PKI NOTE

March 2001

US Healthcare

This Note examines the critical need to create a secure IT infrastructure for healthcare that would increase efficiency of service without compromising patient privacy. It also identifies the challenges that exist, such as interoperability and government legislation, on the path to accomplishing such a monumental and necessary goal.

Overview

More than most sectors, the US healthcare industry is labeled as being desperately in need of the efficiencies provided by ubiquitous networking. A study compiled by McKinsey states that if medical organizations spent $50 billion each year on information technology, they would save $270 billion each year. This massive savings is related to the fact that the healthcare industry has had a lower percentage of expenditure for information technology as compared to other industries. This provides an opportunity to increase efficiency and to reduce risks by investing in a strong information technology infrastructure.

However, hot-button issues like privacy and confidentiality of personal medical data have taken center stage in recent years, leading to government regulation initiatives of such great scope that realizing the e-healthcare future has become a project many see as a significantly greater challenge than preparations for Y2K.

With the passage of Public Law 104-191 (Health Insurance Portability and Accountability Act of 1996), and requirements for electronic clinical information systems and services, the protection of patient records has become increasingly complex and more critical. Although identification, authentication, authorization, and integrity services have traditionally been provided on an application-by-application basis, the requirements of today's health care and business world make "point" solutions impractical and ineffective.

A comprehensive security system for distributed networks needs to provide integrated, extensible, and flexible services, based on public interfaces. One effective way to provide this is through infrastructure components, shared among applications.

PKI, or Public Key Infrastructure, services are the solution of choice for shared encryption/decryption, digital signature, and authentication services. These services can be used in a variety of settings, including web-enabled patient and clinical information services, Virtual Private Networks for e-business, and secure E-mail.

PKI is a standards-based, flexible and extensible set of services. One of the downsides of flexible standards is that the choice of options implemented may have a significant impact on interoperability. Unless everyone agrees on which options are to be supported, and how those options are implemented, interoperability is not assured.

Acknowledgements

"US Healthcare PKI Note" is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Editor:

Ray Wagner
Phyve

Contributors:

Dave Barnette
Kaiser Permanente

Colin Frahm
Phyve

Laura Robinson
Xcert

Steve Mathews
Conclusive Logic

Reviewers:

Yuriy Dzambasow
Digital Signature Trust Co.

Victor Pollak
Digital Signature Trust Co.

Su Thomas
Chrysalis-ITS

Lisa J. Pretty
PKI Forum

Derek Brink
RSA Security

Richard Booth
Phyve

Harold Bandy
Phyve

Russell Goldberg
Phyve

PKI forum

Although there is some utility in a PKI that is only used internally (i.e., within an organization), the benefits are significantly greater when PKI is used to support secure and trusted electronic communications with partners, affiliates, and patients. Healthcare is an integrated industry that requires secure and trusted electronic communication between many business partners. According to the California Medical Association, physicians typically do business with 50 to 100 different healthcare organizations on a regular basis.

Although interoperability concerns are not restricted to healthcare, it is crucial that standardized options and agreements on interoperability be developed for use within the healthcare community of interest, which shares many common concerns. The more we can agree on how to implement PKI, the easier it will be to work together for the common benefit of patients and our organizations.

The US Healthcare Landscape

The US healthcare industry is comprised of a tangle of different sets of enterprises, all with different business goals and concerns. In general, this marketplace mimics the general marketplace of many regulated industries, except that within the healthcare industry, all participants, from partners to competitors, must cooperate in the provision of actual care. This creates a complex environment in which fostering of communication and development of standards become both vitally important and extremely difficult.

A comprehensive security system for distributed networks needs to provide integrated, extensible, and flexible services, based on public interfaces. One effective way to provide this is through infrastructure components, shared among applications.

