U.S. DEPARTMENT OF COMMERCE, Barbara Hackman Franklin, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Foreword

The Federal Information Processing Standards Publication Series of
the National Institute of Standards and Technology (NIST) is the
official series of publications relating to standards and
guidelines adopted and promulgated under the provisions of Section
111(d) of the Federal Property and Administrative Services Act of
1949 as amended by the Computer Security Act of 1987, Public Law
100-235. These mandates have given the Secretary of Commerce and
NIST the responsibilities for improving the utilization and
management of computer and related telecommunications systems in
the Federal Government. The NIST, through its Computer Systems
Laboratory, provides leadership, technical guidance, and
coordination of Government efforts in the development of standards
and guidelines in these areas.

Comments concerning Federal Information Processing Standards
Publications are welcomed and should be addressed to the Director,
Computer Systems Laboratory, National Institute of Standards and
Technology, Gaithersburg, MD 20899.

James H. Burrows, Director
Computer Systems Laboratory

Abstract

This standard specifies a particular selection of options for the
automated distribution of keying material by the Federal Government
when using the protocols of ANSI X9.17. ANSI X9.17 defines
procedures for the manual and automated management of keying
materials and contains a number of options. Systems which are
built to conform to all options of ANSI X9.17 are likely to be
complex and expensive. The selected options specified in this
standard will allow the development of cost effective systems which
will, in addition, increase the likelihood of interoperability.

Key words: ADP security, computer security, cryptography, Federal
Information Processing Standard (FIPS), key management.

Federal Information
Processing Standards Publication 171

1992 April 27

Announcing the Standard for

KEY MANAGEMENT USING ANSI X9.17

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

1. Name of Standard. Key Management Using ANSI X9.17 (FIPS PUB 171).

2. Category of Standard. Computer Security Standard; Cryptography.

3. Explanation. ANSI X9.17-1985, Financial Institution Key Management (Wholesale), is a voluntary industry standard that defines procedures for the manual and automated management of the data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships. This data is known as keying material. ANSI X9.17 specifies the minimum requirements for:

    o   Control of the keying material during its lifetime to
         prevent unauthorized disclosure, modification or
         substitution;

    o   Distribution of the keying material in order to permit
         interoperability between cryptographic equipment or
         facilities;

    o   Ensuring the integrity of keying material during all
         phases of its life, including its generation,
         distribution, storage, entry, use and destruction; and

    o   Recovery in the event of a failure of the key management
         process or when the integrity of the keying material is
         questioned.

ANSI X9.17 utilizes the Data Encryption Standard (DES) to provide key management solutions for a variety of operational environments. As such, ANSI X9.17 contains a number of options. Systems which are built to conform to all options of ANSI X9.17 are likely to be complex and expensive. This document adopts ANSI X9.17-1985 and specifies a particular selection of options for the automated distribution of keying material by the Federal Government using the protocols of ANSI X9.17. Interoperability between systems built to conform to this selection of options will be more likely, and the

cost of building and testing such systems will be reduced.
However, less restrictive implementations may be used as long as
the necessary restrictions can be effected when used for Federal
Government applications.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. U.S. Department of Commerce, National
Institute of Standards and Technology (NIST), Computer Systems
Laboratory.

6. Cross Index.
    a.   FIPS PUB 1-2, Code for Information Interchange, Its
         Representations, Subsets, and Extensions.
    b.   FIPS PUB 46-1, Data Encryption Standard.
    c.   FIPS PUB 81, DES Modes of Operation.
    d.   FIPS PUB 113, Computer Data Authentication.
    e.   FIPS PUB 161, Electronic Data Interchange (EDI).
    f.   ANSI X9.17-1985, Financial Institution Key Management
         (Wholesale).
    g.   ANSI X9.9, Financial Institution Message Authentication
         (Wholesale).
    h.   Federal Information Resources Management Regulations
subpart 201-20.303, Standards, and subpart 201-39.1002, Federal
Standards.

Other FIPS and Federal Standards may be applicable to the
implementation and use of this standard. A list of currently
approved FIPS may be obtained from the National Institute of
Standards and Technology, Computer Systems Laboratory,
Gaithersburg, MD 20899.

7. Objectives. The objective of this standard is to provide an
interoperable key management system when the protocols of ANSI
X9.17 are used, and the same option set is selected. The options
selected in this standard were chosen with regard to the degree of
cryptographic protection that can be provided for the data with
which the keys will be used, as well as a decision to reduce the
complexity and cost of ANSI X9.17 implementations by limiting the
number of options which are implemented and tested.

8. Applicability. This standard shall be used by Federal
departments and agencies when designing, acquiring, implementing
and managing keying material using the manual and automated
procedures of ANSI X9.17. In the future, other key management
methods may be approved by NIST for Federal Government use (e.g.,
public key based key management methods).

In addition, this standard may be adopted and used by non-Federal
Government organizations. Such use is encouraged when it is either
cost effective or provides interoperability for commercial and
private organizations.

9. Applications. This standard, along with ANSI X9.17, provides
a key management system for:

    o   a Point-to-Point environment in which each party to a key

exchange shares a key encrypting key which is used to
distribute other keys between the parties,

o   a Key Distribution Center environment in which each party
shares a key encrypting key with a center who generates
keys for distribution and use between pairs of parties,
and

o   a Key Translation Center environment in which each party
shares a key encrypting key with a center who translates
keys generated by one party which will be distributed to
another party, the ultimate recipient.

10. Implementations. This standard covers key management
implementations which may be in software, hardware, firmware or a
combination thereof. Key management implementations that are
validated by NIST will be considered as complying with this
standard. Information about the key management validation program
can be obtained from the National Institute of Standards and
Technology, Computer Systems Laboratory, Gaithersburg, MD 20899.

11. Specifications. The specifications for Federal Information
Processing Standard (FIPS) 171, Key Management Using ANSI X9.17,
(affixed) are contained in ANSI X9.17-1985, Financial Institution
Key Management (Wholesale), as modified by the technical
specification section of this document.

12. Implementation Schedule. This standard becomes effective
October 30, 1992.

13. Export Control. Certain cryptographic devices and technical
data regarding them are deemed to be defense articles (i.e.,
inherently military in character) and are subject to Federal
Government export controls as specified in Title 22, Code of
Federal Regulations, Parts 120-128. Some exports of cryptographic
modules conforming to this standard and technical data regarding
them must comply with these Federal regulations and be licensed by
the Office of Defense Trade Controls of the U.S. Department of
State. Other exports of cryptographic modules conforming to this
standard and technical data regarding them fall under the licensing
authority of the Bureau of Export Administration of the U.S.
Department of Commerce. The Department of Commerce is responsible
for licensing cryptographic devices used for authentication, access
control, proprietary software, automatic teller machines (ATMs),
and certain devices used in other equipment and software. For
advice concerning which agency has licensing authority for a
particular cryptographic device, please contact the respective
agencies.

