Development of a Public Key Infrastructure Across Multiple Enterprises

by T. M. Sharick, J. P. Long, B. J. Desind, V. A. Hamilton, and B. J. Wood¹

Abstract

Main-stream applications are beginning to incorporate public key cryptography. It can be difficult to deploy this technology without a robust infrastructure to support it. It can also be difficult to deploy a public key infrastructure among multiple enterprises when different applications and standards must be supported.

This discussion chronicles the efforts by a team within the US Department of Energy's Nuclear Weapons Complex to build a public key infrastructure and deploy applications that use it. The emphasis of this talk will be on the lessons learned during this effort and an assessment of the overall impact of this technology.

RECEIVED

MAY 08 1997

Introduction

Developers are constantly seeking new and better ways to integrate strong security mechanisms into information systems. Classically, highly-secure information systems have been slow and clumsy at best. Researchers have long speculated that the integration of public key cryptography [1] into these networks could improve overall security without adding an unacceptable burden on users, developers, or administrators.

Recently, main-stream applications have begun to incorporate sophisticated public key cryptography features. Some examples include the popular families of World Wide Web browsers and servers by Netscape and Microsoft [2] [3] as well as security-enhanced messaging products that support the new Secure Multipurpose Internet Messaging Extensions (S/MIME) [4].

Unfortunately, it can be argued that many of today's applications that implement public key cryptography simply shift the security and administration burden from the end user to the network administrator. Although this may be an appropriate shift in responsibility, it represents a new challenge to developers of modern information management networks. Many of today's network administrators simply are not prepared to provide the services required of a Public Key Infrastructure (PKI).

The remainder of this discussion chronicles the attempts of a team within the US Department of Energy (DOE) to develop a PKI among different facilities.

The Project

The project that brought the PKI team together was the DOE Advanced Manufacturing / National Information Infrastructure (AM/NI) effort. AM/NI's primary goal was to develop advanced technologies that leverage the National Information Infrastructure to improve a variety of manufacturing processes within the DOE.

Early in this project, it became clear that participants wanted to leverage some of the new commercial products to accomplish their goals. The participants also saw the need to respect DOE's traditional emphasis on security. Therefore, the overall goal of the AM/NI Security team was to develop a security-enhanced manufacturing infrastructure using commercial products. The team's emphasis was to develop tools and techniques that could be used to protect unclassified information which all sites could safely share among themselves or with other trading partners over the Internet.

The team also realized that they would have to leverage some of the new public key cryptography features in these products to deliver security solutions that did not create an unacceptable burden on their users. This led the team to the conclusion that AM/NI would have to lead the development of a PKI within the US Department of Energy's Nuclear Weapons Complex.

MASTER

¹ This work was supported by the United States Department of Energy under Contract DE-AC94-94AL84000.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

The Players

The US Department of Energy's Nuclear Weapons Complex is rather unique in many respects:

Locations: The core complex consists of three laboratories and two production facilities: Sandia National Laboratories (Albuquerque, NM and Livermore, CA), Lawrence Livermore National Laboratory (Livermore, CA), Los Alamos National Laboratory (Los Alamos, NM), Allied Signal / Federal Manufacturing & Technologies (Kansas City, MO), and Lockheed Martin Energy Systems (Oak Ridge, TN). The complex also includes the Pantex assembly and storage facility (Amarillo, TX) and other operations.

Contractors: Each of these sites is operated for the DOE by various contractors representing divisions of some large diverse enterprises. The managing contractors include various divisions of Allied Signal Aerospace, the Lockheed Martin Corporation, the University of California, and others. Each of these operating contractors contributes a unique culture and perspective to their facilities.

Management: Oversight for these facilities is also provided by different DOE authorities and offices in Oakland CA, Albuquerque NM, and Washington DC.

Therefore, one of the early challenges for the AM/NH PKI team would be to accommodate the diversity of interests and stake holders represented throughout the complex.

The Process

The basic process that the team created for this project included five steps or phases:

1. **Survey** - Survey each site to determine what PKI products and applications were already in use. The survey also gathered data that revealed certain requirements the new PKI must meet.
2. **Design** - Given the survey results, develop a basic system design or approach that would meet most perceived requirements.
3. **Evaluate Products** - Determine how well existing commercial products met the system's perceived requirements. The team was committed to finding a commercial solution rather than developing its own products.
4. **Deploy** - Given that a commercial solution would be acceptable, deploy that system to each site in the complex.

5. **Evaluate Performance** - Continuously evaluate network performance and document both lessons learned and needed improvements.

