Global Information Assurance Certification Paper

Jennifer Main Cathcart

GSEC version 1.4b

Option 1

February 22, 2004

Building Trust for Public Key Infrastructure

Identity management is a common problem today. The Federal Trade Commision received over 500,000 consumer fraud and identity theft complaints in 2003. Even teenagers can change their identity, using fake ids to buy alcohol. So, how do you know whom to trust online?

One of the services Public Key Infrastructure provides is authentication. Certificates issued by the Certificate Authority (CA) bind keys to a person's identity, and the users in the architecture trust that these certificates are valid. Standing up the CA is a crucial piece, and is deceptively complicated. Installing and configuring the actual hardware and software for the Root CA can be done in an afternoon. But, developing the policies and procedures leading up to that installation is a large, complex undertaking.

1.0 Intro

Public Key Infrastructure has been a hot topic in the last few years. Some companies were less interested in it for the ability to provide authentication, data integrity, confidentiality and non-repudiation, and more for the cool factor of the peripheral products such as smart cards or biometric devices. Many PKI implementations never got off the ground. One of the most difficult parts of the implementation is designing and planning the Certificate Authority architecture.

1.1. What is PKI?

Public Key Infrastructure is the policies, processes, platforms, software and workstations used for creating, managing, using, and revoking public-private key pairs and their certificates. PKI is not a single product, but an infrastructure that enables other products to use its capabilities.

1.2. What capabilities does PKI provide?

PKI provides several capabilities to the applications that use it.

1.2.1. Authentication

Authentication ensures that the parties in a transaction are who they claim to be. PKI can provide this through digital signature certificate. The digital signature certificate is associated with the subscribers private key, which only the subscriber holds.

1.2.2. Data Integrity

Data integrity is the assurance that an electronic transaction has not been altered, either intentionally or unintentionally, in any way. PKI can provide this with the digital signature function. When a message is signed by a sender's private key, a hash value is created, which is a unique "fingerprint" of the message. If any part of the message is altered, even just one character, this hash value changes. The recipient of the message can validate this hash using the sender's public key, and verify that no alterations have been made.

1.2.3. Confidentiality

Confidentiality is the assurance that a transaction can only be viewed by the party for which it was intended. Confidentiality, using encryption with a recipient's public key, can be used for both email messages and Internet traffic. The encrypted message can then only be decrypted using the recipient's private key.

1.2.4. Non-Repudiation

Information Management Forum defines non-repudiation as follows: "Non-repudiation ensures that strong and substantial evidence is available to the sender of the message that the message has been delivered, and to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the message." (2000).

2.0 Designing Trust

PKI is based on the concept that a set of public and private keys can be used to create the same type of trust in a transaction that paper-based things like signatures and identification cards do.

2.1. Trust

"trust (trŭst) *n.* Firm reliance on the integrity, ability, or character of a person or thing." (Webster.com)

Much of the work that is done by organizations today is done electronically. How do organizations trust that the data they receive or send is accurate and the people who are involved in transactions are who they say they are?

2.2. Who needs trust?

There are several groups in an organization that are involved in creating and using trust relationships.

2.2.1. Relying parties

Relying parties are the entities that rely on the trust of the information or identity. In an email transaction, it is the recipient of the signed email. In an e-commerce transaction, it is the vendor that is trusting that the credit card belongs to the person making the purchase. But, it can also be the purchaser, relying that the website is actually the site the purchaser intended to visit.

2.2.2. Subscribers

Subscribers are the entities receiving and using credentials, in the form of PKI certificates, which prove that they are who they say they are. A subscriber can be the sender of the email or the purchaser of the goods. Subscribers can also be devices. Certificates could be issued to a web server for a bank, so that users can verify they are not sharing account information with an organization they don't know.

