Key Management Using ANSI X9.17

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:

- · Control of the keying material during its lifetime to prevent unauthorized disclosure, modification or substitution;
- · Distribution of the keying material in order to permit interoperability between cryptographic equipment or facilities;
- · Ensuring the integrity of keying material during all phases of its life, including its generation, distribution, storage, entry, use and destruction; and
- · 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:

- · 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,
- · 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
- · 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:

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**