Survey Results

The survey was conducted in the Spring and Summer of 1995 with the preliminary results presented in August 1995 [5]. This survey indicated that a variety of encryption products were used, but there were no clear leaders among the products of interest. Most security-enhanced applications included electronic messaging, forms management, and other workflow applications. In addition, *Netscape Navigator* was seen as becoming the *de facto* standard for sites that had already embraced the technology of the World Wide Web (WWW).

These results lead the team to design a relatively-simple PKI to meet the following (non-inclusive) list of requirements:

1. The system should support both certificate hierarchies and cross-certification. The team felt that cross-certification of Certificate Authorities (CAs) provided the best performance. However, the team was concerned that the DOE would implement a strictly-hierarchical PKI, so the team concluded that support for both hierarchical and cross-certified CAs was needed.
2. The CAs must be readily accessible over an open public network. The public network of choice was the global Internet. This was somewhat of a departure for the team, because valuable DOE computing resources are not traditionally exposed to the global Internet.
3. The PKI should provide support for products and applications currently used within the complex. At the time of the survey, the following products were seen as standards within the complex:
 - *Netscape Navigator* and the *Netscape Commerce Server* for hypertext applications.
 - Oracle database servers. The expectation was that *Netscape Navigator* would eventually replace the Oracle clients that had already been deployed on desktops.
 - X.500 for directory services. Most DOE sites had made significant investments in X.500 technology, so it was highly desirable for the team to leverage this investment rather than require that each site develop a new public directory service.

4. The PKI should provide broad support for applicable existing and emerging standards for both the US government and the private sector. The primary government standard of interest was Federal Information Processing Standards Publication (FIPS PUB) 186 [6] for digital signatures and FIPS PUB 140-1 [7] for security validation. However, the team was aware that other Federal PKI standards were under development at the National Institute for Standards and Technology. The team was also monitoring PKI developments within the private corporate environment and on the Internet. The team also sought support for various Applications Programming Interfaces (APIs) such as Microsoft's CryptoAPI [8] and others.

Product Evaluation

The team conducted a thorough product evaluation in parallel with the site surveys (Summer 1995). The evaluated products included:

- *Certificate Issuing System (CIS)* by RSA Data Security². [9] [10]
- *Entrust* by NORTEL (formerly Northern Telecom)³. [11]
- *MIME (Multipurpose Internet Mail Extensions) Object Security Services / Privacy Enhanced Mail (MOSS/PEM)* as distributed by Trusted Information Systems. [12]
- *Navigator and Commerce Server* by Netscape Communications Corporation. [2]
- *Pretty Good Privacy (PGP)* as distributed by the Massachusetts Institute of Technology (MIT) [13] and ViaCrypt⁴. [14]

In addition, other products were evaluated early in the process, including Apple's *DigiSign* [15] and AT&T's *SecretAgent* [16].

The actual evaluation results are not included in this report, because the AM/NII team was privy to some proprietary information, and some of this information was also gathered under non-disclosure agreements.

² RSA has since established a subsidiary, VeriSign, to supply PKI products and services.

³ NORTEL has since established a subsidiary, Entrust Technologies, to supply PKI products and services.

⁴ The commercial version of PGP is now distributed by PGP, Inc.

Deployment

Based on the information gathered from the site surveys and product evaluation, the team selected *Entrust* for the AM/NII PKI.

Strengths

The *Entrust* product line was selected primarily because it exhibited the following perceived strengths:

Emphasis on automated key management - *Entrust* manages a full range of key management services, including (but not limited to): distribution, destruction, and revocation. The product normally performs these services when appropriate without user or manager intervention.

Seamless key archive and recovery - *Entrust* also performs automatic key backup, recovery, and archive. This avoids some of the problems associated with verifying signatures on documents after the private key used to sign the document has either expired or been revoked. This feature may also satisfy future US government requirements to support a key escrow or key recovery infrastructure.

Separate keys for signing and encrypting - *Entrust* uses separate key pairs for both signing and encrypting documents. This feature gives the manager the capability to better control who has the capability to sign or encrypt documents.

Algorithm flexibility - *Entrust* also allows the user and manager to choose among a variety of cryptographic algorithms for both signing and encrypting documents.

Weaknesses

Unfortunately, the *Entrust* product line is not perfect. It contains the following problematic features:

Licensing fees - The majority of the costs for deploying *Entrust* are incurred in license fees charged for each key pair issued by the system. These costs can be significant—as much as \$100 per key pair. However, the exact cost for each key pair is negotiated as part of the price for each *Entrust* installation. So, this fee varies from site to site, even within the AM/NII PKI.