2.2.3. Certificate Authorities

Webopia.com defines Certificate Authorities as "A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be." The CA also manages certificates, by maintaining status information of the certificates it has issued. The CA publishes a directory of valid certificates. This gives relying parties a location to find subscribers' public keys for encryption and authentication. For certificates that have been revoked, the CA publishes a certificate revocation list (CRL). CAs need to also have information on all certificates ever issued archived and retrievable.

2.2.4. Different types of trust

An organizations needs to look at the types of trust that would be appropriate for the organization's needs. Size of the organization, sensitivity of the data that needs protection, and even the user community need to be taken into consideration.

2.2.4.1. Direct Trust

An Entrust White Paper on trust states "Direct Trust refers to a situation in which two individuals have established a trusting relationship between themselves… direct trust is predicated on the existence of a personal relationship prior to exchanging secure information."

This is the type of trust with which most people are familiar. When one receives an email from a friend, there is no thought about whether the sender actually wrote to invite the recipient to lunch. An email from a manager containing instructions for a work assignment would not be questioned. This type of trust is appropriate for much of the electronic correspondence that happens on a day-to-day level. But, more and more, businesses are using electronic transactions that require trust between parties that may not have ever met. And, in order to satisfy legal requirements, these transactions may need to have an assurance that they took place exactly as the parties believe they did.

2.2.4.2. Third Party Trust

An Entrust White Paper on trust states:

> Third-party trust refers to a situation in which two individuals implicitly trust each other even though they have not previously established a personal relationship. In this situation, two individuals implicitly trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the two people. (2000)

2.2.5. Trust models

"Security is a chain; it's only as strong as the weakest link" (Ellison, C., and B. Schneier, 2000). The relying parties have to be able to follow the "chain of trust" to a point in which the relying party has trust.

Trust models show the methods by which users receive certificates and rely on the presented certificates during transactions with other users. These are based on the two types of trust.

2.2.5.1. Web of Trust

PGP (Pretty Good Privacy) is a web of trust model. This is based on direct trust, as users themselves sign each other's keys.

Alice receives an email from Fred. Alice doesn't know Fred, but his key is signed by Bob, whom she knows and trusts. Alice can then trust Fred's key.

This model would obviously have some problems scaling to larger organizations. But, it does work well in smaller organizations where everyone knows each other. It is also works well as a catalyst for social interaction in some circles, as in key signing parties.

2.2.5.2. Single Point

In this model, a certificate authority directly issues and signs certificates for the community's users' keys to provide trust. All of the users in this community can trust each other, because they are all working under the policies and practices of that particular CA.

Bob and Alice work for the same organization but have never met. They both received certificates for the organization's single CA. Bob sends Alice and email. Alice can view Bob's certificate, verify that it is signed by the same CA as hers, and trust Bob's certificate.

This model can use Registration Authorities in order to help it scale better to larger organizations. Registrations Authorities can be responsible for one or more functions: registration of subscribers, verifying identity, approval of certificate applications, initiating revocations.

2.2.5.3. Hierarchical

Most large implementations of PKI use some form of the hierarchical model. A root certificate authority issues and signs the certificates for the CAs below it. Those CAs can issue and sign certificates for sub CAs, or subscribers. Registration Authorities can be added for even more scalability

Bob and Alice work for the same organization but have never met. They are in different divisions, and received certificates from the CAs of their respective divisions. Bob sends Alice and email. If Alice views Bob's certificate, she sees that it was signed by a different CA as hers. But, she can view that CAs certificate, and see that it was signed by the same root CA as hers. Therefore, she can trust Bob's certificate.

2.3. Trust and Risk

"According to the X.509 definition of trust, the risk of that the key-holder might fail to behave as expected naturally attaches to the relying party" (Boeyen S., 1997).

This “use at your own risk” philosophy means that, while the organization that provides the certificates has created them for the purposes of authentication, data integrity, confidentiality, and non-repudiation, it is not responsible if these certificates being used in a fraudulent manner.

So, why would we trust these certificates? What can the organization do to define the level of trust that should be placed in these certificates?