14. Patents. Cryptographic devices used to implement this standard
and ANSI X9.17 may be covered by U.S. and foreign patents.

15. Waiver Procedure. Under certain exceptional circumstances, the
heads of Federal departments and agencies may approve waivers to
Federal Information Processing Standards (FIPS). The head of such
agency may redelegate such authority only to a senior official
designated pursuant to Section 3506(b) of Title 44, U.S. Code.

Waivers shall be granted only when:

     a.   compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or

     b.   cause a major adverse financial impact on the operator which is not offset by Governmentwide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Technology Building, Room B-154; Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee of Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.

16. Where to Obtain Copies. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. (Sale of the included specifications document is by arrangement with the American Bankers Association.) When ordering, refer to Federal Information Processing Standards Publication 171 (FIPSPUB171), and title. Payment may be made by check, money order, credit card or NTIS deposit account.

Federal Information
Processing Standard Publication 171

1992 April 27

Specifications for

KEY MANAGEMENT USING ANSI X9.17

INTRODUCTION

ANSI X9.17-1985, Financial Institution Key Management (Wholesale),
is a voluntary standard that utilizes the Data Encryption Standard
(DES) to provide key management solutions for a variety of
operational environments. As such, ANSI X9.17 contains a number of
options. Systems which are built to conform to all options of ANSI
X9.17 are likely to be complex and expensive. This document adopts
ANSI X9.17 and specifies a particular selection of options for the
automated distribution of keying material by the Federal Government
using the protocols of ANSI X9.17. Interoperability between systems
built to conform to this selection of options will be more likely,
and the cost of building and testing such systems will be reduced.
It is assumed that the reader of this standard is familiar with
ANSI X9.17.

OPTIONS SELECTED FOR FEDERAL GOVERNMENT USE

This standard discusses 27 of the options which are provided in
ANSI X9.17. In this section, each option is numbered and listed,
its use in ANSI X9.17 is described, the selection for Federal
Government use is specified along with any other additional
requirements, and a brief justification for the selection is
provided. Underlined bold face type and the use of the word
"shall" are used to indicate mandatory requirements. The use of
the word "should" is used to indicate recommendations.

1   ROLE ASSUMED BY A PARTY TO A KEY EXCHANGE

     USE IN ANSI X9.17:

     Party A is responsible for sending keys to the other party.
     Party B is the receiver of those keys. A party to a key
     exchange may assume the role of either Party A or Party B.
     Implementations may be designed to (1) always assume the role
     of Party A, (2) always assume the role of Party B, or (3)
     assume either role.

     Implementations which assume the role of Party A in the PTP or

CKT environments must be able to generate or otherwise acquire
keys (and optionally an IV) and send the keys (and IV) in a
KSM. Implementations which assume the role of Party A in the
CKD environment requests keys (and an IV) from a CKD (see
Option 23). Implementations which assume the role of Party A
in the CKT or CKD environments must be able to communicate
directly with a CKD or CKT. Implementations which assume the
role of Party B in any of the environments must be able to
receive keys (and an IV) in a KSM.

SELECTION FOR FEDERAL GOVERNMENT USE:

The role(s) which may be assumed by an equipment is optional.
The information management needs of an organization or agency
will in large measure determine the roles to be assumed by the
equipment. Implementations which offer both roles offers
greater flexibility, but is more costly. Implementations
which offer a single role is restricted to that role, and can
only communicate with parties which can assume the opposite
role.

2   RSI FROM PARTY B TO PARTY A

     USE IN ANSI X9.17:

     In the event that a party does not have the capability to
     generate or otherwise acquire keys (and an IV) or it is deemed
     advisable not to do so, an RSI permits that party (assuming
     the role of Party B) to request that another party (assuming
     the role of Party A) generate or otherwise acquire the keys
     (and IV) and send them in a KSM.

     Note that a Party A may also send keys (and an IV) to a Party
     B without receiving an RSI from Party B.

     SELECTION FOR FEDERAL GOVERNMENT USE:

     The implementation and use of RSIs from Party B to Party A is
     optional. There may be applications where Party B will be
     required to let Party A know that keys (and an IV) are needed.
     There may be other applications where Party B may not need to
     request keys, and RSI's will not be used.

3   SVR SUBFIELD ORDERING

     Use in ANSI X9.17:

     When an RSI is sent, it contains an SVR field. One KD is
     implicitly requested. A second KD, an IV, and/or a (*)KK may
     be requested by including subfields in the SVR field (except
     in the CKD environment. The ordering of these subfields is
     unspecified, although an ordering is shown in the examples of
     key field formats.

     SELECTION FOR FEDERAL GOVERNMENT USE:

When the subfields of the SVR field are used, it is mandatory that the ordering of subfields be as follows:

    *KK   (requests key encrypting key pair)

    KD   (requests second data key)

    IV   (requests Initialization Vector)

For example, SVR/*KK.KD.IV requests a *KK, two KDs and an IV. The selection of a fixed ordering simplifies implementation and improves interoperability.

4   EDC FIELD IN THE RSI AND ESM

USE IN ANSI X9.17:

The error detection code (EDC) is a Message Authentication Code (MAC) computed on a message using a fixed, publicly known key. An EDC field is an optional field in RSI and ESM messages. The EDC field may be appended to these messages to aid in the detection of errors missed by network error handling protocols.

Upon receiving an RSI or ESM with an EDC field, a recipient who does not implement the EDC option may choose to either respond with an ESM containing an "O" (option not implemented) in the ERF field, or may simply ignore the EDC field.

SELECTION FOR FEDERAL GOVERNMENT USE

The implementation and use of EDC fields in RSIs and ESMs is mandatory. EDCs provide a simple automated means of detecting errors missed by network error-handling protocols. An EDC is easy to compute using an existing feature of the cryptographic system (i.e., the MAC computation). Since the use of EDCs is mandatory, the recipient of an RSI or ESM with an EDC field must process the field.

The sending of an ESM in response to an ESM with an EDC error is forbidden.

5   GENERATE OR OTHERWISE ACQUIRE KEYS AND AN IV

USE IN ANSI X9.17:

During a key exchange, new keys and IVs may be either generated or otherwise acquired by Party A in the PTP and CKT environments. In the CKD environment, Party A may request keys and IVs from the CKD, who either generates or otherwise acquires them. Alternatively, the CKD may send unsolicited keys and IVs to Party A which have been generated or otherwise acquired.

SELECTION FOR FEDERAL GOVERNMENT USE:

The choice of whether to generate or otherwise acquire keys
and IVs is optional. The generation of keys is the most
sensitive of all COMSEC functions. Any inadequacies in the
implementation of the key generation function or in the
physical security safeguards of that function will seriously
undermine the security of the cryptographic mechanisms. It is
imperative that the physical security measures implemented to
protect the key management facility be designed to restrict
access to both the key generation system and the keys
generated therein. These measures are necessary to prevent
unauthorized disclosure, insertion and deletion of the system
or keys produced by the system. The provisions of ANSI
X9.17-1985 paragraphs 3.2, 3.4.2 and 5.2 should be fully
considered in the design and operation of the key management
facility.

