FIPS PUB 185 - ESCROWED ENCRYPTION STANDARD

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 185

1994 February 9

U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

CATEGORY: TELECOMMUNICATIONS SECURITY

U.S. DEPARTMENT OF COMMERCE, Ronald H. Brown, Secretary NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Arati Prabhakar, 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 important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal Government. The NIST, through the 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 an encryption/decryption algorithm and a Law Enforcement Access Field (LEAF) creation method which may be implemented in electronic devices and used for protecting government telecommunications when such protection is desired. The algorithm and the LEAF creation method are classified and are referenced, but not specified, in the standard. Electronic

devices implementing this standard may be designed into cryptographic modules which are integrated into data security products and systems for use in data security applications. The LEAF is used in a key escrow system that provides for decryption of telecommunications when access to the telecommunications is lawfully authorized.

Key words: Cryptography, Federal Information Processing Standard, encryption, key escrow system, security.

FIPS PUB 185

Federal Information Processing Standards Publication 185

1994 February 9

Announcing the

Escrowed Encryption Standard (EES)

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.

Name of Standard: Escrowed Encryption Standard (EES).

Category of Standard: Telecommunications Security.

Explanation: This Standard specifies use of a symmetric-key encryption (and decryption) algorithm (SKIPJACK) and a Law Enforcement Access Field (LEAF) creation method (one part of a key escrow system) which provides for decryption of encrypted telecommunications when interception of the telecommunications is lawfully authorized. Both the SKIPJACK algorithm and the LEAF creation method are to be implemented in electronic devices (e.g., very large scale integration chips). The devices may be incorporated in security equipment used to encrypt (and decrypt) sensitive unclassified telecommunications data. Decryption of lawfully intercepted telecommunications may be achieved through the acquisition and use of the LEAF, the decryption algorithm and the two escrowed key components.

One definition of "escrow" means that something (e.g., a document, an encryption key) is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition" (Webster's Seventh New Collegiate Dictionary). The term, "escrow", for purposes of this standard, is restricted to this dictionary definition.

A key escrow system, for purposes of this standard, is one that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called "escrow agents"). In accordance with the above definition of "escrow", the key component holders provide the components of a key to a "grantee" (e.g., a law enforcement official) only upon fulfillment of the condition that the grantee has properly demonstrated legal authorization to conduct electronic surveillance of telecommunications which are encrypted using the specific device whose device unique key is being requested. The key components obtained through this process are then used by the grantee to reconstruct the device unique key and obtain the session key which is then used to decrypt the telecommunications that are encrypted with that session key.

The SKIPJACK encryption/decryption algorithm has been approved for government applications requiring encryption of sensitive but unclassified data telecommunications as defined herein. The specific operations of the SKIPJACK algorithm and the LEAF creation method are classified and hence are referenced, but not specified, in this standard.

Data for purposes of this standard includes voice, facsimile and computer information communicated in a telephone system. A telephone system for purposes of this standard is limited to a system which is circuit switched and operating at data rates of standard commercial modems over analog voice circuits or which uses basic-rate ISDN or a similar grade wireless service.

Data that is considered sensitive by a responsible authority should be encrypted if it is vulnerable to unauthorized disclosure during telecommunications. A risk analysis should be performed under the direction of a responsible authority to determine potential threats and risks. The costs of providing encryption using this standard as well as alternative methods and their respective costs should be projected. A responsible authority should then make a decision, based on the risk and cost analyses, whether or not to use encryption and then whether or not to use this standard.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Department of Commerce, National Institute of Standards and Technology.

Applicability: This standard is applicable to all Federal departments and agencies and their contractors under the conditions specified below. This standard may be used in designing and implementing security products and systems, which Federal departments and agencies use or operate or which are operated for them under contract. These products may be used when replacing Type II and Type III (DES) encryption devices and products owned by the government and government contractors.

This standard may be used when the following conditions apply:

- 1. An authorized official or manager responsible for data security or the security of a computer system decides that encryption is required and cost justified as per OMB Circular A- 130; and 2. The data is not classified according to Executive Order 12356, entitled "National Security Information," or to its successor orders, or to the Atomic Energy Act of 1954, as amended.

However, Federal departments or agencies which use encryption devices for protecting data that is classified according to either of these acts may use those devices also for protecting unclassified data in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security.

