

White Paper

Implementing a Public Key Infrastructure (PKI)

Table of Contents

Executive Summary	1
PKI In a Nutshell.....	3
What is a Public Key Infrastructure?.....	3
What is a Digital Signature?.....	3
Why Do We Need PKI?.....	5
Health Insurance Portability and Accountability Act (HIPAA).....	5
Government Paperwork Elimination Act (GPEA).....	5
Other Legislation.....	5
IHS PKI Pilot Project.....	7
Project Phases	7
Appendix A — What is Public Key Infrastructure (PKI)?	9
Encryption Defined.....	9
Enter PKI.....	9
The Digital Certificate and Certificate Authorities	10
Where are Certificates used?.....	11
How Does PKI Satisfy Those Business Environment Needs?.....	11
Apparent Conclusions.....	11
Certificates, Certificate Authorities, and Registration Authorities	12
Who and What Are the PKI Functional Entities?	12
Appendix B — For Additional Information Sources	15
Public Key Infrastructure (PKI)	15
Health Insurance Portability and Accountability Act (HIPAA).....	15
Government Paperwork Elimination Act (GPEA).....	15

Executive Summary

Driven by statutes, administrative policies, and the recognition that electronic transactions promise to provide far greater efficiencies and improve service delivery to the public and trading partners, Federal agencies are using the Internet for an increasing spectrum of applications. Doing so requires that agencies confront the issues of user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary, known as non-repudiation.

While there are many technologies which meet some of these requirements, only one provides the tools for meeting all of them: public key technology, implemented in the form of a Public Key Infrastructure (PKI). As we implement PKI suited to our needs, we have discovered that one of those needs is the ability to have electronic credentials (called digital certificates) which we issue to our employees or trading partners accepted by other agencies. This recognition has prompted extensive discussion of the mechanisms available for interoperation, and the development of one in particular, called the Federal Bridge Certification Authority, which promises to provide peer to peer interoperability that honors the autonomy agencies enjoy pursuant to statute and practice.

This report discusses the Indian Health Service's PKI activities to support digital certificate interoperability and to provide services aimed at promoting a single infrastructure for interactions with the public. The report documents the growing maturity of PKI products and increased understanding of just how flexible the technology is—a single infrastructure supplying a spectrum of interoperable services that can meet a variety of Indian health security needs.

What is a Public Key Infrastructure?

Public Key Infrastructure (PKI) is a technology that provides the following benefits:

- 1) **Strong authentication** — The use of digital certificates signed by a trusted authority provides convincing assurance of the user's identity.
- 2) **Message confidentiality and integrity** — Once encrypted, messages which are altered will not decrypt properly. Therefore, any message which properly decrypts is guaranteed to be unchanged.
- 3) **Non-repudiation** — Only a message encrypted with an entity's private key will decrypt with that entity's public key, and visa versa. Therefore, if a message is properly decrypted using an entity's public key, the message had to have been encrypted by that entity's private key.

A trusted Certificate Authority (CA) issues a signed digital certificate to an entity following verification of that entity's identification. The digital certificate contains the entity's public key. At the same time, a private key—which will be securely stored—is issued to the entity. The public and private keys are mathematically related such that:

- 1) A message encrypted with either key will be successfully decrypted by the other.
- 2) Neither key can be determined from the other.

What is a Digital Signature?

In a common form of digital signature associated with email, when the user wishes to sign a document digitally, he or she applies the private signing key to a hash of the document being signed which transforms the hash into a new, different value. The hash is like a unique fingerprint of the document, expressed in the form of a large number. The user then sends the signed hash along with the original document to the recipient. The recipient, in turn, takes the signed hash, applies the sender's public key which transforms the signed hash into the original unsigned hash, and then creates a fresh hash of the original document as sent. The two hashes must be identical for the digital signature to validate. The email client software performs all of these functions – the user does not have to go through each step manually.