There may be some applications where the generation of keys
may be desirable, and other applications where the
distribution of keys from another source (e.g., a central
authority) may be desirable, depending on the desired
management structure.

6   KEY GENERATION TECHNIQUE

     USE IN ANSI X9.17:

     Cryptographic keys may or may not be generated by each party.
     ANSI X9.17 does not specify the method to be used for key
     generation, but does supply a key generation technique in
     Appendix C which may be used.

     SELECTION FOR FEDERAL GOVERNMENT USE:

     Only NIST approved key generation algorithms (e.g., the
     technique defined in Appendix C of ANSI X9.17) shall be used.
     The generation of keys is the most sensitive of all
     cryptographic functions. Any inadequacies in the
     implementation of the key generation function or in the
     physical security safeguards of that function will seriously
     undermine the integrity of other cryptographic mechanisms.

7   KEY NAMING

     USE IN ANSI X9.17:

     When one or more keys are shared between two parties, the
     standard provides a means for naming the keys. The IDK1
     subfield of a key field may be used to name that key. The
     IDK2 subfield of a key field may be used to name the key
     encrypting key used to encrypt the key transmitted in that
     field. The IDD and IDA fields of a DSM, and the IDD field of
     an RSM to a DSM identify keys to be discontinued.

If one and only one key of a particular type ((*)KK or KD) is
shared between two parties, then that key does not have to be
named. If the key is not named, then the IDK1 and IDK2
subfields are NULL, and the IDA field is omitted.

Keys of different types (i.e., a *KK and a KD) may have the
same name.

Two data keys with the same name may be sent in the same
message. The first data key is to be used for
authentication, and the second is to be used for encryption.

SELECTION FOR FEDERAL GOVERNMENT USE:

It is mandatory that:

o   All keys are named, even if one and only one key of that
      type is shared.

o   All keys of a particular type (i.e., *KK or KD) which
      are shared at any given time between two parties must be
      uniquely named.

o   Key names (i.e., in IDK1, IDK2, IDD, and IDA fields) must
      be used in CSMs whenever keys are sent or referenced,
      even if one and only one key of that type is shared.

o   If an unnamed key is received in a CSM and it is
      permissible to respond to the CSM with an ESM, then an
      ESM must be returned with a "C" (cannot process) in the
      ERF field (see Option 18).

The use of key names, even when one and only one key of a
particular type is shared, simplifies implementations and
operations. The use of key names is a means of eliminating
ambiguities during use and storage of a key, and aids in the
message reconstruction at a later time.

It is also mandatory that:

o   Two KD's within a single KSM must not have the same name.

o   A manually transmitted key must be identified by placing
      the name for that key on the material itself and on the
      package (e.g., envelope) used to provide confidentiality
      protection for the keys. The outer security wrapping
      should not contain this identification.

It is highly recommended that all keys, regardless of type,
which are shared between a communicating pair be uniquely
named. This implies that a key cannot be replaced by a key of
the same name (and type), but must always be deleted by a DSM.
However, it allows all keys, even discontinued and archived
keys, to be easily identified by their name alone.

It is also recommended that a structured and consistent naming
convention be used within a network, department, or agency.
Such a convention may be of great long term benefit in key
management, audit, and in the conduct of investigations.

8   KEY AND FACILITY IDENTIFIER CHARACTER SETS

USE IN ANSI X9.17:

Each facility identifier (e.g., the contents of the ORG, RCV,
IDU, and IDC fields) consists of 4 to 16 characters
(inclusive). Key identifiers (e.g., contained in the IDK1 and
IDK2 subfields and the IDD and IDA fields) consist of up to 16
characters.

The character set for these identifiers has not been precisely
defined, however. Several characters have been defined in the
standard as delimiters or otherwise reserved for special
use. These are: period (.), blank (), solidus (/), open and
close parentheses ("(" and ")"), carriage return (CR) and line
feed (LF). Additionally, the asterisk (*) is used to
designate key encrypting key pairs in the ANSI X9.17 standard,
and it is used to indicate a failed MAC in the ANSI X9.9
standard. While the ANSI X9.17 standard restricts the use of
the period and blank within fields and subfields, and hence,
in key and facility identifiers, there is doubt as to whether
the remaining characters should be allowed in these
identifiers.

SELECTION FOR FEDERAL GOVERNMENT USE:

Three characters in addition to the period and blank are
forbidden in facility and key identifier fields and subfields
because they may cause confusion. These characters are the
asterisk, carriage return, and line feed. The other
characters used for special purposes (i.e., the solidus and
the open and close parentheses) may be used since they do not
cause any confusion. The implementation and use of a
standardized and unambiguous character set will allow greater
interoperability.

9   KEY ENCRYPTING KEY LENGTH

USE IN ANSI X9.17:

The standard permits manual key encrypting keys shared between
two parties to be either single key encrypting keys (KKs) or
key encrypting key pairs (*KKs). Manual keys shared between
a party and a center must be *KKs. In the PTP and CKT
environments, the standard permits two parties to exchange
either KKs or *KKs.

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of *KKs is mandatory for manual key encrypting keys

shared between two parties in the PTP environment, and for new
key encrypting keys exchanged between two parties in the PTP
and CKT environments. The use of KKs is forbidden. The use
of *KKs may:

o   allow for longer cryptoperiods,

o   provide more security,

o   substantially reduce the requirements for operators to
     enter new manual key encrypting keys,

o   reduce the number of errors which occur during the manual
     entry of keys because of the less frequent need to enter
     *KKs, and

o   result in lowered overall communications costs.

10   NOTARIZATION OF KEYS

      USE IN ANSI X9.17:

      In the CKT and CKD environments, the notarization of keys is
      required in RTRs generated by the centers. Notarization is
      also used in the subsequent KSMs. However, in the PTP
      environment, the notarization of keys is optional in KSMs
      generated by Party A.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The implementation and use of notarization in the PTP
      environment is mandatory. Notarization improves security and
      can provide a digital signature capability when properly
      implemented in physically secure modules.

11   SENDING KEY ENCRYPTING KEYS IN A KSM IN THE PTP ENVIRONMENT

      USE IN ANSI X9.17:

      In the PTP environment, Key Service Messages (KSMs) may carry
      an automatically distributed key encrypting key ((*)KK) in
      addition to one or two KDs and possibly an IV. The (*)KKs may
      be used to encrypt KDs in subsequent messages which do not
      contain (*)KKs. Alternatively, systems may be designed which
      never carry (*)KKs in KSMs, but only carry one or two KDs
      and,optionally, an IV.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The sending of a *KK in KSMs in the PTP environment is
      optional.   The sending of a *KK in a KSM and its subsequent
      use in sending KDs in other messages may reduce the use and
      exposure of the manually distributed *KKs. The operational
      needs of an organization will in large measure determine
      whether or not the option is used. Implementations which use

the option will provide greater flexibility.