3.0 Documenting Trust

When standing up a CA architecture, an organization should take great care in defining and documenting the policies that govern this architecture and the processes followed by the CA architecture and its subscribers.

3.1. Certificate Policy

“Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements” (Chokhani, S. et al, 2003). In other words, the CP is a security policy that is an overview of what the Certificate Authority can do. It does not state specifically how this is carried out. This will be the responsibility of the Certificate Practice Statement.

The certificate policy has a number of uses, other than to set the policy. It will be referenced by the Certificate Practice Statement. It will also be used to by other CAs for review before cross-certification. It will help auditors structure their auditing procedure.

3.1.1. Types of CPs

There are two main types of CPs. One is defines certificates use in a particular community. The other defines certificate use for a particular application.

3.1.1.1. Community

This defines the policies for the community of users. This could be the parties that will be subscribers, as well as relying parties. The community could be defined as a work group, such as a division of a company, or a location, such as a geographic area.

3.1.1.2. Usage

These “CPs identify a set of applications or uses for certificates and say that these applications or uses require a certain level of security.” (Chokhani, S. et al, 2003) For example, a CP of this type could define policies for encryption or signing certificates.

3.1.2. Assurance levels

The policy needs to state the level of assurance the issued certificates are expected to provide. The level of the assurance should match the sensitivity and value of the information it is used to protect and verify. A low assurance certificate would be used for low risk transactions. Higher assurance for sensitive data requires tighter controls on all policies and procedures.

3.1.3. Object Identifiers (OIDs)

There can be multiple CP used by a single CA. The certificates that this CA issues need to contain a reference to the applicable CP. This is done in the Object Identifiers. An OID is string of numbers that identifies an object for the certificate, such as an algorithm or a CP.

3.1.4. Audit

Audits provide the assurances that the policies and practices are being followed correctly. The CP should outline how often audits are performed, who is responsible for performing them, and which processes need to be reviewed.

3.2. Certification Practice Statement

“Certification Practice Statement (CPS) - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.” (Chokhani, S. et al, 2003). This outlines how the Certificate Authority does its job.

The CPS needs to take into consideration a number of things in order to provide a precise definition of how the Certificate Authority works.

3.2.1. How the CA will verify identity

An important part of the CPS is how the CA will verify identity. For a certificate with a low assurance, simply giving your name and email address may be enough to get a certificate. Several commercial vendors provide such certificates, purchased over the Internet, for a nominal fee. These vendors also will provide, at additional cost, certificates with a higher assurance. Subscribers may be required to have forms notarized, and show one or more forms of identification. The forms of identification can also provide higher assurance, with

a work ID providing less than a driver's license, and a military ID and a fingerprint matched to a database providing even more.

3.2.2. How the subscribers will receive the certificates

There are several different methods a CA can issue certificates to the user. They can be sent over the Internet. A subscriber can visit a dedicated workstation directly connected to the CA.

3.2.3. How the users will store certificates

For software certificates, storing on a hard drive or floppy disk may be enough. There are plenty of hardware tokens on the market that can be used to store certificates, as well, such as smartcards and USB tokens. Servers also have the option to store their certificates on the server, or on a separate hardware security module.

3.2.4. Certificate lifetimes

The CPS should not provide a certificate expiration date that is just based on the CA vendor's usual one or three year lifetimes. The duration of life of the certificate needs to take into consideration the length of time the user will need it.. Also, a key "…has a theft lifetime, as a function of the vulnerability of the subsystem storing it, the rate of physical and network exposure, attractiveness of the key to an attacker, etc. From these, one can compute the probability of loss of key as a function of time and usage." (Ellison, C., and B. Schneier, 2000).

3.2.5. Certificate Validation

Basic certificate checking involves just viewing the certificate to see if the dates are valid and it is issued to the person who is using it. Further checking should show that the trust chain is one that the recipient is a member of. The CPS can give the location of the CRL, which is used to confirm the certificates have not been revoked.

