July 1997

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PUBLIC KEY INFRASTRUCTURE TECHNOLOGY

As business transactions are automated, information technology security services based on cryptography become essential. Public key cryptography can play an important role in providing needed security services including confidentiality, authentication, digital signatures, and integrity. Public key cryptography uses two electronic keys: a public key and a private key. These keys are mathematically related but the private key cannot be determined from the public key. The public key can be known by anyone while the private key is kept secret by its owner.

As long as there is strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. A Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA). This bulletin describes PKI technology and discusses implementation issues.

Basic Components of a PKI

Public Key Certificate - An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity.

Certificate Revocation List (CRL) - A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost or if the owner's name changes.

Certification Authority (CA) - A trusted entity that issues and revokes public key certificates and certificate revocation lists.

Registration Authority (RA) - An entity that is trusted by the CA to register or vouch for the identity of users to a CA.

Certificate Repository - An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to repositories.

Certificate User - An entity that uses certificates to know, with certainty, the public key of another entity.

Digital Signatures and PKI

The widespread use of PKI technology to support digital signatures can help increase confidence of electronic transactions. For example, the use of a digital signature allows a seller to prove that goods or services were requested by a buyer and therefore demand payment. The use of a PKI allows parties without prior knowledge of each other to engage in verifiable transactions.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, Room 562, Building 820, Gaithersburg, MD 20899, telephone (301) 975-2817. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since December 1995:

- *An Introduction to Role-Based Access Control,* December 1995
- *Human/Computer Interface Security Issues,* February 1996
- *Millennium Rollover: The Year 2000 Problem,* March 1996
- *Guidance on the Selection of Low Level Assurance Evaluated Products,* April 1996
- *The World Wide Web: Managing Security Risks,* May 1996
- *Information Security Policies for Changing Information Technology Environments,* June 1996
- *Implementation Issues for Cryptography,* August 1996
- *Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems,* October 1996
- *Federal Computer Incident Response Capability (FEDCIRC),* November 1996
- *Security Issues for Telecommuting,* January 1997
- *Advanced Encryption Standard,* February 1997
- *Audit Trails,* March 1997
- *Security Considerations in Computer Support and Operations,* April 1997

For example, a buyer interested in purchasing widgets for company A electronically would need to obtain a public key certificate from a Certification Authority (CA). In one possible scenario, the buyer would generate a public-private key pair, provide a Registration Authority (RA) with a valid photo-id, and ask for a certificate. The RA would verify the buyer's identity based on the photo-id and vouch for the identity of the buyer to a CA, who would then issue the certificate.

The newly certified buyer can now sign electronic purchase orders for widgets. The widget vendor receiving the purchase order can obtain the buyer's certificate and the certificate revocation list (CRL) for the CA that issued the buyer's certificate, check that the certificate has not been revoked, and verify the buyer's signature. By verifying the validity of the certificate, the vendor ensures receipt of a valid public key for the buyer; by verifying the signature on the purchase order, the vendor ensures the order was not altered after the buyer issued it.

Once the validity of the certificate and the signature are established, the vendor can ship the requested widgets to company A with the knowledge that their buyer ordered the widgets. This transaction can occur without any prior business relationships between the buyer and the seller. Potentially, a user's private-public key pair can be used for multiple applications. For example, the same key used to sign the purchase order could be used by the buyer to authenticate an electronic payment to the vendor through the buyer's bank.

Most of the processing in the above example can occur automatically depending of the application. After obtaining a certificate, perhaps a click on an icon is all it takes for a user to sign a message. Similarly, the verification process on the receiver's end would occur as a message is received without requiring much intervention from the person receiving the message.

Confidentiality and PKI

A PKI could also support confidentiality services, using a public-private key pair that is different from the one used for signing. In this case, users need to obtain a separate certificate for the confidentiality public key. To send an encrypted message, a user could obtain the recipient's confidentiality certificate from a certificate repository and verify that it is valid. Then the sender can encrypt the message using the public key. Only the recipient, in possession of the private key, will be able to decrypt the message.

Certificates

Although there have been several proposed formats for public key certificates, most certificates available today are based on an international standard (ITU-T X.509 version 3). This standard defines a certificate structure that includes several optional extensions. The use of X.509v3 certificates is important because it provides interoperability between PKI components. Also, the standard's defined extensions offer flexibility to support specific business needs.

PKI Architectures

A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a network. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate. The National Institute of Standards and Technology (NIST) has developed a hybrid architecture specification based on both a hierarchical and a network architecture model in the document, *Public Key Infrastructure (PKI) Technical Specifications (Version 2.3): Part C - Concept of Operations.*

Implementation Issues

Many issues must be considered when developing and using PKI technology. Some of these important issues are discussed below.