12   SEND EITHER ONE OR TWO DATA KEYS

      USE IN ANSI X9.17:

      Either one or two data keys (KDs) may be contained in KSM, RFS
      or RTR messages. At least one KD is always present.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The sending of two KDs in a KSM (all environments) or an RTR
      (CKD environment) is optional. Without the option of sending
      two data keys (which is a major feature of the standard),
      equipment will lack the ability to distribute data keys for
      both authentication and encryption within a single key
      exchange. The sending of two KDs in an RFS or RTR (CKT
      environment) is disallowed in accordance with Option 26.

13   SEND ODD PARITY ON KEYS

      USE IN ANSI X9.17:

      The standard requires that all manually transmitted and
      entered plaintext keys have odd parity. The plaintext form
      of automatically transmitted keys may optionally have odd
      parity.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The use of odd parity on the plaintext form of all keys,
      whether manually entered or automatically transmitted, is
      mandatory in order to provide interoperability.

14   SEND INITIALIZATION VECTORS WITH KEYS

      USE IN ANSI X9.17:

      When Party A sends keys in a KSM, an Initialization Vector
      (IV) may also be sent. In a CKD environment, an IV may be
      sent in an RTR message.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The sending of an IV is optional. If an IV is needed for
      encryption and is not reliably transmitted by other means, the
      presence of an IV is necessary. The inclusion of an IV in a
      CSM provides a reliable means of exchanging IVs.

15   ENCRYPTION OF INITIALIZATION VECTORS

      USE IN ANSI X9.17:

When an IV is sent in a KSM, the encryption of the IV is optional.

SELECTION FOR FEDERAL GOVERNMENT USE:

It is mandatory that IVs be encrypted. FIPS 140 requires encrypted IVs for the CBC mode. The encryption of all IVs simplifies implementation and processing, and improves security when IVs are transmitted over unprotected channels.

16   SEND EFFECTIVE DATE OF KEY (EDK) WITH KEYS

USE IN ANSI X9.17:

When Party A sends keys in a KSM or the CKD sends keys to Party A in an RTR, the Effective Date of Key (EDK) field may be used to indicate the date and time of key activation (i.e., the start of the cryptoperiod).

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of the EDK field is optional. The use of the EDK field will permit the exchange of keys prior to their activation. This option may be desired for some applications.

17   USE OF DISCONNECT SERVICE MESSAGES

USE IN ANSI X9.17:

DSMs may be used to disconnect (i.e., delete) one or more keys, and may be used to terminate a keying relationship. The DSMs may be used to protect a party in the event of the compromise of a key or keying material, to terminate a business relationship or simply to reduce the number of keys that must be stored.

When a DSM is sent to request the deletion of keys, the RSM returned to the party which sent the DSM provides an authenticated response which acknowledges the receipt of the instruction to delete the key(s); if errors are detected in the reception of the DSM, an ESM is returned. If the DSM is implemented, the RSM and ESM are required by the standard.

SELECTION FOR FEDERAL GOVERNMENT USE:

The implementation of the ability to both send and receive DSMs is mandatory. It is desirable to have a convenient and reliable automated means to discontinue keys that are no longer needed or may be suspected of compromise. The use of the DSM capability is optional for the sender, i.e., other means may be used to discontinue keys.

18   USE OF THE IDA FIELD IN A DSM IF ONLY ONE DATA KEY IS SHARED

USE IN ANSI X9.17:

If one and only one KD is shared between two parties, then the identity (name) of the key for authenticating a Disconnect Service Message (DSM) may or may not be specified in an IDA field of the DSM.

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of the IDA field in a DSM is mandatory, even if one and only one KD is shared between the two parties. This provides a consistent and interoperable method for generating DSMs.

19   USE "C" AS A GENERAL ERROR CODE IN ESM AND ERS MESSAGES

USE IN ANSI X9.17:

A "C" in the ERF field of ESM and ERS messages is a general error code which may be used when a more specific error code is not appropriate. The "C" indicates an inability to process the previous message. Another ERF code which may be used is the "F" (format error).

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of "C" as a general error code in the ERF field of an ESM and ERS is mandatory when other error codes are not readily applicable.

20   ACTION WHEN A COUNT ERROR IS REPORTED

USE IN ANSI X9.17:

When a CSM (i.e., KSM, RFS, RTR) is received with a count (i.e., CTA, CTB, CTP) less than the recipient's expected (stored) count, the message is rejected and an ESM is returned to the originator of the CSM. In the event of a count error in a KSM in a center environment, Party B returns an ESM to Party A, and Party A sends an ERS to the center. The ESM or ERS includes an indication of a count error, the count received in the related CSM, and the recipient's expected (stored) count. Upon receipt of the ESM or ERS indicating a count error, the counters may be resynchronized by either:

(1)   automatically adjusting the origination count up to the expected count received in the ESM or ERS, or

(2)   replacing (possibly manually) the (*)KK associated with the count in error, thereby also re-initializing the counters.

SELECTION FOR FEDERAL GOVERNMENT USE:

It is mandatory that automatic adjustment of the counters be

attempted at least once upon receipt of an ESM or ERS
reporting a count error in a previously received CSM. In the
event that this first attempt to automatically adjust the
counters does not correct the error, then subsequent attempts
to correct the error may either be (1) to adjust the counters
automatically, or (2) to replace the associated *KK.

If the associated *KK is replaced, and an organization has a
security officer or an individual designated as crypto
custodian, that individual should be notified immediately.

All attempts to resynchronize counters manually should be
logged. The organization responsible for the auditing should
be notified of such attempts.

Automatic resynchronization of counters may eliminate the need
for human intervention (e.g., manual distribution and entry of
new *KKs) and the errors induced by this process.

21   USE "CRLF" AS A CSM FIELD DELIMITER

      USE IN ANSI X9.17:

      Normally, the field delimiter in CSMs is a blank (). In
      order to improve the readability of CSMs displayed on a screen
      or hard copy listing, the field delimiter may be a blank
      followed by a carriage return and line feed (CRLF).

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The use of a "CRLF" as the field delimiter in CSMs is
      forbidden. The use of the "CRLF" may adversely affect
      interoperability. As the standard was originally written, it
      referenced ANSI X9.9-1982 and defined the MAC such that the
      "CRLF" would be edited out before CSM authentication.
      However, when ANSI X9.9-1986 was revised, it required that all
      characters in the CSM be utilized in the authentication
      process. Therefore, the use of "CRLF" is not compatible with
      the use of only a "".

22   LOGGING OF A CSM

      USE IN ANSI X9.17:

      This option is referenced in the standard in the table for
      processing counters. The table indicates that logging is
      mandatory when counts disagree, whereas logging is optional
      when the counts agree. There is no indication of what
      information is to be logged.

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The logging of all CSMs is mandatory. Logging is a prudent
      accounting and control practice.