To describe an analogous situation using fingerprints, consider a case where the message sender wishes to send an emissary whom the recipient can trust. The sender takes the emissary's fingerprints (the "hash"), then seals the fingerprints in an envelope on which the sender signs his or her name manually so that it would be apparent if the envelope had been opened by anyone else (the envelope and content now constitute the "signed hash"). The emissary then carries the envelope and presents himself or herself to the recipient. The recipient takes the fingerprints of the emissary as he or she arrived; takes the envelope, verifies the written signature on it (converts the "signed hash" to the original hash), then opens the envelope and compares the fingerprints inside the envelope to those just taken from the emissary. If

they are identical, the emissary is deemed to be the person sent by the sender. While this analogy is not perfect, it illustrates the concept in a human setting.

The action of digitally signing and then validating the signature to authenticate the sender provides data integrity for the document because any change to the document after the original hash is generated and signed would cause the signature to fail to validate. This affords *technical* non-repudiation—the user cannot later deny that his or her private signing key was used to make the digital signature. Of course, it is still necessary to demonstrate that the user had control of the private signing key to establish *legal* non-repudiation.

Why Do We Need PKI?

Health Insurance Portability and Accountability Act (HIPAA)

Originally, the bill—also known as the Kennedy-Kassebaum bill—had the simple objective to assure that health insurance coverage continued following and between jobs. Congress added the “Administrative Simplification” portion, in large part at the urging of the health care industry. The Administrative Simplification portion of the act had the goal of saving money through standard electronic transactions and standard record formats, code sets, and identifiers. However, electronic transactions have a down side: increased risk to security and privacy. As a result, pursuant to the statute, the Department of Health and Human Services issued additional security and privacy regulations.

The most challenging portions of the HIPAA regulations deal with privacy, but privacy for electronic records and transactions cannot be guaranteed without an effective security infrastructure. Included in this infrastructure are strong authentication, transaction integrity, the assurance of medical information confidentiality, and non-repudiation. These requirements are satisfied through a Public Key Infrastructure (PKI).

Government Paperwork Elimination Act (GPEA)

The Government Paperwork Elimination Act (P.L. 105-277, Title XVII), allows citizens to use electronic technologies when filing information with, or retrieving it from the Federal Government. The Act, signed into law October 1998, directs Federal agencies to provide public access to government services and documents by 2003 and give the public the option of submitting government forms electronically.

GPEA provides the legal framework for agencies to accept electronically submitted forms and documents. Under GPEA, agencies will develop information systems that enable online submissions of forms, reports and other data. Agencies will be required to guard privacy and protect documents from being altered. PKI, digital signatures, and other measures will be used to authenticate citizens and protect their information transfer as they electronically transact business with the Government.

Other Legislation

Other legislation, including the Government Information Security Reform Act (GISRA), the Computer Security Act, and the Clinger-Cohen Act, all require that each federal agency put in place the policies, practices, and technology sufficient to safeguard the agency’s investment in information technology assets. These acts consistently require strong authentication, data integrity, and appropriate confidentiality. These requirements are all satisfied by PKI.

IHS PKI Pilot Project

How Should IHS Make PKI a Cost-Effective Reality?

The most common approach to launching PKI is a pilot project. Get your feet wet. Map the due diligence and procedural requirements against the culture of the organization. Look at the volatility of the certificates that will be issued. What is their life expectancy and need for modification? Check the interface issues. What is the prospective growth curve for certificate use? How many entities will be involved? Is cross-certification necessary? Above all else, examine the authorization process requirements that must co-exist with PKI. PKI is not a full-function access-control process. Look into the standards and regulations that affect our industry. Is interoperability a major requirement? If so, how flexible is the design of the solutions being considered?

Project Phases

The IHS PKI Pilot Project is a joint DoD, VA, and IHS pilot project under the auspices of the Government Computer-Based Patient Record (GCPR) project.

In the first phase, the participants will establish appropriate policies, define necessary practices, and install and test enabling technologies for a Public Key Infrastructure. These PKI policies, practices, and technologies must be compatible with the GSA Federal Bridge Certificate Authority (FBCA).

