Workshop for the Development of a Federal Key Management Standard

Background:

The explosion in the use of electronic commerce in recent years has led to the need for well-established schemes that can provide data integrity and confidentiality services. Symmetric encryption schemes such as Triple DES, defined in Federal Information Processing Standard (FIPS) 46-3, and the Advanced Encryption Standard (AES), which is currently under development, can provide these services. Symmetric key encryption techniques are efficient, and their security requirements are well understood. Furthermore, these schemes have been or will be standardized to facilitate interoperability between systems. However, such schemes require the establishment of a shared secret key in advance. As the number of entities using such a system increases, key establishment and key management become a problem. Public key cryptography offers an attractive solution to this problem.

A key establishment scheme is a cryptographic scheme that establishes keying data for subsequent cryptographic use. Key establishment schemes include both key agreement and key transport schemes. A key agreement scheme is a key establishment scheme in which the keying data established is a function of contributions provided by both parties in a communication in such a way that neither party can predetermine the value of the keying data. A key transport scheme is a key establishment scheme in which the keying data is determined by only one party.

The Federal Government currently has no public key-based standard for the establishment of keys for unclassified applications. Several techniques and classes of algorithms have been proposed. Several of these techniques are applicable to one type of application or environment, but not another. Since the government relies heavily on COTS products, it is imperative that Federal agencies understand which techniques afford appropriate security and can procure suitable products. The government needs key establishment products that afford adequate security for its diverse applications and provide interoperability among the government agencies, between the government and the private sector, and between the U.S. government and the governments of other countries.

In anticipation of the development of a standard for key establishment, NIST requested comments from the public concerning the development of such a standard, and concerning the availability, security, and adequacy of existing standards for public key-based key agreement and exchange (i.e., key establishment). Comments were received recommending the use of RSA, Diffie-Hellman, MQV and elliptic curves, and several comments recommended the adoption of American National Standards Institute (ANSI) X9.42, X9.44 and X9.62.

The following list of techniques for key establishment is proposed for discussion during the workshop:

1. ANSI X9.42, *Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*, defines schemes for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. The Diffie-Hellman key agreement mechanism is a well-understood and widely implemented public key technique that facilitates cost-effective cryptographic key agreement across modern distributed electronic networks such as the Internet. The MQV algorithm is a variation of the Diffie-Hellman algorithm. This standard provides six schemes using Diffie-Hellman and two schemes using MQV.

2. ANSI X9.44, *Key Establishment Using Factoring-Based Public Key Cryptography For The Financial Services Industry*, defines mechanisms for transporting symmetric cryptographic keys (e.g., TDEA or AES keys) using reversible public key cryptography (i.e., using the RSA or Rabin-Williams public key algorithms). Two schemes are defined in this standard.

3. ANSI X9.63, *Key Agreement and Key Transport Using Elliptic Curve Cryptography*, defines a suite of mechanisms based on the elliptic curve analogue of the Diffie-Hellman and MQV mechanisms. Eleven key agreement schemes and two key transport schemes are defined in ANSI X9.63.

4. In 1998, the National Security Agency (NSA) released its Key Exchange Algorithm (KEA) to the public. The KEA is based upon a Diffie-Hellman protocol. Two versions are defined: one version for interactive applications where both parties actively participate in the determination of the shared key, and another version for email (i.e., store-and-forward) applications.

Workshop Objective:

This workshop will focus on the security and interoperability requirements of the Federal government, the key establishment options available, and the planned development of a FIPS that will address those needs. Topics may include:

- The applications and environments for key establishment,
- The schemes for each class of techniques and each environment,
- The minimum key sizes needed,
- The security afforded by each technique,
- Key recovery/key archiving issues,
- Guidance on secure key storage,
- Considerations for a Public key Infrastructure (PKI),
- Scheme specific recommendations/requirements, including domain parameter generation and validation, public key pair generation and validation, key derivation procedures, and random number generation, and
- Communication protocol issues.