23   USE OF CENTERS (CKD AND CKT)

      USE IN ANSI X9.17:

      A CKD is used to generate or otherwise acquire keys and IVs
      when a party cannot or may not be allowed to perform this
      process. A CKT is used to translate keys for a party with
      whom the requesting party does not share an appropriate (*)KK
      (i.e., a manually distributed (*)KK if (*)KKs are to be sent,
      otherwise a manually or automatically distributed (*)KK).

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The use of centers is optional. In large networks, the use of
      centers reduces procedural problems and the operational costs
      of manual entry. Centers are used to reduce the operational
      and security problems inherent in the manual distribution of
      large numbers of keys. Their use does not reduce the number
      of keys that must be sent (by whatever means), but provides an
      electronic mechanism that substitutes for costly and
      inefficient manual key distribution (e.g., by a courier
      service).

24   RSI FROM PARTY A TO A CKD

      USE IN ANSI X9.17:

      In the Key Distribution Center (CKD) environment, an RSI
      allows Party A to request that the CKD generate or otherwise
      acquire data keys and IVs and send them to Party A in a
      Response-To-Request (RTR) message.

      Note that the CKD may send the data keys and IVs to Party A
      without receiving an RSI from Party A (i.e., send an
      unsolicited RTR) (see Option 24).

      SELECTION FOR FEDERAL GOVERNMENT USE:

      The use of RSIs from Party A to the CKD is optional. If Party
      A must use a CKD to get keys and IVs when Party A determines
      that they are needed, then the RSI provides an automated
      method of doing so.

25   UNSOLICITED RESPONSE TO REQUEST (RTR) MESSAGES

      USE IN ANSI X9.17:

      In the Key Distribution Center (CKD) environment, a request
      for keys may be initiated by Party A. Alternatively, in an
      unsolicited action, the CKD can send keys to Party A for Party
      A to use in establishing a keying relationship with Party B.
      The CKD sends one or two KD(s) for Party A, and sends the same
      keys as KDU(s) for Party A to forward to Party B. An optional

IV may be included.

The use of the unsolicited RTR provides a centralization of control over key generation and acquisition as well as the timing of key exchanges.

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of unsolicited RTRs is optional. The use of the unsolicited RTR will reduce communications costs by eliminating the use of the RSI from Party A to the CKD and will allow the CKD to control the timing of key exchanges.

26   SEND (*)KK OR KD TO A CKT FOR TRANSLATION

USE IN ANSI X9.17:

In the CKT environment, Party A may generate or otherwise acquire and send one or two KDs in a RFS to a CKT for translation, notarization, and return as one or two KDUs for forwarding to Party B. Alternatively, Party A may generate or otherwise acquire and send a (*)KK in an RFS to a CKT for translation, notarization, and return as a (*)KKU for forwarding to Party B. In the latter case, a KD is also sent in the RFS message which is used only for message authentication of the RFS and the responding RTR message.

SELECTION FOR FEDERAL GOVERNMENT USE:

In the CKT environment, it is mandatory that Party A only send *KKs in an RFS message to a CKT for translation and notarization. The translation of one or two KDs may not be requested. This restriction significantly reduces the load on the CKT since the parties to the exchange may then enter a PTP mode to send KDs.

27   USE OF A COUNT WINDOW

USE IN ANSI X9.17:

In the CKD and CKT environments, it is possible for a recipient to receive CSMs whose counts are out of sequence, yet the MACs in these CSMs indicate that the messages are authentic. A recipient of these CSMs may establish a window which represents a range of reception counter values such that the corresponding CSMs, should they arrive out of sequence, shall be accepted without declaring an error.

Appendix F of ANSI X9.17 describes a method of defining and managing such a window.

SELECTION FOR FEDERAL GOVERNMENT USE:

The use of the window technique described in Appendix F of ANSI X9.17 is mandatory in the CKD and CKT environments. It

is desirable to have a uniform window technique for Federal
Government use. The use of the window technique in Appendix
F of ANSI X9.17 in the CKD and CKT environments will permit
interoperabilty. Note that when the window size is equal to
one, the window technique functions as if no window technique
was present. However, the implemented window technique shall
allow for a window size greater than one to be used.

```
                       TABLE I
         SUMMARY OF OPTIONS AND SELECTIONS: ALL ENVIRONMENTS
```

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
1	8.6.2 8.6.3 8.6.4	Role assumed by a party to a key exchange	Optional	Implementing both roles provides flexibility
2	8.2 8.6.2	RSIs from Party B to Party A	Optional	Implementation provides flexibility
3	Table II	SVR subfield ordering	Defined order is mandatory	Simplifies implementation; improves interoperability
4	7.2.8	EDC in RSIs and ESMs	Mandatory	Automated means of detecting errors
5	8.6.2 5.	Generate or other- wise acquire keys and IVs	Optional	Implementation provides autonomy; no generation or acquisition capability
6	5. 5.3	Key generation technique	As defined in Appendix C	Provides required randomness
7	Table II	Key naming	Mandatory (see Option 6)	Eliminates ambiguities; allows a better journaling capability
8	8.3 8.4 8.5 Table II	Key and facility identifier character sets	Mandated per Option 7	Eliminates ambiguities; improves interoperability
13	Table II	Send odd parity on keys	Mandatory	Improves interoperability

TABLE I (Cont'd).
SUMMARY OF OPTIONS AND SELECTIONS: ALL ENVIRONMENTS

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
14	8.6.2 8.6.3 8.6.4	Send IVs with keys	Optional	Provides a reliable means of transmitting an IV
15	7.2.6	Encrypt IVs	Mandatory	Simplifies implementation since encryption requires encrypted IVs
16	Table II	Send EDKs with keys	Optional	Permits the exchange of keys prior to activation
17	8.2 8.6.4	Use of DSMs	Mandatory	Automated, convenient and reliable means of discontinuing keys
18	Table II	Use of the IDA field in a DSM if only one data key is shared	Mandatory	Provides interoperability
19	Table II	Use "C" as a general error code in an ESM and ERS	Mandatory	Eliminates confusion
20	7.3.3	Action when a count error is reported	Mandatory for one attempt to adjust before sending new keys	Eliminates the need for human intervention

TABLE I (Cont'd).
SUMMARY OF OPTIONS AND SELECTIONS: ALL ENVIRONMENTS

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
21	8.3 8.4 8.5	Use " CRLF" as a field delimiter	Forbidden	Provides interoperability
22	Table I	Logging of CSMs	Mandatory	Prudent accounting and control practice
23	8.1	Use of centers (CKD and CKT)	Optional	Reduces cost; improves security

```
                        TABLE II
       SUMMARY OF OPTIONS AND SELECTIONS: POINT_TO_POINT ENVIRONMENT
```

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
9	8.6.2 8.6.4	Key encrypting key length	Use of *KK is mandatory	Reduces cost; improves security
10	Table II	Notariza-tion of keys	Mandatory	Provides a digital signature capability; improves security
11	8.6.2 Table III	Sending key encrypting keys in KSMs	Optional	Operational flexibility
12	4.3 8.6.2 8.6.3 8.6.4	Send either one or two data keys	Optional	Implementation allows encryption and authentication keys to be sent in the same message

```
                         TABLE III
    SUMMARY OF OPTIONS AND SELECTIONS: KEY DISTRIBUTION CENTER
                        ENVIRONMENT
```