In phase two, security tokens (smart cards, keys, fingerprint readers, etc.) to enable two-factor authentication (two of the three following categories: something you know (passwords, PINs), something you have (token, smart card), something you are (biometric)). This two-factor authentication is especially important for Internet access or remote access using dial-up modems.

In phase three, one or more existing application packages will be selected for modification to enable programmatic implementation of PKI technologies. Here, techniques for the automated use of PKI to secure file transfers will be explored. This will enable us to develop reliable estimates of the time and resources needed to implement secure transfer of medical information as required by HIPAA, and personal privacy information as required by GPEA.

Appendix A — What is Public Key Infrastructure (PKI)?

Encryption Defined

Encryption is a process for making intelligible information unintelligible through the application of sophisticated mathematical conversion techniques. Obviously, to be useful the process must be reversible (decryption). The three major components of the encryption/decryption process are as follows:

- 3) *The information stream in clear or encrypted form.*
- 4) *The mathematical encryption process*—the algorithm. Interestingly, most commercial algorithms are publicly available and are not secret. What turns a public process into a uniquely secret one is the encryption key.
- 5) *The encryption key.* The encryption key is a data string that is mathematically combined with the information (clear or encrypted) by the algorithm to produce the opposite version of the data (encrypted or clear). Remember that all data on computers is represented in binary number coding. Binary numbers can be operated upon by the same arithmetic functions as those that apply to decimal numbers. So by combining complex arithmetic operations, the data and key are converted into an encrypted message form and decrypted using the same process and *same key—with one critical exception.*

Before explaining the exception, one more definition is required. The process that uses the *same key* to decrypt and encrypt is called *symmetric* cryptography. It has several advantages, including exceptional speed on computers. It has a serious drawback. In any population of communicating users (n), in order to have *individually unique* links between each pair of users, the total number of keys required is $n(n+1)/2$. Try it with a small number and round up. If the population of users gets large enough, the number of individual keys required rapidly becomes unmanageable. This is one (but not the only) reason why symmetric cryptography has not had a great reception in the commercial marketplace in the last 20 years.

The salvation of cryptography for practical business use has been the application of a different class of cryptographic algorithms using *asymmetric* key pairs. The mathematics is complex and is not intuitively obvious, but the result is a *pair of linked keys* that must be used together. However, only one of the pair, the private key, must be kept secret by the key owner. The other half of the pair—the public key—can be openly distributed to anyone wishing to communicate with the key owner. A partial analogy is the cash depository in which all customers have the same key for depositing through a one-way door, but only the bank official has a key to open the door to extract the cash. This technique vastly reduces the number of keys required for the same population to communicate safely and uniquely.

Enter PKI

If the public key is distributed openly, how do you know that it is valid and belongs with the appropriate secret key and the key owner? How do you manage the creation, use, and termination of these key pairs? That is the foundation of PKI. Several definitions follow:

The comprehensive system required to provide public-key encryption and digital signature services is known as the *public-key infrastructure* (PKI). The purpose of a public-key infrastructure is to manage keys and certificates

Entrust Inc.

A public-key infrastructure (PKI) consists of the programs, data formats, communications protocols, institutional policies, and procedures required for enterprise use of public-key cryptography.

Office of Information Technology, University of Minnesota

In its most simple form, a PKI is a system for publishing the public-key values used in public-key cryptography. There are two basic operations common to all PKIs:

1. Certification is the process of binding a public-key value to an individual organization or other entity, or even to some other piece of information such as a permission or credential.
2. Validation is the process of verifying that a certificate is still valid.

How these two operations are implemented is the basic defining characteristic of all PKIs.