Certificate Access - *Entrust* uses an X.509 v3 certificate [17] with extensions. However, this certificate is not generally available to the applications developer, even when using the *Entrust* API.

Development of a Public Key Infrastructure Across Multiple Enterprises

Multiple signature support - *Entrust* does not normally support multiple signatures on documents. Ideally, developers would have the option to add hierarchical and parallel signatures to a given document. Unfortunately, *Entrust* does not currently support either of these types of multiple signatures. *Entrust* Technologies has committed to provide multiple signature support for the AM/NII sites. However, it is not clear what form this support will take.

Support for other PKI-enabled applications - *Entrust* is optimized for applications that are "*Entrust-aware*". However, there are some common popular applications that require PKI support but are not *Entrust-aware*. The most notable example of this kind of application is the *Netscape Navigator*. Netscape optimizes their product line for the VeriSign PKI. *Entrust* Technologies currently offers a separate product to generate Netscape-compatible certificates, the *Entrust WebCA*. However, *WebCA* is not currently integrated into the *Entrust* PKI. *Entrust* Technologies has stated that they intend to integrate the *WebCA* product into the standard *Entrust* PKI at some future date.

Deployment Schedule

The AM/NII team proceeded to develop their PKI by deploying *Entrust* at each of the AM/NII sites at a conservative but steady pace.

Spring 96 - *Entrust* was deployed at Lawrence Livermore National Laboratory (LLNL). The primary use for the PKI at LLNL was an electronic forms application using the Shana *InFormed* [18] product family.

Summer 96 - *Entrust* was deployed at Sandia National Laboratories (SNL). The primary use for the PKI at SNL is to provide privacy and authentication for electronic mail using IBM's *cc:Mail* [19], Microsoft Mail, and Qualcomm's *Eudora* [20] products.

Fall 96 - *Entrust* was installed at the Allied Signal / Federal Manufacturing & Technologies Kansas City Plant (KCP). The primary use for the PKI at KCP was to authenticate documents generated at SNL / New Mexico. These documents are used to transfer funds between the two sites.

Spring 97 - *Entrust* is being installed at the US Department of Energy's Headquarters (DOE/HQ) in Washington, DC. The primary application for the PKI at DOE/HQ is to evaluate its use in a travel reimbursement system and other security-enhanced applications.

Entrust will be installed at the other AM/NII sites as resources and requirements dictate.

Deployment Issues

One result of the deployment process is that the project team has identified many new issues that must be addressed to fully leverage the PKI. These issues, for the most part, have not yet been resolved in the AM/NII PKI.

Identity verses authority - A certificate can certify the public key for a given user in the PKI, but it cannot normally convey the authority that the user's signature represents. For example, a certificate can certify the public key for "John Q. Public @ Acme Corporation", but it cannot tell the verifying party whether John Q. Public is signing as a staff member, manager, or procurement officer for the company. This problem is further complicated by the situation when one party delegates their signature authority to another party for some specific period of time. One solution to this problem would be to communicate this authority in an extension to the X.509 v3 certificate. However, this approach could be problematic, and the feature is not currently supported in *Entrust*.

Unique personal identifiers - It is essential that users be able to uniquely identify every user in the PKI. The most common or natural way to identify users is through their distinguished or common name. However, this technique is complicated by the fact that a large PKI will likely have some users with the same common name. Another logical personal identifier is a user's Social Security Number. However, the AM/NII team did not want to make its users' Social Security Numbers readily available to anyone over the Internet. This situation is further complicated by the fact that some users do not commonly refer to themselves by their distinguished or legal names. All of these factors can make it difficult for a verifying party to retrieve a certificate from the PKI, even if the directory subsystem is properly configured.

Tracking personnel changes - It is important for the PKI to accurately reflect the employment status of users whose public keys are being certified. For example, if an employee is dismissed, it is important that the PKI reflect this by revoking that user's public key or some similar action. Ideally, the PKI would be tightly integrated with the organizations' human resources database. However, this level of integration can be difficult to achieve. It is even more difficult to insure that these changes are reflected in the PKI in a timely manner.

X.500 directory maintenance - *Entrust* relies on X.500 directory services to provide user certificates to verifying parties. This can require a great deal of local X.500 expertise, especially if the X.500 database is normally populated from systems other than the PKI. In some cases, a site's X.500 database had been setup and running without intervention or maintenance for a period of many months. When changes were indicated, the organization discovered that it had lost their X.500 expertise some time earlier.