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
12	4.3 8.6.2 8.6.3 8.6.4	Send either one or two data keys	Optional	Implementation allows encryption and authentication keys to be sent in the same message
24	8.2 8.6.3	RSIs from Party A to a CKD	Optional	Automated method of acquiring keys
25	8.6.3	Unsolicited RTR messages	Optional	Reduces communication costs; allows centralized control
27	7.3.3	Use of a count window	Window technique of Appendix F of ANSI X9.17 is mandatory	Reduces costs; provides interoperability

```
                         TABLE IV
      SUMMARY OF OPTIONS AND SELECTIONS: KEY TRANSLATION CENTER
                         ENVIRONMENT
```

Option Number	Section(s) of ANSI X9.17	Description of Option	Federal Government Use	Impact(s)
9	8.6.2 8.6.4	Key encrypting key length	Use of *KK is mandatory	Reduces costs; improves security
26	8.6.4	Send KDs or (*)KKs to a CKT for translation	Mandatory that *KKs be sent	Reduces costs and load on the CKT
27	7.3.3	Use of a count window	Window technique of Appendix F of ANSI X9.17 is mandatory	Reduces costs; provides interoperability

APPENDIX A
ANSI X9.17 INTERPRETATIONS

Ambiguities and inconsistencies have been noted in ANSI X9.17
during the implementation of the standard. The following items
contain interpretations of the standard which have been made. The
requirements for Federal Government use appear in underlined bold
face type.

A.1   SENDING AN ESM IN RESPONSE TO AN RSM SENT IN RESPONSE TO A
       DSM.

       Problem:
       The standard explicitly states that "when an RSM [sent in
       response to a DSM] is received in error, no ESM shall be
       sent, and manual recovery procedures are required". In
       addition, the figures which depict message flow with errors
       do not show an ESM in response to an RSM to a DSM

       However, the description in the processing of an RSM
       contradicts this and implies that an ESM to an RSM to a DSM
       is required. In particular, it states that "If an IDD
       field is present, this RSM is in response to a DSM ... If
       the IDD does not match one of the IDD fields sent in the
       DSM to which this RSM responds, this shall cause processing
       of the RSM to cease and the generation and transmission to
       the originating party of an ESM with an "I" in the ERF
       field. I.e., ERF/I."

       Interpretation
       The first statement is considered to be the appropriate
       action, i.e., an ESM shall not be sent in response to an
       RSM which responds to a DSM. An error found in the RSM to
       a DSM should cause processing of the RSM to cease, and
       manual recovery procedures should be used to resolve the
       discrepancy.

A.2   THE USE OF NAMED AND UNNAMED KEYS

       Problem:
       The standard specifies that a key may be unnamed if it is
       the only key of that type shared between two parties or
       between a party and a center . The standard does not
       forbid naming a key even if it is the only key of that type
       shared. The combination of these two facts implies that if
       one and only one key of a particular type is shared, then
       that key may or may not be named; and that if more than one
       key of a particular type is shared, then all such keys must
       be named.

       In addition, there are numerous statements in the standard
       which specify that the key name need not be used in key
       identifier subfields if it is the only key of that type
       shared.

The following difficulties arise:

o   What is the appropriate action when several
           keys of a particular type are shared (and
           hence named), and a KSM is received containing
           a single unnamed key of the same type?

o   How should a party respond when a single key
           of a particular type is shared, the key is
           unnamed, and a KSM is received containing a
           named key of the same type?

o   If a key of a particular type has a name, but
           it is the only one shared, should the name be
           used in the key identity subfields of a KSM or
           in the IDD or IDA fields of DSMs, and RSMs
           which respond to DSMs?

o   When the standard discusses actions which may
           be taken if the key is the only key of that
           type shared, does this mean that the key is
           the only key of that type that may ever be
           shared (e.g., there is storage for only one
           key of that type), or does it mean that there
           is only one key of that type that is currently
           shared (i.e., more keys may have been shared
           previously or may be shared in the future)?

Interpretation:
The parties to a key exchange must have a prior bi-lateral
agreement to name keys or not to name them. Once such an
agreement is made, a change from naming to not naming (or
the converse) cannot be made without changing the
underlying agreement concerning the keying relationship.
If key(s) are received in violation of this agreement, an
ESM should be returned with a "C" (cannot process) in the
ERF field. In particular, if two parties share one or more
named keys and an unnamed key is received, the recipient
shall return an ESM with a "C" in the ERF field. If two
parties share one unnamed key and a named key is received,
the recipient should return an ESM with a "C" in the ERF
field.

In addition, when keys are named, the names should always
be used. Refer to Option 6.

A.3   DISCONTINUING VERSUS REPLACING KEYS.

Problem:
The standard states that "when a (*)KK is discontinued, all
keys sent encrypted under that (*)KK shall also be
discontinued without being named in the DSM". This may
be implemented by maintaining a linkage between the higher
level (*)KK and the (*)KKs and KDs encrypted by it.
However, when a manually or automatically distributed (*)KK

is replaced by a new (*)KK of the same name, it is not
clear whether or not all other (*)KK's and KD's distributed
(encrypted) by the original (*)KK should be discontinued.

Interpretation:
When a (*)KK is replaced (as opposed to discontinued) then
only that (*)KK shall be affected, and other keys which may
have been encrypted by that (*)KK should not be affected.
A "linkage" shall be made between the new (*)KK and the
keys encrypted by the replaced (*)KK, so that if a
compromise of the replaced (*)KK is later discovered, all
keys encrypted by the replaced (*)KK can easily be
identified and discontinued.

A.4   ARCHIVING OF KEYS

Problem:
Section 3.6.3 discusses the archiving of keys, but does not
state that archiving MUST be done or suggest when it should
be done. However, it is a good business practice to archive
a discontinued key if the key may be needed later. Should
replaced keys also be archived?

Interpretation:
Replacing a key by a new key with the same name
effectively discontinues the original key, and the key
should, therefore, be archived. The archiving of keys in
any system is regarded as good accounting practice. The
transactions may have to be reconstructed at a later date
to verify that the correct action was taken.

A.5   DELAYS BETWEEN THE SENDING OF AN RSM TO A KSM AND THE
       RECEIPT OF A RESPONSE

Problem:
If an RSM is sent in response to a KSM, either an ESM
response is expected or no response is expected. The
standard does not address the time interval to wait until
it is known that the RSM was received successfully.

Interpretation:
This is outside the scope of ANSI X9.17. However, this
problem does not occur if, upon correct receipt of the RSM,
the sender of the KSM immediately sends valid data
protected using the data keys sent in the KSM. Receipt of
that data and its subsequent successful authentication or
decryption provides a positive acknowledgement that the RSM
was received correctly.