In general, groups may be loosely divided into at least five categories:

- **Consumers** of healthcare services.
- **Providers**, which produce actual care services, and span a wide spectrum of definition, from large enterprises like hospitals, Integrated Delivery Networks and clinics to the local, unaffiliated general physician, who may take the role of an independent contractor or employee of larger provider enterprises. Health management organizations may fall into this category as well as that of payers. Provider organizations may be further divided into for-profit and non-profit subcategories.
- **Vendors**, which provide equipment and services necessary to carry on the work of both the providers and the payers, including medical equipment, infrastructure, information systems, etc.
- **Payers**, which provide the largest portion of revenues to providers and, more indirectly, vendors. Payers include insurance companies and the federal government.
- **Transaction processors**, which act as clearing houses, brokering the submission and transmission of care authorizations, insurance claims, informational transactions, and financial transactions among the larger market players.

Complicating the landscape within the healthcare industry are several factors, including:

- The aforementioned "coopetition"
- A historic stinginess with respect to investment in information technology infrastructures (healthcare enterprises historically spend approximately 1/3 of the percentage of revenues on information technology spent by all enterprises on average)
- A lack of expertise with regard to internet and security technologies within the industry
- The oversight of many state and federal authorities, which regulate the industry in all areas.

The following is a representative list of many of the important issues related to the Healthcare use of PKI.

Certificate Policies

Inter-organizational agreements can be time consuming and expensive. Certificate Policies and Certification Practice Statements are legal documents identifying limits of liability. Conflicts, misalignment, and differing interpretations of requirements can result in significant interoperability problems.

Because the Healthcare industry is extremely complex and interconnected, it would benefit most parties to work toward the development of a model CP and CPS for healthcare enterprises. The ASTM (http://www.astm.org) Healthcare Informatics working group (E31) has advanced a Model Certificate Policy for Healthcare PKI.

Because the Healthcare industry is extremely complex and interconnected, it would benefit most parties to work toward the development of a model Certificate Policies and Certification Practice Statements for healthcare enterprises.

Assurance of Identity

There is a lack of commonly understood and accepted terms describing various levels of assurance for certificate issuance. Each certificate binds an identity to a public key, and can be used to authenticate that individual. However, the proof of identity that is required in order to issue the certificate varies by certificate issuer. This can result in situations that may cause increased risk of harm to patients and increased liability.

As with the case of Certificate Policies, it would benefit most parties within the healthcare industry to develop, define, and publish a set of standard assurance levels for healthcare digital certificates. The IETF PKIX body has done general work in this area, defining Qualified Certificates (a certificate whose primary purpose is identifying a person with high level of assurance in public non-repudiation). These standards can be integrated into the Model Certificate Policy for Healthcare PKI mentioned above.

Profile Proliferation

There is a tendency to create specialized X.509 certificate profiles (sets of options), by application, by organization, and by community of interest. Each profile represents a significant amount of potentially duplicated effort. The end result, if unchecked, could be a need to issue and manage dozens of certificates for each end user. This substantially increases maintenance efforts, cost, complexity, and presents significant barriers to interoperability.

It seems obvious that simplicity dictates that the healthcare industry converge on the smallest number of profiles that will meet the industry's requirements. This can only occur through the work of standards bodies like IETF PKIX and ASTM E31.20, and the general acceptance of that work within the industry.

Simplicity dictates that the healthcare industry converge on the smallest number of profiles that will meet the industry's requirements. This can only occur through the work of standards bodies like IETF PKIX and ASTM E31.20, and the general acceptance of that work within the industry.

Trust Models

If PKIs are created within organizations, and then are allowed to grow and establish *ad hoc* trust relationships with other organizations, the inter-organization agreements (including Certificate Policy mapping) can rapidly become unmanageable.

Once again, the benefit of minimizing the complexity of the problem of inter-organizational trust is obvious, but in this case, it is unlikely that standards bodies will come to the rescue, as trust models for inter-organizational interoperability are firmly within the decision domain of the directors of the given organization. Large organizations can minimize the problem somewhat by creating a bridge CA within the organization to provide a controlled trust interface to all external CAs. Smaller organizations could benefit from the services of a third party Bridge CA service provider. External Bridge CAs, when extant, could help manage trust relationships among all participants by limiting the number of unique trust agreements required by an enterprise to do business within the industry.