Emergency access - Situations regularly arise when parties need to sign a document, but they are not in a convenient location to perform this function. In the paper paradigm, this is usually handled through a temporary delegation of authority. In the electronic paradigm, this can be more difficult. A similar situation occurs when an individual holds vital information that is stored in an encrypted format on their workstation. Although the *Entrust* management subsystem can provide emergency access to data, this feature is not designed for use on an everyday basis. Often, users compromise their pass phrases over the telephone to colleagues in order to satisfy these emergency requirements. A better solution to this problem is definitely needed.

Common trust models - It is also necessary for each CA in the PKI to accurately interpret the trust models for each of the cooperating CAs in the network. This is especially important where high-reliance certificates are offered by any of the CAs. The AM/NII team cooperated to develop a common trust model for the entire PKI. However, this may not be an option for other CAs in a given PKI. In addition, this approach may not work as private enterprises are added to the AM/NII PKI.

Other Issues and Impressions

Support for hierarchies - The AM/NII PKI uses cross-certification among its CAs. However, the team has considered how it might accommodate hierarchical certification within the PKI. This is currently thought to be problematic, primarily because of the high level of effort required to verify some certificates in a hierarchical PKI. The team's current preference would be to cross-certify new CAs in the PKI rather than implement a classical PKI hierarchy.

Human factors - Human factors play an important role in a surprising number of PKI operations:

- **Explaining PKI concepts** - It can be difficult to explain some PKI concepts to management and staff who do not have a background in

mathematics or cryptography. This can make the process of obtaining management concurrence on some PKI operations problematic.

- **User training** - Users need to know when to sign or encrypt documents, and they need utilities that make these processes simple and intuitive. Some users may require training, whereas other users may need new applications software.
- **Installation and maintenance** - PKI deployment requires support from knowledgeable staff who can properly install and maintain PKI components, especially at the desktop. Support staff may also need special training to address user questions and concerns, especially for those providing Help Desk services.

Emerging federal PKI - As the federal government embraces PKI technology, it is not clear how the AM/NII PKI might accommodate some of these emerging standards. For example, the current draft Federal PKI Specification [21] is modeled after the GCS-API [22] whereas *Entrust* conforms to the GSS-API [23]. In addition, it is not clear how the AM/NII PKI might accommodate other federal PKI efforts such as that underway by the United States Postal Service [24].

Integration among infrastructures - It is essential that the PKI be integrated within an enterprise's intranet including systems such as an organization's human resources network. However, this may require integration with legacy applications and other dissimilar resources that could be problematic. Another troubling trend is that many sites now have many security infrastructures. Examples include the PKI, the Distributed Computing Environment (DCE) [25], and Windows NT domains. Ideally, each of these security infrastructures would be integrated in a cooperative and complementary fashion. However, this appears to be one of the next substantive challenges in Information Security.

Next Steps

The AM/NII PKI project is proceeding, despite reductions in the original program. Additional work is indicated, depending on the availability of resources and priorities at each site.

Continued deployment - The goal remains to install *Entrust* at each of the AM/NII sites. Remaining sites include Los Alamos National Laboratory (Los Alamos NM), Lockheed Martin Energy Systems (Oak Ridge TN), and the Pantex facility (Amarillo TX).

Wider applicability - The PKI has been successfully used in certain specific applications. Additional work is needed to extend the PKI to other enterprise information systems such as hypertext-based applications using World Wide Web technology. In addition, *Entrust* has not been widely deployed at some sites, simply because the support infrastructure is not in place to support a majority of possible users at those sites.

Application to new problems - The AM/NII team has speculated that the PKI could be extended to address new and different problems. For example, *Entrust* could provide need-to-know separation for classified networks. The PKI could also be more tightly integrated with certain database functions to give users easier access and developers better control over valuable corporate data.

Demonstrate compliance to new standards - Additional work is indicated to demonstrate that the AM/NII PKI could be extended to satisfy certain new perceived standards such as the Federal PKI [21] and the S/MIME [4] messaging standard.

Summary

Security based on public key cryptography is only now becoming viable with the introduction of products that provide PKI services. Still, much of this technology can still be characterized as developmental. Deploying a PKI is based on much more than technology choices and product selection. There are few clear directions in this industry, and some new developments are still expected. Still, there are many advantages to deploying this technology.

About the Authors

T. M. (Tim) Sharick is the manager of the Advanced Technology Center / Open Systems Laboratory at Lawrence Livermore National Laboratory (LLNL) in Livermore, CA. Tim was responsible for much of the AM/NII PKI project and its deployment at LLNL. Tim can be reached through his office at 510-423-3931 or via email as tsharick@llnl.gov.