Marc Branchaud

The Digital Certificate and Certificate Authorities

A digital certificate is the focal point of the PKI process. What is it? In simplest terms, a digital certificate is a credential (in digital form) in which the public key of the individual is embedded along with other identifying data. That credential is encrypted (signed) by a trusted third party or certificate authority (CA) who has established the identity of the key owner (similar to but more rigorous than notarization). The “signing key” ties the certificate back to the CA and ultimately to the process that bound the certificate holder to his or her credentials and identity proof process.

By “signing” the certificate, the CA establishes and takes liability for the authenticity of the public key contained in the certificate and the fact that it is bound to the named user. Now total strangers who know or at least trust a common CA can use encryption not just to *conceal* the data but also to *authenticate* the other party. The *integrity* of the message is also ensured. If you change it once encrypted, it will not decrypt. The message *cannot be repudiated* because it has been encrypted using the sender’s certificate.

Who are CAs? Some large institutions are their own CAs, especially banks (private CAs). There are some independent services (public CAs) developing, and government, using the licensing model as a take off point, is moving into this environment.

As you would expect, there has been a move by some security professionals to include more information in the certificate, making it a multipurpose “document.” There is one major problem with this. Consider a driver’s license, which is printed on special watermarked paper, includes the driver’s picture and is encapsulated in plastic. If one wished to maintain more volatile information on it, such as current make of car(s), doctor’s name and address, or next of kin, the person would have to get a new license for each change.

The same is true for a certificate. The user would have to go back to the CA for a new certificate each time he made a change. For a small and readily accessible population, this may be reasonable. However, PKI is usually justified based on large populations in open environments, often across multiple enterprises. The cost and administrative logjam can build up with the addition of authorization updates *embedded in the certificate*. This is why relatively changeable authorization data (permissions) are seldom embedded in the certificate but rather attached. There are several certificate structures that allow attachments or permissions that can be changed independently of the certificate itself.

To review, the certificate is the heart of the PKI system. A given population of users who wish to intercommunicate selects or is required to use a specific CA to obtain a certificate. That certificate contains the public-key half of an asymmetric key pair as well as other indicative information about the target individual. This individual is referred to as the “distinguished name”—implying that there can be no ambiguities in certificate-based identification—all Smiths must be separately distinguished by ancillary data.

Where are Certificates used?

Certificates are used primarily in open environments in which closed network security techniques are inappropriate or insufficient for any or all of the following:

- Identification/authentication
- Confidentiality
- Message/transaction integrity
- Nonrepudiation

Not all PKI systems serve the same purposes or have the same protective priorities. This is important to understand when one is trying to justify a PKI system for a specific business environment.

How Does PKI Satisfy Those Business Environment Needs?

Market Expectation. As PKI becomes interoperable, scalable, and generally accepted, companies will begin to accept the wide use of encryption-related products. Large enterprises such as government, banks, and large commercial firms will develop trust models to easily incorporate PKI into everyday business use.

Current Reality. It is not that easy. Thus far, a significant number of PKI projects have been curtailed, revised, or temporarily shelved for reevaluation. The reasons most often given include the following:

- Immature technology
- Insufficient planning and preparation
- Underestimated scope
- Infrastructure and procedural costs
- Operational and technical incompatibilities
- Unclear cost-benefits

Apparent Conclusions

PKI has compelling justifications for IHS, but there are likely to be more variables and pitfalls than anticipated. Broadside implementation, though sometimes necessary, has not

been as cost-effective, and will not be attempted at IHS. Pilots and test beds are planned (see IHS PKI Pilot Project plan below).

A properly designed Certificate Authority/Registration Authority (CA/RA) administrative function is always a critical success factor.

Certificates, Certificate Authorities, and Registration Authorities

How do they work and how are they related?

First look at the PKI certificate lifecycle. It is more involved than one may think. A digital certificate is a secure and trustworthy credential, and the process of its creation, use, and termination must be appropriately controlled.

Not all certificates are considered equally secure and trustworthy, and this is an active subject of standards and industry discussion. The strength of the cryptography supporting the certificate is only one discriminating factor. The degree to which the certificate complies with a given standard, X.509, for example, is another criterion for trustworthiness. The standards cover a wide range of requirements, including content, configuration, and process. The following is hardly an exhaustive list, but it will provide some insight into some of the basic requirements of the process.