A.6   CONFUSION ABOUT THE UNIQUE IDENTIFICATION OF DATA KEYS

Problem:
The standard never explicitly states how keys are to be
uniquely identified. At first, it appears that keys can be
uniquely identified by their sharing party, key identifier,

and key type ((*)KK or KD). However, the standard
explicitly states that "Two data keys with the same name
may be sent in the same message". Unless otherwise
determined by prior agreement, if two KDs are sent in the
same message, the first KD shall be used by the ultimate
recipient for authentication; the second shall be used for
encryption". Therefore, KDs may be identified not only
by the sharing party, key identifier, and type (KD), but
also by a subtype (authentication or encryption).

Interpretation
(*)KKs may be uniquely identified by their sharing party,
key identifier and their type (i.e., key encrypting key).
KDs may be identified by their sharing party, key identity,
their type (data key) and their subtype (data key for
authentication or data key for encryption).

A.7   KD REPLACEMENT CONFUSION

Problem:
When two data keys are sent in the same message, the first
is designated as an authentication key; the second as an
encryption key. If a KSM is received with two KDs having
distinct identifiers, the first KD (say, KDX) is an
authentication key, and the second KD (say, KDY) is an
encryption key. If another KSM is received using the same
two distinct KD identifiers, but the key with identifier
KDY is first and the key with identifier KDX is second, it
is unclear whether the new KDY (an authentication key)
replaces the old KDY (an encryption key), or if this
situation is illegal. The same goes for the replacement of
the old KDX (an authentication key) by the new KDX (an
encryption key).

Interpretation:
The new KDY (an authentication key) replaces the old KDY
(an encryption key), and the new KDX (an encryption key)
replaces the old KDX (an authentication key). Section 6.4
states that "all stored keys of the same type (key
encrypting keys or data keys) with the same name shall be
replaced".

A.8   IMPLICIT DESIGNATION OF THE USE OF A DATA KEY FOR
        AUTHENTICATION OR ENCRYPTION.

Problem:
The standard states that "A data key can be used for either
encryption or authentication but not both, except for a
Cryptographic Service Message". This is interpreted to
mean that this stipulation applies to the entire
cryptoperiod of the key, not just for a single message.
I.e., once a key is used for authentication of one message,
it can never be used as an encryption key, and conversely,
once a key is used as an encryption key, it can never be

used as an authentication key.

The standard does not designate the purpose of a single KD field in a message. However, if an IV accompanies that KD, the KD could be considered to be an encryption key. If the single KD is not accompanied by an IV, the designation as an authentication or encryption key is not known.

Interpretation:
When one KD is sent in a message, the first use of that KD after it is sent in a CSM shall determine its use for the remainder of the key's cryptoperiod unless a bilateral agreement states otherwise.

A.9   TERMINATION OF A KEYING RELATIONSHIP UPON THE RECEIPT OF A
        DSM CONTAINING A NULL IDD FIELD

        Problem:
        The standard indicates that an empty IDD field in a DSM
        means that the entire keying relationship should be
        terminated. However, the standard never explicitly states
        what the entire relationship is.

        Interpretation:
        The keying relationship consists of all manually and
        automatically distributed keys and IVs shared with the
        other party. The keying relationship is terminated (i.e.,
        all keys and IVs are deleted) if the DSM contains either a
        single NULL IDD field, or several IDD fields, one or more
        of which are NULL. Resumption of the keying relationship
        will then require a redistribution of manual keys, or, in
        the case of a center environment, utilization of the center
        to re-establish a keying relationship.

        Note that in generating the RSM to the DSM, the IDD fields
        must be copied from the DSM to the RSM. This is
        interpretated to mean that the fields are copied in the
        order in which they were received in the DSM.

A.10   RECEIPT OF AN RSI WHICH REQUESTS A *KK TO BE SENT WHEN ONLY
        A MANUALLY DISTRIBUTED KK IS SHARED

        Problem:
        If an RSI is received with a *KK in the SVR field, but only
        a single manually distributed KK is shared, there is no
        error identified to return in an ESM. In fact, in Section
        10.7 on processing an RSI message, the SVR field is not
        even checked.

        Interpretation:
        The SVR field of an RSI must be checked for appropriate
        requests, including the presence of a *KK request when only
        a KK is shared, as well as a request for both a KK and a
        *KK. An error code of "C" shall be returned in the ERF
        field of an ESM when an error of this type is detected.

A.11   PROCESSING A MISROUTED CSM

        Problem:
        The standard indicates that if the party identified in the
        RCV field of a received CSM is not the party processing the
        CSM, then the message has been misrouted and shall not be
        processed further. The standard does not discuss the
        handling of this misrouted CSM.

        Interpretation:
        If the originator of the CSM is known, the party processing
        the CSM may notify the originator by manual means, since no
        error code is specifically indicated for this type of
        error, or an ESM may be returned with the general purpose
        error code "C", or the receiver could ignore the received
        message and send no response. If the originator of the CSM
        is not known (e.g., in the context of the cryptographic
        system data base, the communications network, or another
        relationship), the CSM should be disregarded.

A.12   USING AN IV ONLY WITH THE KD WITH WHICH IT WAS SENT

        Problem:
        When an IV is sent in a CSM, it is encrypted by the last
        (or only) KD in the message. No restriction is made
        concerning its use in the encryption of data messages.
        Specifically, the standard does not indicate whether or not
        the IV may be used with KDs other than the one which
        encrypted it in the CSM.

        Interpretation:
        The IV is intended to be used with the KD which encrypted
        it in the CSM. However, this is outside the scope of ANSI
        X9.17.

A.13   PRESENCE OF THE IDK2 SUBFIELD IN THE KD FIELD OF A KSM

        Problem:
        When a (*)KK field is present in a KSM, the KD(s) present
        in that KSM is encrypted by that (*)KK. The IDK2
        subfield is not really necessary in the KD field because
        the key encrypting key is known. However, there is also a
        statement that "If an IDK2 subfield is not present, the
        (*)KK used to decrypt the (*)KK [replace with KD] is the
        only one shared by the message originator and
        recipient". This is confusing when a manually
        distributed (*)KK is shared, since if there is a (*)KK in
        the message, there are at least two (*)KKs to choose from,
        the (*)KK in the message and the manually distributed one.

        Interpretation:
        If a (*)KK is present in the KSM, use that (*)KK to decrypt
        the KD in the field. If no (*)KK is present in the KSM,

but the IDK2 subfield is present in the KD field(s), use
the (*)KK named in the IDK2 subfield to decrypt the KD(s).
If no (*)KK is present in the message and no (*)KK is named
in the IDK2 subfield of the KD field(s), use the only (*)KK
shared by the parties identified in the ORG and RCV fields.
If more than one (*)KK is shared, send an ESM with a "C"
(Cannot process) code in the ERF field.