Applications: This standard may be used in any unclassified government and commercial communications. Use of devices conforming to this standard is voluntary for unclassified government applications and for commercial security applications.

Implementations: The encryption/decryption algorithm and the LEAF creation method shall be implemented in electronic devices (e.g., electronic chip packages) which are protected against unauthorized entry, modification and reverse engineering. Implementations which are tested and validated by NIST will be considered as complying with this standard. An electronic device shall be incorporated into a cryptographic module in accordance with FIPS 140-1. NIST will test for conformance with FIPS 140-1. Conforming cryptographic modules can then be integrated into security equipment for sale and use in a security application. Information about devices that have been validated, procedures for testing equipment for conformance with NIST standards, and information about approved security equipment are available from the Computer Systems Laboratory, NIST, Gaithersburg, MD 20899.

Export Control: Implementations of this standard are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations, Parts 120 through 131 (International Traffic of Arms Regulations - ITAR). Exporters of encryption devices, equipment and technical data are advised to contact the U.S. Department of State, Office of Defense Trade Controls for more information.

Patents: Implementations of this standard may be covered by U.S. and foreign patents.

Implementation Schedule: This standard becomes effective thirty days following publication of this FIPS PUB.

Specifications: Federal Information Processing Standard (FIPS 185), Escrowed Encryption Standard (EES) (affixed).

Cross Index:

- a. FIPS PUB 46-2, Data Encryption Standard. b. FIPS PUB 81, Modes of Operation of the DES c. FIPS PUB 140-1, Security Requirements for Cryptographic Modules.

GLOSSARY:

The following terms are used as defined below for purposes of this standard:

Data - Unclassified voice, facsimile and computer information communicated over a telephone system. Decryption - Conversion of ciphertext to plaintext through the use of a cryptographic algorithm.

Device (cryptographic) - An electronic implementation of the encryption/decryption algorithm and the LEAF creation method as specified in this standard.

Digital data - Data that have been converted to a binary representation.

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Key components - The two values from which a key can be derived (e.g., KU1 ~ KU2).

Key escrow - The processes of managing (e.g., generating, storing, transferring, auditing) the two components of a cryptographic key by two key component holders.

LEAF Creation Method - A part of a key escrow system that is implemented in a cryptographic device and creates a Law Enforcement Access Field.

Type I cryptography - A cryptographic algorithm or device approved by the National Security Agency for protecting classified information.

Type II cryptography - A cryptographic algorithm or device approved by the National Security Agency for protecting sensitive unclassified information in systems as specified in section 2315 of Title 10 United States Code, or section 3502(2) of Title 44, United States Code.

Type III cryptography - A cryptographic algorithm or device approved as a Federal Information Processing Standard.

Type III(E) cryptography - A Type III algorithm or device that is approved for export from the United States. Qualifications: The protection provided by a security product or system is dependent on several factors. The protection provided by the SKIPJACK algorithm against key search attacks is greater than that provided by the DES algorithm (e.g., the cryptographic key is longer). However, provisions of this standard are intended to ensure that information encrypted through use of devices implementing this standard can be decrypted by a legally authorized entity.

Where to Obtain Copies of the Standard: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 185 (FIPS PUB 185), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

Federal Information Processing Standards Publication 185

1994 February 9

Specifications for the

ESCROWED ENCRYPTION STANDARD

1. INTRODUCTION

This publication specifies Escrowed Encryption Standard (EES) functions and parameters.

2. GENERAL

This standard specifies use of the SKIPJACK cryptographic algorithm and a LEAF Creation Method to be implemented in an approved electronic device (e.g., a very large scale integration electronic chip). The device is contained in a logical cryptographic module which is then integrated in a security product for encrypting and decrypting telecommunications. Approved implementations may be procured by authorized organizations for integration into security equipment. Devices must be tested and validated by NIST for conformance to this standard. Cryptographic modules must be tested and validated by NIST for conformance to FIPS 140-1.

3. ALGORITHM SPECIFICATIONS

The specifications of the encryption/decryption algorithm (SKIPJACK) and LEAF Creation Method 1 (LCM-1) are classified. The National Security Agency

maintains these classified specifications and approves the manufacture of devices which implement the specifications. NIST tests for conformance of the devices implementing this standard in cryptographic modules to FIPS 140-1 and FIPS 81.

