Fast Track Public Key Infrastructure Implementation

By Eric Williams
Information Brokers, Inc.

1309 S Street S.E.
Washington, DC 20020-6925

Abstract: This document outlines some key areas for consideration in implementing Public Key Infrastructure Services on a fast track basis to satisfy deployment and funding constraints. As concerns for data integrity and privacy increase, so to does the desire of large organizations and their offices, for a timely implementation of Public Key Infrastructure, a.k.a. PKI. Outlined in this paper are some issues in implementing a "Web Of Trust" PGP (WOT) PKI model, Vendor Managed PKI (VM-PKI) or Organizationally Managed PKI (OM-PKI) in a 'Fast Track' implementation mode. The reader should at minimum have a grasp of PKI as in D-H/DSS[i]

The issues for large organizations in implementing Public Key Infrastructure (PKI) are many. As concerns for data integrity and privacy increase, so to do the desires of large organizations and their offices, for a timely implementation of PKI. The concerns of the sub-ordinate offices often overtakes the policy and implementation processes of the whole, parent, organization. In order to address these issues organizations have normally opted for one of the following models in PKI implementation:

- Pretty Good Privacy (PGP)
  "Web Of Trust" (WOT)
- Vendor Managed PKI (VM-PKI)
  Central Authority (CCA)
- Organizationally Managed PKI (OM-PKI)
  Hierarchical Authority (HA)

The reasons for choosing either of the three models primarily rests on the ease of implementation with in the organizations messaging architecture and secondarily on the encryption methodology utilized.

Public Key Cryptography

Public Key Cryptography (PKC) came into being about 20 years ago. In 1976 a cryptographer, Whitfield Diffie, together with an electrical engineer, Martin Hellman; discovered **public-key cryptography.** The method developed included a method to exchange a cryptographic key (**cipher**) in a secure fashion, such that the parties in the exchange could then exchange information with each other using the others **public** cipher. The method used to exchange the keys is known as Diffie-Hellman (DH) key exchange, and is still used today. In this discussion PKC I will use the DH key exchange as a base for simplicity.

DH Key Exchange

In standard DH key exchange the two parties generally fix the *base* as a publicly available, often fixed number; e.g. a packet sequence number. The protocol for the exchange has two stages, a key exchange where **A** and **B** negotiate a DH Key (**K**) based on the shared base number (**S**), and a verification stage where they prove to each other that they each know the same **K**.

Diffie-Hellman Key Exchange		
S	a shared base number or secret	
p	a large prime number, where (p-1)/2 is also prime	
R_A	secret random number chosen by A	
R_B	secret random number chosen by B	
h(*x*)	one-way hash of *x*, like SHA1(*x*)[ii]	
Key Exchange		
A		B
$Q_A = S^{(2R_A)}$	☞	
	☜	$Q_B = S^{(2R_B)}$
$K = Q_B^{(2R_A)}$	☢	$K = Q_A^{(2R_B)}$
ABORT *if* K<2	☑	ABORT *if* K<2
Key Verification		
A		B
	☜	V1 = h(h(K))
V2 = h(K)	☞	
ABORT *if* V1 != h(h(K)	☑	ABORT *if* V2 != h(K)

After A and B verify use of the same K, it Is known they used the same S. K can now be used as a mutually-authenticated *session key*[iii]. The beauty of this is that an very small, easily transferred **S** can produce a very large **K**. Also note two messages QB and V1 may be combined in one reply from B. This would results in a short 3 message exchange mutual authentication protocol.

What is PKI?

PKI stands for Public Key Infrastructure. The desired PKI is an electronic data interchange infrastructure which allows the transfer of information that supports methods for the three primary criteria used for commerce transactions:

I-C-A-N
INTEGRITY
CONFIDENTIALITY
AUTHENTICITY
NON-REPUDIATION

INTEGRITY, is the guarantee that the message contents have not been altered from the original contents, sent by the originator.
CONFIDENTIALITY, is the guarantee that the contents of a message are private between the corresponding parties.
AUTHENTICITY, is the assurance that the messages' encoded originator is indeed the bona-fide originator.
NON-REPUDIATION, this is a real area of interest and has been since the standardization of X.400 messaging; it represents the inability of a individual to renege on a transaction after the fact.