Privilege Management

A Privilege Management Infrastructure (PMI) is a worthwhile approach for managing enterprise healthcare authorization services, particularly those that justify an infrastructure approach because of size or complexity. The endorsement of Attribute Certificates by the IETF indicates that PMI may become a significant component in electronic commerce applications. An Attribute Certificate framework could be closely integrated with PKI and Directory services, and could fit well with many current efforts. The use of the Authorization API (aznAPI) is also an attractive component of a PMI, and could be used in conjunction with Attribute Certificates, if supported by vendors. The aznAPI would also allow very complex authorization decisions to be made by a rules engine, and a simple yes/no result returned to applications.

Because the products are at early stages of development, and the standards have not stabilized, current attempts at implementation would be risky, and require care. The growing interest and body of knowledge in the industry indicates that this is an architectural direction worth pursuing. Many PKI vendors now offer some type of PMI, and several independent vendors focus primarily on this area.

It is clear that strong penetration of PKI technology within the healthcare industry will depend, at least in part, on the ability of PKI and healthcare information technology vendors to supply solutions which can operate, and interoperate, within this complex environment..

Long Term Storage

Long term storage (greater than 50 years) of medical records poses several problems, especially in light of any potential litigation. (1) It is difficult to prove that an electronic record has not been altered. (2) Media deteriorate over time, destroying information and invalidating digital signatures. (3) Storage media technology changes over time, which may render archives obsolete and unreadable. (4) Key lengths are generally determined by an estimated lifetime of "computational infeasibility" of ten to fifty years. This is not long enough for electronic medical records, or others which require long-term archival.

It will be left to industry participants to create a process and standard that allows for digitally signed records to be copied onto new media (and new technology) on a periodic basis (e.g., every 10 years). This issue is one that may be relatively unique to the healthcare industry, and may require some research by the vendor community in order to advance a credible long term solution.

Rights Delegation

An issue of particular importance within the healthcare industry is that of *rights delegation*, which refers to the ability of a participant to transfer, or delegate, some or all of his or her authorizations to another. For example, a vacationing doctor might need to delegate the right to access the medical records of his patients to another doctor within his practice. Many current medical practices may fall under the umbrella of rights delegation, including referral, consultation, test result review, etc.

Many PKI vendors now offer some type of Privilege Management Infrastructure, and several independent vendors focus primarily on this area.

This is likely the least resolved of all the issues presented here. Some within the industry see this as a non-issue: the problem is resolved by providing credentials to all participants (this in itself would be a problem for an enterprise, since participants may be from other institutions and external participants could outnumber internal ones manyfold) and instituting some type of administrative oversight to manage the situations described above. However, it remains to be seen whether this type of solution would be accepted by the industry as a whole. A rights delegation system could allow the primary physician to decide who should be able to access patient records. Needless to say, this also may cause problems, not the least of which would be from a liability standpoint for enterprises responsible for the confidentiality of patient medical data.

Certificate Validation

E-health applications deal with very sensitive data requiring maximum security; i.e. once confidential information is revealed it cannot be recovered. This, coupled with the fact that the U.S. Healthcare industry has high staff turnover and rapid changes in business relationships, generates the potential for misuse of non-valid certificates. There has been some concern raised from the healthcare industry that validating a certificate by using Certificate Revocation Lists can be problematic since the CRL may not be completely up to date. There are various ways of implementing status checking using CRLs as well as Online Certificate Status Protocol. One potential problem with OCSP is that, in an environment of many geographically dispersed CAs (as may be the case with healthcare), the speed of the on-line certification status checking will be affected by network latency.

Interoperability

Many of the issues mentioned above are related to interoperability issues within the PKI industry. Healthcare providers and health plans use many and varied types of IS, Internet and network technologies. It seems clear that PKI in healthcare will be a heterogeneous system based on multiple vendors, products, multiple PKIs, and numerous CAs, both within and external to the enterprise. It is clear that strong penetration of PKI technology within the healthcare industry will depend, at least in part, on the ability of PKI and healthcare information technology vendors to supply solutions which can operate, and interoperate, within this complex environment.