3.2.6. Key Archival and Recovery Process

Keys can be archived in case of loss or damage. However, if a second copy of the signature key is archived, then there is the potential for that key to be used fraudulently. Backing up an encryption key is a better idea, as the user may need to retrieve it. The organization itself may want to include provisions for others to recover the key, as well. In cases where files may need to be decrypted without the subscriber's permission, a CPS should provide very clear guidance that has been cleared through legal experts.

4.0 Summary

As organizations rely more on electronic transactions, organizations will need more ways to secure those transactions. PKI is one of the layers of protection that can be used to make an organization more secure. But, like any other tool, it has to be used properly in order to work. Organizations must take a look at what their needs are, and not try to fit into a vendor's solution. An organization must define trust for the users of its PKI, and to provide clear policies and procedures for the use of its certificates.

References

Boeyen S., “Certificate Policies and Certification Practice Statements”, Entrust White Paper, February 1997, v 1.0, URL: http://www.entrust.com/resources/download.cfm/21108/cps.pdf (February 8, 2004)

Boeyen S., and T. Moses, “Trust Management in the Public-Key Infrastructure”, Entrust White Paper, URL: http://www.entrust.com/resources/download.cfm/21126/trustmodels.pdf (February 8, 2004)

“Certificate Authority”. Webopedia.com, URL: http://www.webopedia.com/TERM/C/Certificate_Authority.html (February 20, 2004)

Chokhani, S. et al. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, November 2003 URL: http://www.ietf.org/rfc/rfc3647.txt (February 8, 2004)

“The Concept of Trust in Network Security”, Entrust White Paper, v 1.2, August 2000,URL: http://www.entrust.com/resources/pdf/trust.pdf (February 8, 2004)

“Digital Signature Guidelines”, Information Security Committee Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association, August 1, 1996, URL: http://www.abanet.org/scitech/ec/isc/dsg.pdf (February 10, 2004)

Ellison, C., and B. Schneier. “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure” Computer Security Journal, v 16, n 1, 2000, pp. 1-7 URL: http://www.schneier.com/paper-pki.html (February 10, 2004)

Gerck, E., “Overview of Certification Systems: x.509, PKIX, CA, PGP, & SKIP”. MCG web site, 2000, URL: http://mcg.org.br/cert.htm (February 8, 2004)

Housley, R., and T. Polk. *Planning for PKI.* New York: Wiley Computer Publishing, 2001.

“Message Authentication, Integrity, and Non-repudiation from Paper to PKI”, Information Management Forum, Canada, Draft. March 14, 2000 http://www.imforumgi.gc.ca/new_docs/authentic_e.pdf (February 7, 2004)

Moses T., “PKI trust models.”, IT University of Copenhagen, Courses, updated February 20, 2004, URL: http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf (February 20, 2004)

“National and State Trends in Fraud & Identity Theft January-December 2003”, Federal Trade Commission, January 22, 2004. consumer.gov URL: http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf (February 22, 2004)

Perlman, R., “An Overview of PKI Trust Models”, IEEE Network, November/December 1999, Computer Network and Protocol Testing Laboratory, URL: http://netlab.cs.tsinghua.edu.cn/~xuke/paperlist/An%20overview%20of%20PKI%20trust%20models.pdf (February 10, 2004)

“PKI Assessment Guidelines”, Information Security Committee Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association, draft v 0.30, June 18, 2001, URL: http://www.abanet.org/scitech/ec/isc/pag/pag.html (February 10, 2004)

“PKI Model Certificate Policy, A White Paper”, NECCC E-Sign Interoperability Work Group, Dec 2001, URL: http://www.sos.state.az.us/pa/ec3/PKI_Model_ED.pdf (February 7, 2004)

The Secure Electronic Environment project. “S.E.E. PKI: Paper 4 - PKI Trust Models.” New Zealand E-government Programme, URL: http://www.e-government.govt.nz/docs/see-pki-paper-4/ (February 7, 2004)

“Trust”, Webster.com, URL: http://dictionary.reference.com/search?q=trust