DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of a Workshop on Key Management Using Public Key Cryptography

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice of Public Workshop

SUMMARY: The National Institute of Standards and Technology (NIST) announces a workshop to examine public key-based management techniques as specified in ANSI X9.42 (Agreement of Symmetric Keys Using Discrete Logarithm Cryptography), ANSI X9.44 (Key Establishment Using Factoring-Based Public Key Cryptography for the Financial Services Industry), and ANSI X9.63 (Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography). The purpose of the workshop is to review the many options and techniques contained in these standards and to discuss other related issues.

DATES: The Key Management Standard (KMS) Workshop will be held on February 10-11 from 9:00 a.m. to 5:00 p.m.

ADDRESSES: The KMS workshop will be held in the Administration Building (Bldg. 101), National Institute of Standards and Technology, Gaithersburg, Maryland. For planning purposes, advance registration is encouraged. To register, please fax your name, address, telephone, fax and e-mail address to 301-948-1233 (Attn: KMS Workshop) by January 31, 2000. Registration questions should be addressed to Vickie Harris on 301-975-2920. Registration will also be available at the door, space permitting. The workshop will be open to the public and is free of charge.

FOR FURTHER INFORMATION:
Further information may be obtained from the KMS web site at http://www.nist.gov/kms or by contacting Morris Dworkin, National Institute of Standards and Technology, Building 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930; telephone 301-975-2354; Fax 301-948-1233, or email Morris.Dworkin@nist.gov

SUPPLEMENTARY INFORMATION: This work effort is being initiated pursuant to NIST's responsibilities under the Computer Security Act of 1987, the Information Technology Management Reform Act of 1996, Executive Order 13011, and OMB Circular A-130.

The explosion in the use of electronic media to expedite commerce in recent years has led to the need for well-established schemes that can provide such services as data integrity and confidentiality. Symmetric encryption schemes such as Triple DES, as defined in FIPS 46-3, and the Advanced Encryption Standard (AES), which is currently under development, make an attractive choice for the provision of these services. Systems using symmetric 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, the implementation of such schemes requires the establishment of a shared secret key in advance. As the size of a system or the number of entities using a system explodes, key establishment can lead to a key management problem. An attractive solution to this problem is to employ key establishment techniques that employ public key cryptography.

The Federal Government currently has no standard for the establishment of keys for unclassified applications using public key cryptographic methods. A number of techniques have been defined in voluntary consensus industry standards; however, the proliferation of techniques, many with security attributes that have been questioned, has lead to a concern that some techniques may not provide suitable security to meet the needs of the Federal Government and may not promote interoperability between agencies of the government. In anticipation of the development of a standard for key establishment, a Federal Register Notice was published by NIST on May 13, 1997 (Vol. 62, No. 92) requesting 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. Comments were received recommending the use of RSA, Diffie-Hellman, MQV and elliptic curves, and several comments recommended the adoption of ANSI X9.42, X9.44 and X9.62.

This workshop will discuss the security and interoperability requirements of the Federal government, the options available in the above referenced voluntary consensus standards to address those needs, and the planned development of a Federal Information Processing Standard (FIPS) that will address those needs by including the appropriate techniques from the voluntary consensus standards referenced above. As with other FIPS, it is NIST's intention that the proposed standard would be published for public review and comment.

.