Regulatory Atmosphere

HIPAA

Governmental regulation of electronic information in healthcare is increasingly widespread and highly complex in issues and implementation. The Health Insurance Portability and Accountability Act (HIPAA) has garnered most of the interest and attention of healthcare enterprises, the health industry and mainstream media. Recently, the HIPAA standards for transactions and code sets were released. Other governmental organizations like HCFA, FDA and private organizations like JCAHO involved in the healthcare field are either mirroring these regulations or looking at instituting even more stringent requirements. There is no requirement for healthcare providers to use electronic communications, which are the subject of most regulatory initiatives. However, an organization that does not use electronic communications will be at a significant disadvantage in the marketplace, and will likely be merely delaying the inevitable, since most other participants in the healthcare industry will be moving toward electronic business and communications and encouraging their business partners to do so as well.

It is crucial that standardized options and agreements on interoperability be developed for use within the healthcare community of interest, which shares many common concerns. The more we can agree on how to implement PKI, the easier it will be to work together for the common benefit of patients and our organizations.

Digital Signatures

Effective October 1, 2000 the Electronic Signatures in Global and National Commerce Act went into effect. It was an extension of the standards of the Government Paperwork Elimination Act of 1997 that began to establish the definition of electronic signatures and their use in the federal government. The Electronic Signatures Act, called the E-Sign Act, establishes the framework for using electronic signatures to sign contracts, agreements, or records involved in commerce. It is to work within the commerce guidelines of the Security Exchange Act of 1934. This law does not cover all legal signatures. For example, it does not cover family law related to divorce, wills, and adoptions. In the medical field it does not cover the Uniform Anatomical Gift Act or the Uniform Health-Care Decisions Act. It can be used to purchase health insurance, but an insurance company cannot use it

to cancel health insurance. The bill does not specify the specific government technology standards; it allows parties to establish reasonable requirements regarding the use and types of electronic records and signatures. It is clear that the bill currently supports the use of PKI. This bill was passed overwhelmingly by the house and senate and was signed by President William J. Clinton using both a pen on paper and PKI technology on June 30, 2000.

Other Legislation

HIPAA and the Electronic Signatures Act are not the end of governmental regulation of electronic healthcare information. There is an increase in other federal and state regulations as well. In the 2000 legislative session, the US House and US Senate produced 17 bills that affect healthcare information technology and are of interest to the Joint Healthcare Information Technology Alliance (JHITA). These bills propose regulation beyond the HIPAA proposal. Ten of those bills are directly related to healthcare and six will have an impact on healthcare practices. There is some redundancy in these bills, but increased regulation is a central issue. One of these bills, H. R. 4049, has the goal of creating a 17-member, federally appointed, bipartisan Privacy Protection Commission to look at protection of personal privacy information, including medical information. If this bill passes, it is doubtful that the newly created commission will advocate for less stringent regulations. Two of the bills are designed to replace more restrictive state regulations with further national regulations. There are common goals among most of these bills, including increased management control of personal information, accountability of entities handling the information, and sanctions against those who do not protect privacy.

Global Legislative Trends

Government regulations' impact on healthcare information system providers is not just related to direct patient information. There are several bills pending related to the reporting of medical errors. There is an increase in other federal reporting requirements like the required reporting of deaths to local organ banks. The trend for more regulations is not unique to the United States. Canada Information Privacy Act went into effect January 1, 2001 and its healthcare provisions go into effect one year later. Great Britain has the Data Protection and Freedom of Information Acts. In Australia, the Privacy Amendment (Privacy sector) Bill 2000 was introduced for consideration. Additionally in Australia, the government has provided access to digital certificates to all health care providers who wish to file medical claims with the Government. More than 80% of the population of Australia uses government health services. Regulations are becoming more specific to actual security equipment levels. Security standards like the Common Criteria are being used to set international practices in the rating of computer security hardware and software solutions. The Common Criteria are also beginning to set standards for operational deployment of information services. ISO I7799 is being established to set best practices in the informational setting and proposed governmental regulations are looking to these standards to be used as a part of public policy.