This is the essential architecture of a trusted infrastructure in commerce. Although the concept of the PKI has been around for a number of years, only recently has the realization of the PKI come close to realization.

The introduction of Secure Sockets Layer™ protocol, by Netscape™ is a primary example of this. The introduction of this protocol drove advancements in the vendor markets for technologies to deliver authentication services for the commerce community, as well as the average end-user.

The Certificate Authority

This particular area comprises the market we know now today as the Certificate Authority, vendor operated *electronic identity licensing*. What is meant by *electronic identity licensing*? A CA essentially takes existing materials, e.g. drivers license, articles of incorporation, etc.; and uses the voracity of that information to form a basis for trust in your public key. This trust is predicated on the CA's trustworthiness, the CA provides procedures and mechanisms that cause the generation of a *Certificate*. That certificate is signed by the CA using its private key and is used to *sign* your public key, and essentially *certifies* that you generated it. This information is presented publicly by the CA in a directory, for the entity desiring I-C-A-N.

PKI/CA Components

Central Authority: CA's depend on the trust of entities that use them. To establish this level of trust the CA may depend on a hierarchically defined set of CA's.

The Root CA: The most hierarchically superior CA would be considered the *Root CA* of an inverted *tree of trust*. The CA's in this model would also depend on lower and peer levels of *cross certification*. This type of configuration of entities could be developed network wide or within a vendor architecture, however, no matter the overall vendor relationships a *Root CA* would be required.

Certification Agents: These *Certifiers* represent the entity which actually verifies and submits information to the CA on your behalf for signing. This limits the exposure of the CA's public key in the certification process. This enhances the certification security model as a whole as the CA private key should be kept *out-of-band*.

Certificate Directory Services: Because of the self verifying nature of certificates, and in lieu of forcing users to store certificates locally, certificates are usually made available in publicly accessible directories/databases. Typically an X.500 standards based directory service which is designed to communicate with industry PKI management protocols.

Certificate Management Protocols

The move to standardization of PKI architecture and implementation has, as an integral component protocols and procedures that must be used in the management of the Public Key Directory systems. These management processes are governed by the PKI Certificate Management Protocols. The management protocols consist of functions to:

- Root CA initialization
- Subordinate Ca Initialization
- Root CA Key Update
- Certificate Revocation List Production
- Process PKI information requests
- Perform Cross Certification
- End Initialization
- Process Certificate Requests
- Perform Key Updates

These activities are performed for end entities throughout the PKI.

PKI/User Operational Protocols

Specific to the User end entity are the operational protocols used to transport the management protocol information, for these operations some commonly used Internet protocols have been designated. The protocols are:

- LDAP
- HTTP
- FTP

These protocols will see further and more widespread implementation in the near future as transports for certificate management information and controls messages between CA's.

Trust and Management Infrastructures

A recent survey by the Giga Group indicated that the cost to implement a PKI for an organization of 5,000 desktops for e-mail and local disk storage encryption, for the Entrust and Verisign systems. The Entrust system for a five-year total cost of operations, including installation, support and certificate life-cycle management costs, weighed in at $2.8 million ($110/user/year) and Verisign's at 3.8 million ($151/use/year). Entrust sponsored the study as you might guess. Currently there are no industry standards for PKI implementation. However, groups at NIST and the IETF PKIX Working Group have both labored developing harmonized profiles for PKI architecture and operation. The Fast Track to PKI must involve a scalable and interoperable management and operational infrastructure while standard protocol and transaction messaging formats are required e.g. X.509, the existence of these mechanisms may not be sufficient to drive convergence of disparate and incompatible subordinate management frameworks.

PGP and the "Web Of Trust"

The implementation of a PKI using the PGP WOT can often be accomplished in a short time frame. The installation and management of the client system software is usually straight forward and freely available implementations make it easy to bring end-users up to speed and correspond with external entities. The WOT model implies Trust on all correspondence and on the integrity of Key Servers. These Key Servers must be implemented in a vendor independent but non-standardized fashion e.g. anon-FTP[iv] to allow for the accurate exchange and updating of public-keys. Further, integrity must be implemented through the use of signing keys on the public key of a 'trusted' client. This can present a significant administrative overhead, even when the key generation and management licensing costs are low relative to the VM-PKI costs.

