ITL BULLETIN FOR DECEMBER 2012

GENERATING SECURE CRYPTOGRAPHIC KEYS: A CRITICAL COMPONENT OF CRYPTOGRAPHIC KEY MANAGEMENT AND THE PROTECTION OF SENSITIVE INFORMATION

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Cryptography provides strong protection for information technology (IT) systems, applications, and information, especially when information is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptographic methods can be used to maintain the confidentiality and integrity of information, verify that information was not changed after it was sent, and authenticate the originator of the information.

Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key. The algorithm is a complex mathematical function for applying cryptographic protection (e.g., encrypting the data) and later reversing or verifying the process (e.g., decrypting the encrypted data), and the key is a parameter used by the function. Secure management of the cryptographic keys is critically important, since the security and reliability of cryptographic processes depend upon the strength of the keys, the effectiveness of the protocols associated with the keys, and the protection given to the keys.

Federal Standards and Recommendations for the Secure Management of Cryptography

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) has developed Federal Information Processing Standards (FIPS) specifying cryptographic algorithms that are approved for federal government use. In addition, NIST Special Publications (SPs) provide recommended practices that assist federal government organizations in applying cryptographic methods and in securely managing the cryptographic keys that are to be used with the approved cryptographic algorithms.

Another effort that helps organizations manage cryptographic keys effectively is the testing and validation of cryptographic modules, which contain the cryptographic algorithms and which are used in commercial products and systems to provide security services. The testing and validation program established by NIST focuses on the validation of cryptographic modules and cryptographic algorithm

implementations, accreditation of independent testing laboratories, and the development of test suites for the cryptographic algorithms. Many of these testing and validation activities are carried out in collaboration with industry and with other government organizations.

See the **For More Information** section below for references to approved cryptographic algorithms, requirements for cryptographic modules, and the operation of the Cryptographic Module Validation Program (CMVP).

In November, ITL issued a new guide, NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, to help federal government organizations generate the cryptographic keys that are to be used with the approved cryptographic algorithms. The publication provides general background information on the generation of cryptographic keys, how and where the keys are generated, and requirements for the generation of keys that provide the security strengths needed by organizations to protect their information.

NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation*

NIST SP 800-133, which was written by Elaine Barker and Allen Roginsky of NIST, discusses technical methods covering the generation of keys using the output of a random bit generator, the derivation of a key from another key, the derivation of a key from a password, and the key agreement process performed by two entities using an approved key-agreement scheme.

SP 800-133 recommends methods for the generation of key pairs for asymmetric algorithms and of keys for symmetric algorithms. Included in the publication are definitions, explanations of acronyms and symbols, and references to standards and to recommendations for the secure implementation of cryptographic algorithms and the effective management of cryptographic keys.

Recommendation for Cryptographic Key Generation is available here.

Cryptographic Algorithms and Keys

A cryptographic algorithm and a key are used to provide a number of cryptographic services, including encrypting data, generating a digital signature, decrypting encrypted data, and verifying a digital signature. Other cryptographic services include generating challenges, random numbers, and Message Authentication Codes (MACs).

In secret-key cryptography, two or more parties share the same key, which is used to encrypt and decrypt data. The key must be kept secret, and the parties who share a key rely upon each other not to disclose the key and to protect it against modification.

Public key cryptography uses a pair of keys for each party: one is public and the other is private. The public key can be made known to other parties; the private key must be kept confidential and must be known only to its owner. Both keys, however, need to be protected against modification. Public key cryptography is used to generate and verify digital signatures to provide assurance to a receiver that a given message was sent by the claimed sender, or to establish symmetric keys between parties that do not share such keys for protecting sensitive information.

Keys may be established through techniques that are based on asymmetric or public key algorithms, or through techniques that are based on symmetric or secret key algorithms. Hybrid techniques are also commonly used in the key-generating process by applying public key techniques to establish symmetric or secret keys, which are then used to establish other symmetric or secret keys or to protect sensitive information.

Summary of NIST Recommendations for Cryptographic Key Generation

NIST SP 800-133 specifies the methods for the computation, establishment, and distribution of key pairs in accordance with existing standards and recommendations. See the online version of the publication for detailed information about implementing the recommendations for the generation of secure cryptographic keys.

Key generation techniques. Keys can be generated through a variety of techniques: the generation of a key using the output of a random bit generator (RBG), the derivation of a key from another key, the derivation of a key from a password, and a key agreement performed by two entities using an approved key-agreement scheme. SP 800-133 specifies that federal organizations base the generation of their cryptographic keys directly or indirectly on the output of an approved random bit generator. Keys that are derived during a key-agreement transaction, derived from another key using a key derivation function, or derived from a password for storage applications are considered to be indirectly generated from an RBG, since the key used in the generation of another key or the random value used to generate a key-agreement key pair was obtained directly from the output of an approved RBG.

