system does 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 and would engage their assistants in the process of signature collection. Similarly then, it would be important to reassure clients (i.e. public or private payers) that the digital signature process would be consistent with their processes for handling disability evaluations.

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, could significantly impact the two applications used for online report submission and generation. The integration of these two applications with the PKI may require significant programming changes and additional hardware. Legislative initiatives surrounding digital signatures began in Utah in 1996 when the first digital signature law was enacted. 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 similar laws, two models – the Utah Model and the Massachusetts Model – emerged as templates for other states. The Utah model 'envisioned a public key infrastructure supported by state-licensed certification authorities' (Garfinkel, *ibid.*) 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 individual state legislative activities were on the increase, the federal government tried to end the debate when it passed the Uniform Electronic Transactions Act (UETA) in 1999, which does not enforce PKI. In 2000, President Clinton signed the Electronic Signatures in Global and National Commerce Act (E-SIGN), which added federal consumer protection elements absent from the 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 organisation 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 organisations, 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 into 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. While doing so, it is important to consider FBCA requirements since the clients are, or eventually will be, a member of FBCA. A vendor must be selected that optimises the cited factors. It should be noted that the cost factor is closely tied to the 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.

### *3.6 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. These include legal compliances, client requirements, industry requirements and end-user requirements.

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 analysed 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.

482 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan***Table 3** Requirement analysis

<i>Meta requirements</i>	<i>Implementation requirements</i>	<i>Evaluation criteria</i>
Legal compliance – this solution should be able to provide legal binding signatures	E-SIGN/UTEA/21 CFR 11 State laws	Match the requirements of E-SIGN and/or UTEA 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 Integrated with current reporting system	Web based solutions Support Microsoft Windows Operating system, and Internet Information Server5 Support Microsoft Word Documentation format Provide online signing and verification
	CA solution	No lock with single CA provider
	Manageability	Provide management interface; audit trails; data storage solution for digitally signed documents.
	Customisable	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 4** Solution comparison

<i>Evaluation criteria</i>	<i>Provider 1</i>	<i>Provider 2</i>	<i>Provider 3</i>
Match the requirements of E-SIGN and/or UTEA	Yes	Yes	Yes
Success case that work with government agents			
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	Yes	Yes	No demo for evaluation
Audit trials Data storage solution for digital signed documents	(1) transaction receipt (2) file management system		
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

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

484 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan*

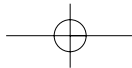
own CA. The size and geographic dispersion of the physician provider network will challenge the CA implementation. The number of CAs, how they will be placed and what performance bottlenecks can appear, are questions that should be addressed.

### *3.7 Stage 7: pilot testing*

This is the final step before making a decision regarding the project. At this stage a comprehensive pilot test for the selected vendor(s)/product(s) should be conducted. Based on analysis conducted during stage one to six of the security framework, recommendations for the company were generated. First, the company must meet client requirements by following current standards and by analysing the enterprise architecture of the client organisations. Within this context, the most important decision is the selection of a Certificate Authority (CA). As noted above, stage 5 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.

Second, 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. Several vendors were evaluated in stage 6 and one was recommended to take into a pilot-testing phase. A multi-step pilot test was conducted. First, an initial lab-based test was completed in which potential software solutions were evaluated prior to testing with actual users. Once this testing was completed and the solution shown to meet the company's requirements, the product was implemented in the real-world environment where it was tested by a technical team for integration and compatibility purposes. The technical test was a major step since a failure in integration can damage the large-scale implementation. Various modification iterations took place during this phase between the vendor and the company to slightly customise the product for the requirements and needs of this specific environment. For the last step of the pilot test, a sample of physicians will be selected from the physician provider network. These physicians will be equipped with certificates, instructed in system use, and will be brought online. The user response, for physician acceptance, system adoption, and inter-organisational impact will be collected to select migration strategies and to predict the success of the large-scale implementation. A concurrent institutional assessment will be conducted based on the willingness of the collaborating organisations (i.e. sponsoring agencies) to accept the digital signature process in their process.

While beyond the scope of this paper, it is important to note that the final two stages (stage 8 and 9) of the security framework address the implementation and evaluation phases for the project once a full-scale implementation is in place. It is expected that this latter evaluation will draw upon the previous results of the impact analysis with recommendations focusing on continuous implementation success rather than the pilot implementation.