Interoperability

To be useful in a global sense, PKI components need to interoperate regardless of the source of the equipment and the software

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

involved. As part of its efforts to further the development of PKI technology, NIST has produced a Minimum Interoperability Specification of PKI Components [MISPC]. The MISPC was produced in cooperation with ten industry partners through Cooperative Research and Development Agreements (CRADAs) and provides a basis for interoperable PKI components from different vendors. The goal of this specification is to further interoperability among heterogeneous public key certificate management systems, thus providing security services to users in large communities.

The MISPC specifies a minimal set of features, transactions, and data formats for the various certificate management components that make up a PKI. The specification addresses certificate generation, renewal, and revocation; certificate validation; signature generation and verification; and other related issues.

Security

It is important to consider the integrity and security of the PKI components. The confidence that can be placed on the binding between a public key and its owner depends much on the confidence that can be placed on the system that issued the certificate that binds them. Provisions in the X.509 standard enable the identification of policies that indicate the strength of mechanisms used and the do's and don'ts of certificate handling. The rules expressed by certificate policies are reflected in certification practice statements (CPSs) that detail the operational rules and system features of CAs and other PKI components. By examining the policy associated with a sender's certificate, the recipient of a signed or encrypted message can determine whether the binding between the sender and the sender's key is acceptable and thus accept or reject the message. By examining a CA's CPS, users can determine whether to obtain certificates from it, based on their security requirements. Other CAs can also use the CPS to determine if they want to cross-certify with that CA.

To aid organizations interested in contracting CA services or implementing their own CA, NIST is producing a Security Baseline document. The Baseline should help to establish sound operational practices and provide criteria for evaluating service and equipment offerings that provide appropriate security functionality and system integrity.

Performance

One of the main challenges in the development of PKIs is the handling of revocation information. For very large communities, where the number of revocations at any given time could be large, the propagation of CRLs can prove to be the source of heavy network traffic, high processing loads, and heightened storage requirements. The handling of revocation poses some interesting technical challenges and a number of alternatives to X.509 and CRL processing are being developed.

Advances in PKI Technology

Several organizations are working to develop PKI technology. Included here are some prominent activities. The U.S. Federal Government Information Technology Services (GITS) board has established a Federal PKI Steering Committee to provide guidance to federal agencies regarding the establishment of a Federal PKI (http://gits-sec.dyniet.com/fpki.htm). The Federal PKI Steering Committee sanctions approximately fifty PKI-related pilots throughout the federal government. The Internet Engineering Task Force (IETF) PKIX Working Group (http://www.ietf.cnri.reston.va.us/) and the American National Standards Institute (ANSI) X9F Working Group (http://www.x9.org/) are developing standards based on the use of X.509 v3 certificates. In addition, the OpenGroup's Security Program Group is developing an architecture for PKI (http://www.Rdg.opengroup.org/public/tech/security/pki).

Contact Information

For more detailed information about NIST's PKI Program , see the web site at the following URL: http://csrc.nist.gov/pki/ or contact Donna F. Dodson at 301-975-2921, ddodson@nist.gov.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor @ 301-975-2832.

References

[CONOPS] *Public Key Infrastructure Technical Specification: Part C - Concept of Operations*, William E. Burr. Available from http://csrc.nist.gov/pki.

[COR95] ISO/IEC JTC 1/SC 21, *Technical Corrigendum 2 to ISO/IEC 9594-8 : 1990 & 1993 (1995:E)*, July 1995.

[CSL94-11] NIST CSL Bulletin, *Digital Signature Standard*, November 1994.

[DAM] ISO/IEC JTC 1/SC 21, Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, June 30, 1996.

[MISPC] Minimum Interoperability Specification for PKI Components, W. Burr, D. Dodson, N. Nazario, W.T. Polk, Available from http://csrc.nist.gov/pki.

[PKIX1] Internet Draft, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, R Housley, W. Ford and D. Solo, June 1996. Working draft "in progress" available at: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki-part1-02.txt.

[PKIX3] Internet Draft, *Internet Public Key Infrastructure Part III: Certificate Management Protocols*, S. Farrell, C. Adams and W. Ford, June 1996. working draft "in progress" available at: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki3cmp-00.txt.

[X9.55] Draft American National Standard X9.55-1995, *Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists*, Nov. 11, 1995.

[X9.57] Working Draft American National Standard X9.57-199x, *Public Key Cryptography for the Financial Services Industry: Certificate Management*, June 21, 1996.

Forward and Address Correction

Official Business
Penalty for Private Use $300

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Building 820/562
Gaithersburg, MD 20899

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195