Cryptographic keys needed by federal organizations are to be generated within tested and validated cryptographic modules. Random values required for key generation must be generated within the module that generates the key. The RBG should provide the security strengths that the implementing organization needs to protect its information. NIST publications that provide recommendations covering the techniques for the generation of keys using RBGs are included in the list of publications below.

Generation of key pairs for asymmetric algorithms. Asymmetric-key algorithms, also known as public-key algorithms, require the use of asymmetric key pairs, consisting of a private key and a corresponding public key. The key to be used for each operation depends on the cryptographic process being

performed; for example, digital-signature generation requires the use of a private key, while signature verification requires the use of the corresponding public key.

Each public/private key pair is associated with only one entity; this entity is known as the key-pair owner. The public key may be known by anyone, but the private key must be known and used only by the key-pair owner. Key pairs are generated by either the key-pair owner or by a trusted party that will provide the key pair to the owner in a secure manner. The trusted party must be trusted by all parties that use the public key.

One use of asymmetric keys is the generation of digital signatures. Digital signatures are generated on data to provide origin authentication, assurance of data integrity, or signatory non-repudiation. Digital signatures are generated by a signer using a private key, and verified by a receiver using a public key. Publications that include recommendations for the generation of key pairs for asymmetric applications are included in the reference section below.

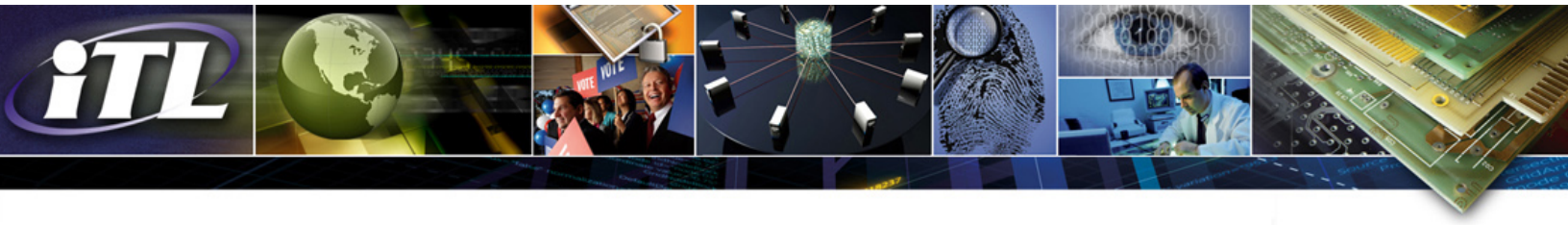
Generation of keys for symmetric key algorithms. Symmetric-key algorithms use the same key to both apply cryptographic protection to information and to remove or verify the protection. Keys used with symmetric-key algorithms must be known only by the entities authorized to apply, remove, or verify the protection, and are commonly known as secret keys. A secret key is often known by multiple entities that may share or own the secret key, although it is not uncommon for a key to be generated, owned, and used by a single entity, such as for secure storage.

A secret key should be generated by one or more of the entities that will share the key, or a trusted party that provides the key to the intended sharing entities in a secure manner. The trusted party must be trusted by all entities that will share the key not to disclose the key to unauthorized parties or otherwise misuse the key. Publications that include recommendations for the generation of keys for symmetric applications are included in the reference section below.

For More Information

The following publications are related to methods for the management of cryptography. For information about these NIST standards and guidelines, as well as other security-related publications, see here.

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules* (The Implementation Guidance for FIPS PUB 140-2 and information about the Cryptographic Module Validation Program is available here.
FIPS 180-4, *Secure Hash Standard (SHS)*
FIPS 186-3, *Digital Signature Standard (DSS)*
FIPS 197, *Advanced Encryption Standard (AES*)



FIPS 198-1, *Keyed-Hash Message Authentication Code (HMAC)*
Special Publication (SP) 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*
SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*
SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
SP 800-56B, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*
SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*,
SP 800-57, Part 1, *Recommendation for Key Management: General (Revision 3)*
SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
SP 800-90B, Draft *Recommendation for the Entropy Sources Used for Random Bit Generation*
SP 800-90C, Draft *Recommendation for Random Bit Generator (RBG) Constructions*
SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*
SP 800-131A, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths*
SP 800-132, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications*
SP 800-135, *Recommendation for Existing Application-Specific Key Derivation Function*

Information about NIST's information security programs is available from the Computer Security Resource Center here.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.