Global Information Assurance Certification Paper

Implementation Considerations for the Federal Public Key Infrastructure

Phillip W. Hayes
GSEC Practical v1.4b
Option A

Table of Contents

Abstract

Over the past several years, the government has made significant efforts to reduce the amount of paper-based processes, and shift more towards e-government. E-government would be designed to promote and facilitate electronic transactions between the government and its customers (i.e. public citizens, other governments, etc.). However, in order to foster trust in such transactions, the government needs to provide assurance that basic privacy and security considerations have been addressed. For this purpose, there are efforts underway to establish a Federal Public Key Infrastructure (FPKI) that will accommodate secure electronic transactions between the government and its customers.

The FPKI is intended to provide four basic assurances: authentication, data integrity, confidentiality, and non-repudiation. The FPKI will rely upon the appropriate mix of hardware, software, people, and processes in order to function adequately. Development efforts will also rely heavily upon communication and coordination with the private sector. In addition, there are several implementation considerations that must be addressed during the design, development, and implementation phases. The primary implementation considerations include interoperability, flexibility, ease of use, and scalability. In this paper, I will detail how each one of these implementation considerations impacts the feasibility and potential for the successful development of a Federal PKI.

Introduction

The growth of the Internet and other communications networks, along with an ever increasing number of computers in the workplace as well as private homes, has revolutionized the way business transactions are conducted, and has created numerous opportunities for organizations to improve service to consumers. Recent studies estimate that over 119 million users have access to the Internet[1], and of those users, approximately one-third are using the Internet to search for product and service information and make online purchases.[2] In the Federal government, there are approximately 80 million transactions each year,[3] and the ability to disseminate information quickly and easily is always a concern. Thus, the Internet provides the government with the opportunity to provide services and information to the public and other customers with less time and effort.

As a result of the National Partnership for Reinventing Government (NPR) and other government reinvention efforts, the concept of electronic government emerged. In the 1997 report "Access America," Vice President Al Gore identified steps to encourage and increase consumer and business access to government resources electronically. However, in order to promote electronic interaction between the government and its consumers, there must be a certain

level of confidence that government systems will provide adequate security for consumer information and sensitive data. According to "Access America,"[4] public confidence in the security of the government's electronic information and information technology is essential to creating government services that are more accessible, efficient, and easy to use. Services such as electronic commerce, electronic mail, and electronic employee benefits involve the transfer of sensitive information within government, between the government and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, assure that the information is not altered in an unauthorized way, and be available when needed. In order to promote and establish a base for this trusted environment, efforts are underway to establish a Federal Public Key Infrastructure (FPKI). The FPKI is being touted as a foundation for establishing secure Federal electronic transactions both internally (among Federal government employees and agencies) and externally (between the Federal government and its trading partners – governments, businesses, and individuals).

Foundation of the PKI

PUBLIC KEY CRYPTOGRAPHY

In the past, a traditional form of cryptography, known as symmetric, or secret key, cryptography was used for the encryption/decryption of messages. However, this cryptographic method has a major flaw, in that the interception of the key by an outside party allows for easy message decryption. Public key infrastructure assumes the use of public key, or asymmetric, cryptography, the most common method of message authentication (digital signatures) and encryption/decryption on the Internet. In public key cryptography, a pair of keys, one public key and one private key, are created simultaneously using the same algorithm. The private key is known only by the owner, and the public key is published in an open directory. Information encrypted using the public key, can only be retrieved using the corresponding private key. Likewise, information encrypted using the private key, can only be decrypted using the corresponding public key. However, public key cryptography alone does not provide a trusted transaction environment. For this reason, the concept of a public key infrastructure was established.

A public key infrastructure is more than simply cryptographic algorithms, but rather a combination of hardware, software, processes, policies, procedures, and agreements that promote secure electronic interactions. The following components represent integral pieces of a public key infrastructure:

- Organizational security policy
- Certificate authority (CA)
- Registration authority (RA)
- Certificate management system.