J. P. (John) Long is a Senior Member of Technical Staff in the Computer Security Department at Sandia National Laboratories in Albuquerque, NM. John designed and manages PKI service at Sandia. John can be reached through his office at 505-845-8622 or via email as jplong@sandia.gov.

B. J. (Brian) Desind is a member of the technical staff at Allied Signal Aerospace, Federal Manufacturing & Technology, Kirtland Area Operations in Albuquerque, NM. Brian and his colleagues developed the PKI applications for the Allied Signal Kansas City Plant. Brian can be reached through his office at 505-844-2987 or via email as bdesind@kcp.com.

V. A. (Vickie) Hamilton is a Senior Member of Technical Staff in the Information Systems Surety Department at Sandia National Laboratories in Albuquerque, NM. Vickie specializes in efficient software implementations of cryptographic algorithms. Vickie can be reached through her office at 505-845-8779 or via email as vahamit@sandia.gov.

B. J. (Brad) Wood is a Senior Member of Technical Staff in the Information Systems Surety Department at Sandia National Laboratories in Albuquerque, NM. Brad was the leader for the AM/NII Security & Intelligent Agents team and specializes in performing information system surety assessments. Brad can be reached through his office at 505-845-8461 or via email as bjwood@sandia.gov.

References

Some references are Uniform Resource Locators (URLs) to documents on the World Wide Web (WWW). URLs are current as of 3/26/97.

- [1] W. Diffie & M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, v. IT-22, n. 6, Nov 1976, pp. 644-654
- [2] Netscape's product information: <http://home.netscape.com/comprod/index.html>
- [3] Microsoft's Web product information: <http://www.microsoft.com/sitebuilder/>
- [4] S/MIME home page: <http://www.rsa.com/rsa/S-MIME/home.html>
- [5] T. Sharick, "AM/NI Security & Intelligent Agents Project, Digital Signatures Sub Project," presentation to AM/NI Security Workshop, Aug 1995, available on the WWW at ftp://saix1130.endo.sandia.gov/AMNI/DFW/PUB_KEY.PPT
- [6] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.
- [7] National Institute of Standards and Technology, NIST FIPS PUB 140-1, "Security Requirements for Cryptographic Modules," U.S. Department of Commerce, January 1994.
- [8] Microsoft CryptoAPI description: <http://www.microsoft.com/intdev/security/capi/cryptapi.htm>
- [9] RSA Certificate Issuing System (CIS) information: <http://www.rsa.com/rsa/PRODUCTS/ssacar96/46b.htm>
- [10] VeriSign home page: <http://www.verisign.com>
- [11] Entrust home page: <http://www.entrust.com>
- [12] MOSS distribution from TIS, Inc.: <ftp://ftp.tis.com/pub/MOSS/README> and <ftp://ftp.tis.com/pub/MOSS/doc>
- [13] MIT PGP distribution Web site: <http://web.mit.edu/network/pgp.html>
- [14] PGP, Inc. home page: <http://www.pgp.com>
- [15] P. Calamera, "DigiSign" *MacTech Magazine*, v. 10, n. 2, Feb 1994, pp. 52-57
- [16] AT&T SecretAgent home page: http://www.att.com/bcs/secure_software/SAssoftware.html
- [17] ITU-T, Recommendation X.509, "Information technology - Open Systems Interconnection - The directory: Authentication framework," International Telecommunications Union, Geneva, Nov 1993
- [18] Shana home page: <http://www.shana.com/>
- [19] Lotus cc:Mail home page: <http://www.ccmil.com/index.htm>
- [20] Eudora home page: <http://www.eudora.com>
- [21] NIST, "PKI Specifications to Support the DOE Travel Manager Program," National Institute of Standards and Technology, Computer Security Division, DRAFT, April 1996
- [22] X/Open, "Generic Cryptographic Services API (GCS-API), Base - Draft 8," X/Open Preliminary Specification, X/Open Company Limited, April 1996
- [23] IETF RFC 1508: "Generic Security Service Application Program Interface," available on the WWW at <ftp://ftp.internic.net/rfc/rfc1508.txt>
- [24] Press release, "Postal Service Leverages Private Sector Expertise to Enable Electronic Commerce Through the Internet," Oct 1996, available on the WWW at <http://www.usps.gov/news/press/96/96108new.htm>
- [25] Distributed Computing Environment (DCE) home page: <http://www.opengroup.org/tech/dce/>