4. FUNCTIONS AND PARAMETERS

4.1 FUNCTIONS

The following functions, at a minimum, shall be implemented:

1. Data Encryption: A session key (80 bits) shall be used to encrypt plaintext information in one or more of the following modes of operation as specified in FIPS 81: ECB, CBC, OFB (64), CFB (1, 8, 16, 32, 64).
2. Data Decryption: The session key (80 bits) used to encrypt the data shall be used to decrypt resulting ciphertext to obtain the data .
3. LEAF Creation: A Family Key (e.g., KF-1) shall be used to create a Law Enforcement Access Field (LEAF) in accordance with a LEAF Creation Method (e.g., LCM-1). The security equipment shall ensure that the LEAF is transmitted in such a manner that the LEAF and ciphertext may be decrypted with legal authorization. No additional encryption or modification of the LEAF is permitted.

4.2 PARAMETERS

The following parameters shall be used in performing the prescribed functions:

1. Device Unique Identifier (UID): The identifier unique to a particular device and used by the Key Escrow System.
2. Device Unique Key (KU): The cryptographic key unique to a particular device and used by the Key Escrow System.
3. Cryptographic Protocol Field (CPF): The field identifying the registered cryptographic protocol used by a particular application and used by the Key Escrow System (reserved for future specification and use).
4. Escrow Authenticator (EA): A binary pattern that is inserted in the LEAF to ensure that the LEAF is transmitted and received properly and has not been modified, deleted or replaced in an unauthorized manner.
5. Initialization Vector (IV): A mode and application dependent vector of bytes used to initialize, synchronize and verify the encryption, decryption and key escrow functions.
6. Family Key (KF): The cryptographic key stored in all devices designated as a family that is used to create a LEAF.
7. Session Key (KS): The cryptographic key used by a device to encrypt and decrypt data during a session.
8. Law Enforcement Access Field (LEAF): The field containing the encrypted session key and the device identifier and the escrow authenticator.

5. IMPLEMENTATION

The Cryptographic Algorithm (i.e., SKIPJACK) and a LEAF Creation Method (e.g., LCM-1) shall be implemented in an electronic device (e.g., VLSI chip) which is highly resistant to reverse engineering (destructive or non-destructive) to obtain or modify the cryptographic algorithm, the UID, the KF, the KU, the EA, the CPF, the operational KS, and any other security or Key Escrow System relevant information. The device shall be able to be programmed/personalized (i.e., made unique) after mass production in such a manner that the UID, KU (or its components), KF (or its components) and EA fixed pattern can be entered once (and only once) and maintained without external electrical power.

The LEAF and the IV shall be transmitted with the ciphertext. The specifics of the protocols used to create and transmit the LEAF, IV, and encrypted data shall be registered and a CPF assigned. The CPF (and the KF-ID, LCM-ID) shall then be transmitted in accordance with the registered specifications.

Various devices implementing this standard are anticipated. The implementation may vary with the application. The specific electric, physical and logical interface will vary with the implementation. Each approved, registered implementation shall have an unclassified electrical, physical and logical interface specification sufficient for an equipment manufacturer to understand the general requirements for using the device. Some of the requirements may be classified and therefore would not be specified in the unclassified interface specification. The device Unique Key shall be composed of two components (each a minimum of 80 bits long) and each component shall be independently generated and stored by an escrow agent. The session key used to encrypt transmitted information shall be the same as the session key used to decrypt received information in a two-way simultaneous communication. The Lead Creation Method (LCM), the Cryptographic Protocol Field (CPF), and the Family Key Identifier (KF-ID) shall be registered in the NIST Computer Security Object Register.

This standard is not an interoperability standard. It does not provide sufficient information to design and implement a security device or equipment. Other specifications and standards will be required to assure interoperability of EES devices in various applications. Specifications of a particular EES device must be obtained from the manufacturer.

The specifications for the SKIPJACK algorithm are contained in the R21 Informal Technical Report entitled "SKIPJACK" (S), R21-TECH- 044-91, May 21, 1991. The specifications for LEAF Creation Method 1 are contained in the R21 Informal Technical Report entitled "Law Enforcement Access Field for the Key Escrow Microcircuit" (S). Organizations holding an appropriate security clearance and entering into a Memorandum of Agreement with the National Security Agency regarding implementation of the standard will be provided access to the classified specifications. Inquiries may be made regarding the Technical Reports and this

program to Director, National Security Agency, Fort George G. Meade, MD 20755-6000, ATTN: R21.