#### 4 Conclusion

This study focused on the decision-making process for implementing a digital signature solution. While digital signatures may be successfully implemented in this case study, this is not to suggest that widespread implementation in the medical arena can be expected in the near term. Even within the (relatively) simple process of this case, several technical, managerial and institutional constraints became apparent. On the technical level, lack of a widespread format for the acceptance of provider-solutions can cause uncertainty in the industry. On the managerial and institutional level (and still related to the technical issues), it is difficult for a company or agency to justify resources for digital signature implementation in the absence of a strong industry-wide drive for adopting this new technology.

In short, while the management framework outlined here can provide a roadmap for managers who would like to implement or evaluate digital signatures for their organisations, it does not replace the complex management judgments that need to be made during the course of this evaluation regarding the nature and timing of digital signature implementation. This study presented one implementation of a framework that can aid digital signature implementations in healthcare organisations. Even though this aid cannot replace solid management decisions, it helps organisations to outline the project layout and gives them a structured plan to follow, hence preventing them from overlooking some important issues for the project.

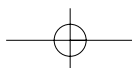
The basic promise of digital signatures is that through implementing such an electronic innovation, there will be enhanced efficiencies in the medical assessment process. As stated at the outset of this article, the disability evaluation process is subject to numerous inefficiencies. By eliminating these inefficiencies, the hope and plan is to aid physicians in focusing on the medical value of their services, not the paperwork associated with it.

#### Acknowledgements

This study was conducted pursuant to a cooperative research agreement between Claremont Information and Technology Institute (CITI) at Claremont Graduate University and the QTC Management. The authors gratefully acknowledge the support of QTC Management. The results reported as well as any inadvertent errors in their reporting are the sole responsibility of the paper authors.

#### References

- Anderson, R. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York, NY: John Wiley & Sons. Inc.
- Department of Veterans Affairs (2003) *Public Key Infrastructure Project*, Retrieved February, 21, 2004, from <http://www.va.gov/proj/vapki/default.htm>.
- Garfinkel, S. (2002) *Web Security, Privacy and Commerce*, (Second ed.) Sebastopol, CA, USA: O'Reilly & Associates.
- Hanna, S. (2003) 'Obstacles to PKI deployment and usage – survey results and draft action plan', *Proceedings of Fifty-Eighth Internet Engineering Task Force*, Minneapolis, MN, USA, Corporation for National Research Initiatives.

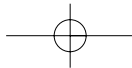


486 B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan

- 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', *37th Hawaii International Conference on System Sciences*, Hawaii.
- Kammer, R.G. (2000) 'Digital signature standard' (No. FIPS PUB 186-2), *Federal Information Processing Standards Publication*, US Department of Commerce/National Institute of Standards and Technology.
- Kleinsteiber, J. (2002) *Authenticated Infrastructures – What They Can and Cannot Provide*. Retrieved December 20, 2004, from: [http://www.snia.org/apps/group\\_public/download.php/1634/Authenticated\\_Infrastructures.pdf](http://www.snia.org/apps/group_public/download.php/1634/Authenticated_Infrastructures.pdf), Storage Networking Industry Association Technology Center.
- PEC Solutions (2000) *Public Key Infrastructure Analysis. PKI Certificate Policy Requirements Analysis*. Available from: [http://www.deadiversion.usdoj.gov/ecommm/csos/cert\\_req/section2/2\\_2.htm](http://www.deadiversion.usdoj.gov/ecommm/csos/cert_req/section2/2_2.htm), United States Department of Justice Drug Enforcement Administration.
- Policy and Communications Staff (2000) *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, Washington, DC: National Archives and Records Administration.
- Polk, W.T. and Hastings, N.E. (2000) *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, Gaithersburg, MD: National Institute of Standards and Technology. Available from: <http://csrc.nist.gov/pki/documents/B2B-article.pdf>.
- Polk, W.T., Hastings, N.E. and Malpani, A. (2003) 'Public key infrastructures that satisfy security goals', *IEEE Internet Computing*, Vol. 7, No. 4, pp.60–67.
- President's Information Technology Advisory Committee (2004) *Revolutionizing Healthcare Through Information Technology*, Arlington, VA: National Coordination Office of Information Technology Research and Development.
- Schneier, B. (1996) *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Second Ed.), New York, NY: John Wiley & Sons.
- The Apache Software Foundation (2003) *Authentication, Authorization, and Access Control*. Available from: <http://httpd.apache.org/docs/howto/auth.html>.
- Tulu, B. and Chatterjee, S. (2003) *A New Security Framework for HIPAA-Compliant Health Information Systems*, Tampa, FL: Ninth Americas Conference on Information Systems.
- Tulu, B., Hilton, B. and Horan, T.A. (2005) 'Improving disability evaluation productivity: linking innovative business models with information technology', *Int. J. Healthcare Technology Management*, in press.
- United States General Accounting Office (2003) *Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies*, (No. GAO-04-157). Washington, D.C.