- *Application*—How do the “certificate owners to be” apply for a certificate? To whom do they apply? What supporting materials are required? Must a face-to-face interview be conducted, or can a surrogate act for the subject? What sanctions are imposed for false, incomplete, or misleading statements? How is the application stored and protected, etc.?
- *Validation*—How is the applicant’s identity validated? By what instruments? By what agencies? For what period of time?
- *Issuance*—Assuming the application meets the criteria and the validation is successful, how is the certificate sent to the individual or, in the case of an organization, some officer of that organization? How is issuance recorded? How are those records maintained and protected?
- *Acceptance*—How does the applicant indicate acceptance of the certificate? To whom? Is Nonrepudiation of acceptance eliminated?
- *Use*—What are the conditions of use? Environments, systems, and applications?
- *Suspension or Revocation*—In the event of compromise or suspension, who must be notified? How? How soon after the event? How is the notice of revocation published?
- *Expiration and Renewal*—Terms, process, and authority?

Who and What Are the PKI Functional Entities?

Certification Authority (CA)

- A person or institution who is trusted and can vouch for the authenticity of a public key
- May be a principal (e.g., management, bank, credit card issuer)
- May be a secretary of a “club” (e.g., bank clearing house)
- May be a government agency or designee (e.g., notary public, Department of Health and Human Services, or post office)
- May be an independent third party operating for a profit (e.g., VeriSign)
- Makes a decision on evidence or knowledge after due diligence

- Records the decision by signing a certificate with its private key
- Authorizes issuance of certificate

Registration Authority (RA)

- Manages certificate life cycle, including Certificate Directory maintenance and Certificate Revocation List (CRL) maintenance and publication
- Thus can be a critical choke point in PKI process and a critical liability point, especially as it relates to CRLs
- An RA may or may not be a CA

Other Entities

- *Other Trusted Third Parties*—These may be service organizations that manage the PKI process, brokers who procure certificates from certificate suppliers, or independent audit or consulting groups that evaluate the security of the PKI procedure
- *Individual Subscribers*
- *Business Subscribers*—In many large organizations, two additional constructs are used:
 - *The Responsible Individual (RI)*—The enterprise certificate administrator
 - *The Responsible Officer (RO)*—The enterprise officer who legally assures the company's commitment to the certificate. In many business instances, it is more important to know that this certificate is backed by a viable organization that will accept liability than to be able to fully identify the actual certificate holder. In a business transaction, the fact that a person can prove he or she is a partner in Deloitte & Touche LLP who is empowered to commit the firm usually means more than who that person is personally.

PKI policies and related statements include the following:

- Certificate policy
- Named set of rules governing certificate usage with common security requirements tailored to the operating environment within the enterprise
- Certificate practices statement (CPS)
- Detailed set of rules governing the Certificate Authority's operations
- Technical and administrative security controls
- Audit
- Key management
- Liability, financial stability, due diligence
- CA contractual requirements and documents
- Subscriber enrollment and termination processes

Appendix B — For Additional Information Sources

Public Key Infrastructure (PKI)

The Evolving Federal Public Key Infrastructure —
http://www.cio.gov/fpkisc/documents/PKI_Brochure.pdf

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology — <http://www.gao.gov/new.items/d01277.pdf>

NIST PKI Program — <http://csrc.nist.gov/PKI/>

NIST Special Publication 800-25: Federal Agency Use of Public Key Technology for Digital Signatures and Authentication — <http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.doc>

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act —
<http://www.hcfa.gov/regs/hipaacer.htm>

Administrative Simplification — <http://aspe.hhs.gov/admsimp/>,
<http://www.hcfa.gov/regs/hipaacer.htm>

Government Paperwork Elimination Act (GPEA)

Government Paperwork Elimination Act — <http://www.ec.fed.gov/gpea.htm>