An organization that does not use electronic communications will be at a significant disadvantage in the marketplace, and will likely be merely delaying the inevitable, since most other participants in the healthcare industry will be moving toward electronic business and communications and encouraging their business partners to do so as well."

Industry and Government Standards-Related

There are many industry initiatives within the US healthcare industry and the various governing bodies related to information security standards and practices. Because this sector is so complex and heavily regulated, with so many competing and interested parties, many initiatives overlap and may have different goals. A short discussion of some of the more important initiatives follows.

- The Workgroup for Electronic Data Interchange (http://www.wedi.org) focuses on improving healthcare through electronic commerce. WEDI has published best practices documents for healthcare security issues, most specifically related to general security policies and electronic data interchange.

- The American Society for Testing and Materials (ASTM, http://www.astm.org) Committee on Healthcare Informatics (E31) develops standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of healthcare information, including proposed standards for certificate profiles specific to healthcare and several standard guides for various healthcare information security issues.

- The American National Standards Institute Healthcare Informatics Standards Board (ANSI HISB, http://web.ansi.org/rooms/room_41/default.htm) has also done some work in this area.

- ISO Technical Committee 215 Work Group 4 (Healthcare Informatics Security, http://www.astm.org/COMMIT/ISO/ISOTC215/) defines standards for technical measures to protect and enhance the confidentiality, availability and integrity of health information and also accountability for users, as well as guidelines for security management in healthcare.

- The Internet Engineering Task Force (IETF, http://www.ietf.org) is concerned with the evolution of internet architecture, and has developed several security standards, including the X.509v3 standard for digital certificates and several other base technology standards for the PKI and information security industry. While not focused on healthcare per se, it would be difficult not to include the work of the IETF here.

- There has also been much interest within the Common Criteria community (http://www.commoncriteria.org) with regard to healthcare standards and practices, especially by the Forum for Privacy and Security in Healthcare (http://www.healthcaresecurity.org).

Other industry initiatives include:

- The 11.19 Working Group (http://www.11-19.org), an industry and vendor consortium that has the stated goal of creating security standards for Internet healthcare systems and transactions.

- The Health Privacy Project (http://www.healthprivacy.org) and the Online Privacy Alliance (http://www.privacyalliance.org) are most focused on consumer awareness of privacy and security issues.

- The Joint Healthcare Information Technology Alliance (JHITA, http://www.jhita.org) focuses on legislation advocacy and industry education.

- Several other industry standards groups, such as HL7, have recently begun to take a more active approach to information security in healthcare.

Initiatives toward industry certification authorities have also appeared. Notable models for distributing strong digital credentials to all or a portion of the participants in the US Healthcare marketplace have come from Medtegrity, MEDePass, and the Intel/AMA project. As yet, there has not been a strong initiative toward nor strong industry support for a US healthcare industry root CA similar to Identrus in the financial industry. A possible model that calls for one or several bridge CAs that bring together industry participants is gaining popularity.

There are common goals among most of these bills, including increased management control of personal information, accountability of entities handling the information, and sanctions against those who do not protect privacy.

Healthcare Issues in Europe

Europe has already implemented legislation very specifically controlling the privacy, collection and distribution of healthcare information. The European Data Protection Directive 95/46/EC sets requirements, standards and penalties for non-compliance that cover all those collecting health related information, not merely healthcare providers.

Europe has a rich and diverse structure for healthcare provision, ranging from the public health provision of the United Kingdom to the privately provided but publicly funded schemes of France. Such diversity has produced a wide difference in healthcare administration even though the delivery of healthcare services is largely common across all countries.

Nonetheless, Europe has engaged in many international standardization activities and Europeans are active in many of the US and ISO groups.

References

Public Key Infrastructure Concerns In Healthcare Settings, Dave Barnette, Kaiser Permanente, 3/3/2000

Current Activities of Selected Healthcare Informatics Standards Organizations (A Compilation), Agency for Healthcare Research and Quality, U. S. Department of Health and Human Services, June 2000

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to under-stand and exploit the value of PKI in their e-business applications.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810