BASIC COMPONENTS OF A PKI

A security policy outlines and defines an organization's policies and procedures for information security, including processes and practices for the use of cryptography. The policy should be designed to also include methods for public/private key management, as well as, appropriate levels of security controls necessary to effectively mitigate the associated risks. Policies and procedures provide the framework for establishing an organization's security posture, and also demonstrate upper-level management's overall expectations and organizational focus.

A certificate authority is an entity that creates, signs, and manages digital certificates for users of a PKI. These digital certificates bind the identity of the owner of a public/private key pair with other information contained in the certificate. For example, the owner of a public/private key pair may be bound to a purchase threshold of $10,000 or less. For the binding to be secure, the certificate must be digitally signed by a CA. The certification authority system is critical for the success of a PKI because it manages digital certificates for their entire life cycle, from generation to revocation. The CA utilizes a certificate practice statement (CPS) that defines the practices employed by the CA to manage digital certificates. The CA may be rated on its ability to adapt a CPS to the needs of an organization, as well as its rules and security methods for user identification.

There are three types of CA architectures that are generally considered when implementing a PKI:

- Hierarchical architecture
- Mesh architecture
- Bridge CA architecture

Of the three architecture types, the bridge CA architecture is being developed within the FPKI to cross-certify CA certificates from member entities. Under this model, trust rests with the bridge CA, and all certificates are certified through the bridge CA. Using this concept, the Federal Bridge Certification Authority (FBCA) would act as a trusted third party, and when an agency needs to accept a certificate from an outside entity, the FBCA would issue a cross-certified certificate that could be trusted by that agency.[5]

A registration authority acts as an intermediary for the user and certification authority. The RA has the responsibility of verifying that the requestors of a certificate identify themselves according to the rules outlined in the issuing organization's security policy. The RA then requests and authorizes the CA to issue a digital certificate to the requestor.

A certificate management system establishes methods for digital

certificate distribution and storage. A certificate management system consists of one or more directories where the certificates and their public keys are maintained. Sound management of digital certificates is essential to the success of a PKI due to the critical nature of digital certificates in the establishment of a trusted environment.

INTENDED SECURITY FUNCTIONS OF THE FEDERAL PKI

The Federal PKI is intended to be an integral piece in establishing secure and trusted electronic transactions between the government and its various customers. In order for acceptance and use of the FPKI to develop, it is important that the government's customers, or users of the FPKI, have assurance that an acceptable level of security and privacy exist. There are four basic security functions that the FPKI is planned to provide:

- Authentication
- Data integrity
- Non-repudiation
- Confidentiality

Authentication ensures that messages and their senders are authentic. The sender and recipient of information need to be confident that the message was sent from and is going to the appropriate parties. Data integrity ensures that data has not been accidentally or maliciously altered from its original state. Non-repudiation prohibits the sender or recipient of a message from denying ownership of the message. This aspect can be of significant importance in a legal dispute, as ownership and receipt of the message cannot be denied. Confidentiality ensures that only authorized parties can read the electronic message, thus information being transmitted must be protected in transit. These basic building blocks form the foundation of the FPKI, but there are still considerations that need to be addressed in order to successfully implement a PKI in general, and the Federal PKI specifically.

Implementation Considerations for the Federal PKI

Many of the considerations that affect PKI in the private sector, will also affect PKI in the public sector. The Federal PKI must be interoperable, flexible, easy to use, and scalable. The development of the FPKI will involve agencies defining their business requirements, defining the requirements of their customers, and working in conjunction with private industry to establish the hardware, software, and processes required to provide a secure and functional solution.

INTEROPERABILITY AND FLEXIBILITY

At the present time, PKI technology and solutions within the Federal government remain in the early design and implementation stages, and it is impractical to try to predict all of the future uses and requirements of PKI-based systems. Although the development of standards governing the use of PKI in the government has advanced considerably, the use of PKI technology has not progressed within the Federal sector as once anticipated.[6] The private industry has developed a number of PKI-solutions, and the implementation methods may be different for each one. For this reason, it is unlikely that all the components of the FPKI will be procured from the same entity. Therefore, the FPKI should attempt to use the most standard commercially available products that will provide the most widely interoperable environment. It is important that the government take into account interoperability when considering development of the FPKI. The FPKI must be fully interoperable among the governments various customers, including individual federal agencies, private sector companies, state and local governments, private citizens, and possibly foreign governments as well. The lack of interoperability will negate the investment into and implementation of the Federal PKI, in that although agencies have the potential for secure electronic transactions, its customers lack the technology or have employed different technologies to interact.

