Panel

PUBLIC KEY CERTIFICATE POLICIES

Chair

Noel A. Nazario, NIST
820 West Diamond Avenue, Room 426
Gaithersburg, MD 20899
NNazario@nist.gov

Panelists

Santosh Chokhani, CygnaCom Solutions Inc.
Suite 100 - West
7927 Jones Branch Dr., McLean, VA 22102
chokhani@cygnacom.com

Warwick Ford, VeriSign Inc.
One Alewife Center
Cambridge, MA 02140
wford@verisign.com

Michael J. Jenkins, NSA X32
9800 Savage Rd. Suite 6734
Fort Meade, MD 20755-6734
mjjenki@missi.ncsc.mil

Synopsis

Most current efforts to establish infrastructures that enable use of public key technology to provide data confidentiality, data integrity, and entity authentication are based on the use and management of public key certificates as defined by ITU Recommendation X.509 version 3 [X509]. Public key certificates bind a public key to the identity of the owner of a public-private key pair allowing the receiver of a message to verify the integrity of a message and to authenticate the identity of its originator. In addition, some public-private key pairs can be used to protect the confidentiality of data through various schemes. The certificate format in X.509 version 3 allows the certification authority (CA) issuing a certificate to identify the certificate policy (CP) or policies under which a certificate was granted. Examination of the CP allows the recipient of a signed or encrypted message to determine whether it can trust the certificate to correctly identify the originator of the message.

Another approach to assessing the quality of certificates and certification services is the examination of certification practice statements (CPS). Recent *Digital Signature Guidelines* issued by the Information Security Committee of the Science and Technology Section of the American Bar Association [ABA] define a CPS as "a statement of the practices which a CA employs in issuing certificates". While the CP prescribes the strength of the binding between a certificate and its holder by imposing requirements on the authentication of the holder, the strength of the cryptography, and the operation of the CA, the CPS details how such requirements are actually met by the issuing CA.

A common taxonomy for both CPs and CPSs is presented in the *Certificate Policy and Certification Practice Statement Framework* [CHO]. The use of a common taxonomy for both has caused some confusion as to their purpose and usage, therefore it is important to note that even though the elements may be the same the main distinction is in their specificity and audience. The CP is generally used by the recipient of a signed or encrypted message to determine whether the binding between the certificate holder and the public key on the certificate is strong enough for the application. The information in the CPS is useful to users of certificate management services when selecting a service provider and to CAs making the decision to cross certify other CAs.

This panel will provide an introduction to CPs and CPSs, discuss their similarities and differences, and offer different views on their roles, development, standardization, and use. Specific topics that may be addressed in this panel include:

- X.509 support for certificate policies;
- Current status of standardization efforts related to certificate policies and certification practice statements;
- Federal Government and industry efforts in the area; and
- Examples of certificate policies and certification practice statements.

References

[ABA] American Bar Association, Section of Science & Technology, *Digital Signature Guidelines* (1996) (hereinafter ABA Guidelines). For information on ordering, see: http://www.abanet.org/scitech/home.html.

[CHO] S. Chokhani and W. Ford, "Certificate Policy and Certification Practice Statement Framework," Internet Draft <draft-ietf-pkix-ipki-part4-00.txt>.

[X509] ISO/IEC 9594-8, *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*. Also published as ITU-T X.509 Recommendation. For X.509 v3 certificates, see edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied.

Note: For additional material related to this session visit http://csrc.nist.gov/pki.