FEDERAL GOVERNMENT KEY MANAGEMENT
FOR SENSITIVE UNCLASSIFIED INFORMATION

1 Introduction

Electronic Commerce needs well-established cryptographic 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 key management system or the number of entities using a system grows, the need for key establishment can lead to a key management problem.

A number of techniques have been defined in voluntary consensus industry standards. However, the proliferation of techniques, many with questionable security attributes, has led 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.

The National Institute of Standards and Technology (NIST) held a workshop on February 10-11, 2000 to examine public key-based key establishment techniques that are currently available and to discuss the approach to the development of a Key Management Standard for Federal Government use. A report of the workshop may be found at http://www.nist.gov/kms. The workshop attendees suggested the following approach:

- Prepare a "framework" document that discusses the documents to be developed, their proposed content and includes a timeline of the development process. This document is intended as the framework document.

- The development effort should be divided into multiple parts. The initial effort should be the identification of key establishment schemes, hereafter called the scheme definition document. Other parts could address protocols and other key management considerations.

- The scheme definition document should include Diffie-Hellman, RSA/Rabin Williams and Elliptic Curve techniques as specified in American National Standards Institute (ANSI) X9.42, X9.44 and X9.63.

- At least one key management scheme should be non-patented or royalty-free.

This white paper is intended to serve as the framework document for the development of standards and guidelines for the management of keys for Federal Government sensitive, unclassified applications.

2 Key Management Approach

Key management includes key establishment and the rules and protocols for generating and establishing keys, and the subsequent handling of those keys. This key management effort will be divided into two documents: a scheme definition document and a key management guidance document. Because the documents are interrelated, the efforts will be performed concurrently.

2.1 Scheme Definition Document

Cryptographic keys may be electronically established between parties using either key agreement or key transport schemes. During key agreement, no keys are sent; information is exchanged between the parties that allows key computation. Key agreement schemes use asymmetric (public key) techniques. During key transport, an encrypted key is sent. Key transport schemes use either symmetric or public key techniques.

2.1.1 Content of the Document

A Federal Information Processing Standard (FIPS) or NIST Recommendation will be developed to define the acceptable key establishment schemes. The standard or recommendation will select Diffie-Hellman (D-H) and MQV key agreement schemes from ANSI X9.42, RSA key agreement and key transport schemes from ANSI X9.44, and Elliptic Curve key agreement and key transport schemes from ANSI X9.63. All three ANSI documents are currently in a draft form, but are expected to be adopted by ANSI in the near future. NIST intends to select a subset of the schemes specified in the draft ANSI standards. The scheme definition document will also include a specification for a key wrapping technique, whereby a symmetric key is encrypted using another symmetric key (e.g., an AES key is encrypted by an AES key). In subsequent revisions of the document (e.g., at the five year review cycle), other schemes may be included.

Selection of the schemes will be based on security afforded by the schemes and usefulness in a variety of protocols (e.g., 1-Pass, 2-Pass and 3-Pass protocols).

The scheme definition document will contain information on:

- The security provided by a scheme in terms of the attacks that the scheme can resist,
- Information flow diagrams for illustrative purposes,
- An abstract definition of the schemes (e.g., ASN.1),
- Object Identifiers (OIDs) for the schemes
- Key recovery guidance (i.e., what information must be saved to allow key recovery when required by an application or environment),
- Key confirmation

The scheme definition document will not address communication protocols, nor will there be any requirements to implement key recovery.

2.1.2 Schedule

The scheme document will be incrementally developed by scheme “family.” The RSA key schemes specified in ANSI X9.44 will be studied first because of the wide availability of current products and standards. If resources permit, the D-H schemes specified in ANSI X9.42 will be studied at the same time. A proposed key wrapping scheme will also be made available.
The schedule for the development of the scheme definition document is as follows:

June 2001	Document available for review of the RSA schemes, and possibly of the D-H schemes; public comments will be accepted.
July 2001	Proposed key wrapping scheme available; public comments will be accepted.
October 2001	Workshop to discuss NIST’s selections and plan the next phase of the scheme document development.
Thereafter	Development of an initial NIST Recommendation for the selected RSA schemes, the key wrapping scheme and (possibly) the D-H schemes. Make available for public comment. Continue work on the D-H and MQV schemes defined in ANSI X9.42 Produce another draft document on D-H and MQV Hold a second workshop to discuss progress to date and discuss the final phase? Update the NIST Recommendation to include the D-H and MQV schemes. Make available for public comment. Continue work on the elliptic curve schemes defined in ANSI X9.63. Produce another draft document on elliptic curve techniques Hold a third workshop to discuss progress to date. Update the NIST Recommendation to include the elliptic curve schemes or develop a FIPS to include all recommended schemes. Make available for public comment.

2.2 Key Management Guidance Document

The security and reliability of any process using a cryptographic key is directly dependent on the protection afforded to that key. A NIST Recommendation or NIST Special Publication will be developed to provide guidance to Federal agencies for the life cycle management of cryptographic keys, including the generation, establishment, storage, cryptoperiod, recovery, and destruction of that key. Secret keys and the private key of a public key pair must be protected from disclosure. All keys must be protected from modification, which includes substitution and unauthorized deletion. An entity receiving or establishing a key must have assurance as to who is sending or establishing that key and for what purpose.

2.2.1 Contents

The guidance document will include the following subjects:

- The negotiation of cipher suites (what algorithm will be used for key establishment? for encryption? what key sizes will be used?)
- The generation and distribution of keys used in key transport schemes (including the use of Key Distribution Centers)
- PKI-related issues
- Handling of keys from generation to destruction
- Key entry into cryptographic modules
- Management of security associations
- Cryptoperiods of keys
- Protocol issues
- Interoperability
- Implementation guidance
- Validation and testing
- Assurance (e.g., domain parameter and public key validation, correct implementation)
- Recommended parameters, encoding restrictions, exponent sizes, key sizes
- Accountability
- Key recovery/archiving and backup

2.2.2 Schedule

Summer 2001	Paper/outline available for public review.
October 2001	Workshop to discuss progress (this is the same workshop where the schemes will be discussed).
Thereafter	Continue development of the Recommendation/Special Pub. Provide updated draft documents prior to workshops. Discuss progress at the workshops. Develop the Final draft of the NIST recommendation/Special Pub. Make available for public comment.