The FPKI should also be flexible enough to adequately accommodate a range of applications, and address the different requirements and operating practices of individual agencies. There are hundreds of applications across the Federal government, and taking into account the various applications that Federal customers employ, flexibility becomes increasingly critical to the success of the FPKI. Similar to a lack of interoperability, the inability of the FPKI to support the resident applications of the various government and commercial entities will hinder the success and widespread use of the FPKI.

Government agencies and other regulatory bodies including the General Services Administration (GSA), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST) have taken steps to promote interoperability and flexibility related to public key infrastructure technology. NIST in particular has taken a leading role in developing a draft set of minimum interoperability standards to be used by Federal agencies and vendors when procuring PKI solutions. The NIST document *Minimum Interoperability Standards for PKI Components* (MISPC) deals primarily with "aspects of PKI interoperation most apparent to end users, that is how to request and be issued a certificate, how to sign documents, how to retrieve the certificates of others, and how to validate signatures.[7]" In addition, the MISPC provides baseline standards for critical operational areas such as certificate generation, distribution, renewal, validation, and revocation. Policies and standards such as the MISPC are necessary to ensure that interoperability considerations are included in the design, development, and implementation phases of the FPKI.

EASE OF USE

The FPKI should be easy to use by all levels of users, ranging from the moderately computer literate citizen, to the computer proficient user. Although the principles underlying PKI are technical and complicated, use of the FPKI should be just the opposite. In order for the FPKI to be used on a large scale, it will have to support a wide-range of individuals with varying knowledge levels. The functions and operations performed via PKI should be simple, and the customer interface should be intuitive. Ease of use will directly affect the return on investment of the PKI, as it determines the amount of training needed, maintenance and system configuration required, and growth in the number of future users. Users will not wish to deal with complex, non-intuitive processes. Ease of use, interoperability, and flexibility must be considered in the design phase, and should all be considered when defining business and customer requirements, and simultaneously working with private industry for functional PKI solutions.

Defined Business and Customer Requirements

To facilitate the development of standards and requirements for the FPKI, the Federal government must identify and define its business requirements. The government is the largest creator, collector, user, and disseminator of information. Programs such as Social Security, tax collection, and national security rely on Federal information systems. It will be the responsibility of each agency to determine how to support such programs, and improve other services to its consumers in a PKI-supported environment. Unclear business requirements may lead to many different PKI-solutions in the government that are not interoperable. Sound business requirements should encompass standards for PKI use and viable solutions. The government will need to answer several key questions, including the following:

- What is our business?
- What key processes and/or functions can be supported electronically?
- How sensitive is the data that will be transmitted?
- What level of privacy and security is needed to provide adequate assurance that transactions are secure?

Equally important is the government's need to clearly define its customer base and identify their needs accordingly. The government has a diverse client base with which it interacts, and the different customers have different needs. For instance, a private citizen may only need to interact with the government electronically on an infrequent basis (i.e. filing personal taxes), whereas a private sector company may have frequent interaction with the government (i.e. submitting bids on a Federal bid posting system). However, although these groups have different business needs, they share the desire for the information to be available, secure, and reliable. Therefore the government must ensure

that its business requirements and customer requirements are clearly defined and adequately considered as design and development of the FPKI continue. It must also be noted that business and customer requirements are not static, and as such, adjustments to requirements should be made as new information, business practices, and technologies are developed.

Continued Interaction with Private Sector Companies

The private sector is leading the way in development of commercially available PKI solutions, and as such, the government must work in conjunction with the private sector to ensure interoperable technology and flexible PKI solutions that are scalable to organizational needs, and provide the requisite functionality to effectively serve its customer's needs. In theory, by working in conjunction with private sector companies, the government has the opportunity to develop a robust infrastructure that is capable of supporting a wide range of applications and user levels. If the government hopes to gain a return on its investment into a PKI, then coordinated efforts with the private sector are essential. Only by keeping up with the latest PKI technology and solutions can the government hope to achieve interoperability on a large scale. There must be a mechanism to ensure that the latest applications, cryptographic methods and products, and other necessary security technologies are considered. In its most basic form, it is reasonable to assume that the FPKI will be successful only if there is a perceived level of trust greater than or equal to paper-based transactions.