A.14   PROTECTION OF THE HEADER, MAC FIELD TAG AND THE CLOSING
        PARENTHESIS IN A CSM

        Problem:
        In the CSMs which are authenticated using a MAC (e.g., KSM,
        DSM, RSM), the MAC is computed on the message from the "M"
        in the message class field tag ("MCL") through the space
        prior to the "M" in the MAC field tag ("MAC"). Since the
        CSM header ("CSM("), the MAC field tag ("MAC") and the
        closing parenthesis are outside the authenticated text,
        these characters could be modified without altering the
        MAC.

        Interpretation:
        This is true. Errors in these areas need to be checked by
        the program itself or by the communications routines. If
        the errors are not detected by the communications routines,
        the message could be disregarded.

A.15   VALUE OF THE CTP FIELD IN AN ESM WHEN THE IDENTITY OF THE
        (*)KK USED TO PROTECT A KSM IS NOT KNOWN

        Problem:
        In the Point-to-Point environment, an ESM which responds to
        a KSM requires a CTP field containing the expected
        count. However, there is at least one situation where
        it is necessary to send an ESM in response to a KSM when
        the expected count is not known. This situation occurs when
        the ESM is being sent because the manual (*)KK identified
        by the IDK2 subfield of the (*)KK field (or the KD field if
        the (*)KK field is not present) is not known and hence its
        associated receive count (the expected count) is not
        known.

        Solution:
        Since the count is not known, the count field returned in
        the ESM shall be a null field (i.e., CTP/ with nothing
        after the solidus (slash)).

A.16   IDA FIELD IN A DSM

        Problem:
        The standard does not permit a data encryption key to be
        used for data authentication and vice versa. However,a
        data encryption key is sometimes used in the authentication
        process for CSMs (i.e., ERSs, RFSs, RTRs, KSMs and RSMs).

This occurs in two cases: (1) when two KDs are sent in the same message and (2), when only one KD is sent which may be an encryption key. In the first case, the KDs are combined to produce the authentication key, and in the second case, the KD in the message is used. The KD identified in the IDA field of a DSM is used to authenticate the DSM and the RSM which responds to the DSM. The standard does not specify whether the KD identified in the IDA field should be an authentication key or an encryption key.

Interpretation:
Since encryption keys are used for the authentication of other CSMs, the KD identified in the IDA field may be either an authentication KD or an encryption KD. In fact, if a communicating pair share only an encryption key, there is no authentication key with which to authenticate a DSM. However, when possible, an authentication key rather than an encryption key shall be identified in the IDA field and used to authenticate the DSM.

A.17   MESSAGE AND EVENT LOGGING

Problem:
The standard states that logging is mandatory when the received count in CSMs is not equal to the expected count. Logging is optional when the received and expected counts are equal. The implication is that the log contains something about the event, but the standard does not specify what should be included in the log.

Solution:
The most appropriate information to log would be the CSM itself, the expected count and the time of receipt as a minimum. It would indeed be desirable to log all CSMs, and the Federal Government is in fact required to do so (see Option 22).

A.18   PROCESSING AN EDK FIELD

Problem:
The inclusion of an EDK field in a KSM or RTR is optional. However, if an EDK field is present in a CSM, it is not clear whether the receiver who does not generate an EDK field is required to process the message and field anyway (i.e., may ignore the field), or may return an "Option Not Implemented" error code ("O") in an ESM, if appropriate.

Interpretation:
Since there is no identified method for checking the contents of the EDK field, a party who doesn't send the EDK field may not know how to check a received EDK for acceptability. Ignoring the field would not be in accordance with the originator's request. Therefore it would be preferable that the receiving party return an ESM with a "Cannot Process" or an "Option not implemented"

error code in this case.

A.19   TWO AND THREE LAYER ARCHITECTURES

Problem:
The standard permits two or three layers of keys in its
architecture. However, there are several conflicting
statements regarding the use of these two architectures.

o   "The architecture shall consist
            of either two or three layers of
            keys." This seems to say that
            the two architectures shouldn't
            co-exist in the same
            implementation.

o   "All implementations shall have
            the capability of functioning in
            a two layer architecture."
            This seems to say that an
            implementation with a three layer
            architecture should also be able
            to switch to a two layer "mode".

o   "In a three layer
            architecture,...When no key
            encrypting key is transmitted,
            one or two data keys shall be
            sent and shall be encrypted under
            an automatically distributed key
            encrypting key which has been
            previously exchanged between the
            communicating pair." This
            seems to say that you can't use a
            manually distributed key
            encrypting key to encrypt a data
            key when a three layer
            architecture is implemented,
            i.e., you can't switch to a two
            layer architecture.

Interpretation:
An implementation may use the manually distributed (*)KKs
to encrypt keys to be exchanged irregardless of whether a
two or three layer architecture has been implemented.
However, if a (*)KK is exchanged, only a manually
distributed (*)KK may be used to encrypt that key.

```
                          APPENDIX B
                 ABBREVIATIONS USED IN THIS DOCUMENT


Abbreviation                              Meaning


ANSI                          American National Standards
Institute
ATM                           Automatic Teller Machine
CBC                           Cipher Block Chaining
CRLF             Space, Carriage Return, Line Feed
CKD                           Key Distribution Center
CKT                           Key Translation Center
COMSEC           Communications Security
CR                            Carriage Return
CRLF                          Carriage Return and Line Feed
CSL                           Computer Systems Laboratory
CSM                           Cryptographic Service Message
CTA                           Count "A"
CTB                           Count "B"
CTP                           Count "P"
DES                           Data Encryption Standard
DSM                           Disconnect Service Message
EDC                           Error Detection Code
EDK                           Effective Date of Key
ERF                           Error Field
ERS                           Error Recovery Service Message
ESM                           Error Service Message
FIPS PUBS                     Federal Information Processing
Standards Publications
IDA                           Identity of Key for Authentication
IDC                           Identity of Key Distribution
Center or Key Translation Center
IDD                           Identity of key to be discontinued
IDU                           Identity of Ultimate Recipient
IDK1                          Key Identifier (subfield)
IDK2                          Key Encrypting Key Identifier
(subfield)
IV                            Initialization Vector
KD                            Data Key
KDU                           Notarized Data Key for the
Ultimate Recipient
KK                            Key Encrypting Key
*KK                           Key Encrypting Key Pair
(*)KK                         Key Encrypting Key or Key
Encrypting Key Pair
*KKU                          Notarized Key Encrypting Key Pair
for the Ultimate Recipient
(*)KKU           Notarized Key Encrypting Key or Key Encrypting
                 Key Pair for the Ultimate Recipient
KSM                           Key Service Message
LF                            Line Feed
MAC                           Message Authentication Code
NIST                          National Institute of Standards
and Technology
ORG                           Originator identity
PTP                           Point-to-Point (environment)
RCV                           Receiver (Recipient) identity
```

```
RFS                             Request for Service Message
RSI                             Request Service Initiation Message
RSM                             Response Service Message
RTR                             Response to Request Message
SVR                             Service Request Message
```