## Notes

- <sup>1</sup> Locking in this instance means that the medical report is finalized and cannot be changed by anyone.
- <sup>2</sup> <http://www.ftc.gov/os/2001/06/esign7.htm#Executive%20Summary>.
- <sup>3</sup> <http://www.ietf.org/rfc/rfc1321.txt>.
- <sup>4</sup> <http://www.rsasecurity.com/rsalabs/node.asp?id=2308>.
- <sup>5</sup> <http://www.ietf.org/rfc/rfc2315.txt>.
- <sup>6</sup> <http://www.ncsl.org/programs/lis/cip/ueta.htm>.

**Appendix: Glossary of terms**

**Authentication:** Process of determining whether someone or something is, in fact, who or what it is declared to be.

**Authorization:** Process of deciding whether someone is allowed to have access to a service or a resource.

**Certificate Authority (CA):** 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.

**Certificate Policy (CP):** A named set of rules that describes terms under which digital certificates are issued to subscribers, managed and revoked, and the requirements under which the CA must operate in order to maintain the trustworthiness of its issued certificates.

**Confidentiality:** Process of protecting against the disclosure of information to parties other than the intended recipient(s).

**Digital signature:** Digital Signature is a digital file that is the result of a transformation of a message by means of a cryptographic system using keys so that a person who has the initial message can determine:

- whether the transformation was created using key that corresponds to the signer's key
- whether the message has been altered since the transformation was made.

**Digital Signature Standard (DSS):** DSS is USA Federal Government standard for digital signatures. It is created by the NIST, and specifies Digital Signature Algorithm (DSA) as the algorithm for digital signatures and SHA-1 for hashing.

**Electronic Signatures in Global and National Commerce Act (E-SIGN):** E-SIGN<sup>2</sup> is enacted by US congress on June 30, 2000 to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

**Federal Bridge Certification Authority (FBCA):** A federal bridge CA to create trust paths among individual agency PKIs. It develops cross-certificates to bridge the gap among dissimilar products and architectures that are used by different agency PKIs.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA):** HIPAA specifies the standards for the security of electronic protected health information.

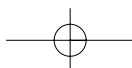
**Integrity:** Process of preventing, deterring and detecting improper modification of the information during or after transit.

**Key:** A sequence of symbols that controls digital signature and encryption processes.

**Message:** The delimited information to be signed.

**Message-Digest Algorithm 5(MD5):** An algorithm, defined in RFC1321,<sup>3</sup> which takes as input a message of arbitrary length and produces as output a 128-bit message digest of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest (Schneier, 1996).

**One-way hash function:** A mathematical function that creates in effect a digital fingerprint of the message, a code usually much smaller than the message but nevertheless unique to it.



488 *B. Tulu, H. Li, S. Chatterjee, B. Hilton and T. Horan*

**Public Key Certificate:** A digital file that contains the public key of a subscriber together with related information, digitally signed with the private key of the Certification Authority that issued it.

**Public Key Cryptography Standard (PKCS):** A set of standards produced by RSA Laboratories in cooperation with an informal consortium for the algorithms of Public-Key Cryptography. PKCS includes both algorithm-specific and algorithm-independent implementation standards.<sup>4</sup>

**PKCS #7:** The standard of the digital signature file defined in RFC 2315.<sup>5</sup> It defines a general syntax for messages that include cryptographic enhancements such as digital signatures and encryption.

**Public Key Infrastructure (PKI):** A cross-governmental, ubiquitous, interoperable infrastructure for implementing e-signature, which is a statutory mandate for e-government. It also means the development and use of applications that employ the PKI in support of agency business process.

**Secure Hashing Algorithm FIPS-180-1 (SHA-1):** An algorithm that operates on any input length less than 264 bits to produce a 160 bit output, a message digest (Schneier, 1996).

**Uniform Electronic Transactions Act (UETA):** A legal framework for electronic transactions. It gives electronic signatures and records the same validity and enforceability as manual signatures and paper-based transactions. The National Conference of Commissioners on Uniform State Laws (NCCUSL) adopted this model act in 1999<sup>6</sup>.

**X.509:** The International Telecommunications Union (ITU) standard that specifies the content and the syntax of the certificate.