SCALABILITY

As trust in the FPKI increases, it can be construed that use of the FPKI would increase; more Federal agencies, state and local governments, private companies, and private citizens would begin to see benefit in using the FPKI. As use increases, scalability of the FPKI becomes more critical; the FPKI must be able to grow as necessary. The infrastructure should not limit the number of possible users, and should be able to accommodate increases in the user community. For example, several programs within the Federal government are attempting to demonstrate the benefits of PKI (i.e. Access Certificates for Electronic Services) in efforts to promote the development and utilization of a Federal PKI and encourage agency buy-in. Assuming such programs can demonstrate successful results, the number of organizations wishing to participate in the development of the FPKI will increase, and the infrastructure must be able to handle this increase. If the infrastructure is not able to scale well, the return on investment will not reach its potential, and the efficiencies provided through electronic government will not be fully realized.

Conclusion

The central purpose of the Federal government is to serve its citizens and consumers efficiently and effectively. The explosion of E-business/government has revolutionized the way in which government can provide services and disseminate information to its customer base. However, along with this opportunity for improved service delivery are associated security risks that put these services and information at risk. It then becomes the responsibility of the government and each of its customers to try to establish a mechanism by which a reasonable level of assurance in electronic transactions can be provided. The Federal PKI presents the opportunity for a trusted computing environment that can support secure electronic transactions between the Federal government and its customers. In order to further develop and establish this trusted environment, the government must continually re-evaluate its business requirements and those of its customers, while partnering with organizations outside of government to foster and maintain relationships that will lead to increased interoperability and trust. Properly developed, the Federal PKI will facilitate information dissemination and an array of electronic commerce opportunities in a manner that protects the privacy of its customers, while establishing a secure environment for the operation of Federal information systems.

---

1 Parker.
2 Pastore.
3 Reuters.
4 Gore.
5 Jones.
6 Jones.
7 NIST PKI Project Team.

Works Cited

General Accounting Office. "Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology." Feb 2001.

URL: http://www.cio.gov/fpkisc/documents/gao-01-277pkireport.pdf (17 Sep 2002).

Gore, Albert. "Access America, Reengineering Through Information Technology." 3 Feb 1997.

Jones, Jennifer. "PKI At the Crossroads." 24 June 2002.
URL: http://www.fcw.com/fcw/articles/2002/0624/tec-pki-06-24-02.asp (17 Sep 2002).

National Institute of Standards and Technology. "Introduction to Public Key Technology and the Federal Public Key Infrastructure." 26 Feb 2001.
URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-32/sp800-32.pdf (17 Sep 2002).

NIST PKI Project Team. "Minimum Interoperability Specification for PKI Components, Version 2 - Second DRAFT." 31 Aug 2000.
URL: http://csrc.nist.gov/pki/documents/MISPC2_public3_20000831.pdf (17 Sep 2002).

Parker, Pamela. "U.S. Internet Population Grows." 19 Aug 2002.
URL: http://isp-planet.com/research/2002/internet_020819.html (17 Sep 2002).

Pastore, Michael. "U.S. Internet Population Continues to Grow." 8 Feb 2002.
URL: http://isp-planet.com/research/2002/us_020208.html (17 Sep 2002).

President's Management Council's Electronic Process Initiatives Committee. "Electronic Commerce for Buyers and Sellers: A Strategic Plan for Electronic Federal Purchasing and Payment." Mar 1998.

Reuters. "U.S. Treasury to Launch Federal Portal." 25 Jul 2000.
URL: http://www.thestandard.com/article/0,1902,17100,00.html (17 Sep 2002)

Stallings, William. Cryptography and Network Security: Principles and Practice.
New Jersey, Prentice-Hall: 1999.