Vendor Managed PKI

Using an outside vendor to manage and implement the organization PKI can mitigate the costs and administration burden to the organization. However the costs for the services of the vendor may offset these savings. Vendor solutions have another feature in that they are nominally implemented using industry standard or *de-facto* standard techniques for key generation, e.g. RSA; and internationally standardized authentication and integrity mechanisms such as X.509 key certificates. These certificates allow the VM-PKI to participate for compliant entities worldwide in a vendor independent way. One other benefit is that the time to implementation for VM-PKI is quick due to the ready availability of software that supports the messaging capabilities of organization, for example Netscape supports S/MIME.

Organizationally Managed/PKI

The organization to be managed may also choose to implement a vendor based solution to mitigate the operational costs for the certificate life-cycle management. This model may prove the most beneficial for the end entities involved. The major vendor is freed to innovate toward simpler management infrastructure, the end entities benefit due to the inside knowledge and cost mitigation. Typically, these types of implementations utilize the same technology as the vendor managed solutions, e.g. X.509, X.500 DSAs etc.

Conclusion

The implementation and management of a viable Public Key Infrastructure has a will have a significant impact on the way we conduct business in the future. With increases in identity theft and the increasing use of electronic debit based cash flows, the role of the CA and PKI will begin to transcend mere convenience to one of necessity. If fact the early introduction of PKI technology may well help mitigate some of the impact of identification crisis's that may arise as the next millennium dawns.

Eric D. Williams

Mr. Eric Williams, President and Principal Consultant of Information Brokers, Inc., has been recognized as a leader in implementing open system solutions. Mr. Williams' projects and technological initiatives have been featured in government and private industry technology forums. Mr. Williams is the current Chairman of the Open System Implementor's Workshop protocol Convergence Sub-committee. Mr. Williams has been quoted in the industry press. In addition, Mr. Williams is consulted by leading industry market research firms to determine major industry trends.

Mr. Williams has intimate knowledge concerning the implementation and integration of Open Systems Interconnection (OSI) technology. OSI is a set of internationally recognized, vendor independent communications standards, and over 15 years experience concerning the development, dynamics and implementation of the Internet Protocol Suite (IPS).

Within the Open System Implementers Workshop (OIW), Mr. Williams is intimately involved with the development of profiles and protocol implementation conformance statements (used internationally for procurement and standardization) specifically concerning the convergence of IPS and OSI technologies, Mr. Williams is uniquely qualified to plan and implement solutions involving OSI, and IPS technology.

Mr. Williams' philosophy is that the IPS and OSI protocol suites will coexist into the near future and eventually converge into a common set of protocols. Various standards organizations involved in the standards process are holding discussions on how these protocols can converge. Mr. Williams is consulted for these discussions and believes discussions should continue and accelerate until there is one interoperable high function protocol suite that delivers full functionality and interoperability. Mr. Williams has stimulated and codified dialog within the OSI and IPS communities. His efforts are aimed at convergence of profiling and IETF standard development paradigms. This is seen as an aid to the procurement of IPS and OSI/IPS converged products by Government and Private Industry procurement entities.

Mr. Williams specializes in technology that provides interoperability in today's world where IPS and OSI are separate. Mr. Williams implements technology providing "application gateways" between IPS and OSI applications. Mr. Williams also implements technology allowing OSI applications to run on top of the Transmission Control Protocol (TCP) layer of the IPS.

Mr. Williams has extensive experience in the implementation of current leading edge IPS technologies including HTML publishing (home page design et. al.), Mobile / Wireless E-Mail and LAN communications, ISDN implementation, Information Kiosk design and implementation, World Wide Web Database Search engines, Video Teleconferencing, , WWW Browsers such as Netscape™ and IPS Security. Mr. Williams also assisted in the development of the Secure Sockets Layer (SSL) implemented by Netscape™ Servers and Clients.

[i] Diffie-Hellman Key Exchange / Digital Signature Standard

[ii] SHA represents Secure Hash Algorithm 1, a hashing algorithm is an mathematical function which: given a unique input of arbitrary size, produces a unique

output of a fixed length. A one-way hash function can not be reversed to determine the input. SHA1 is a one-way hash function.

[iii] A session key is a cipher which is used in data transfer for a limited time, a session.

[iv] Anonymous FTP