Draft NIST Special Publication 800-57 Part 2
Revision 1

Recommendation for Key Management

Part 2: Best Practices for Key Management Organization

Elaine Barker
William C. Barker

C O M P U T E R S E C U R I T Y

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-57 Part 2 Revision 1

Recommendation for Key Management

Part 2: Best Practices for Key Management Organization

Elaine Barker
Computer Security Division

William C. Barker
Dakota Consulting

April 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-57 Part 2 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-57 Part 2 Rev. 1, 71 pages (April 2018)
CODEN: NSPUE2

Public comment period: *April 2, 2018* through *May 31, 2018*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: keymanagement@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Special Publication (SP) 800-57 provides cryptographic key management guidance. It consists of three parts. Part 1, *Recommendation for Key Management, Part 1: General*, provides general guidance and best practices for the management of cryptographic keying material. Part 2, *Best Practices for Key Management Organization*, provides guidance on policy and security planning requirements. Finally, Part 3, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, provides guidance when using the cryptographic features of current systems. Part 2 (this document) 1) introduces key management concepts that must be addressed in key management policies, practice statements and planning documents by any organization that uses cryptography to protect its information; 2) provides guidance for the development of organizational key management policy statements and key management practices statements; and 3) identifies key management information that needs to be documented for all federal applications of cryptography. Appendices provide examples of key management infrastructures and supplemental documentation and planning materials.

Keywords

accreditation; assurances; authentication; authorization; availability; backup; certification; compromise; confidentiality; cryptanalysis; cryptographic key; cryptographic module; digital signature; key management; key management policy; key recovery; private key; public key; public key infrastructure; security plan; trust anchor; validation.

Acknowledgements

The National Institute of Standards and Technology (NIST) gratefully acknowledges and appreciates contributions Lydia Zieglar from the National Security Agency concerning the many security issues associated with this Recommendation, and by Tim Polk, Bill Burr, and Miles Smid who co-authored the first edition of this publication. NIST also thanks the many contributors from both the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Table of Contents

1. Introduction

"Best Practices for Key Management Organization," Part 2 of the *Recommendation for Key Management*, NIST Special Publication (SP) 800-57, is intended primarily to address the needs of system owners and managers who are setting up or acquiring cryptographic key establishment and management capabilities. Parts 1 and 3 of SP 800-57, the *Recommendation for Key Management* focus on technical key management mechanisms. SP 800-57 Part 1, *General*, (hereafter referred to as Part 1) contains basic key management guidance intended to advise users, developers and system managers; and SP 800-57 Part 3, *Application-Specific Key Management Guidance*, (hereafter referred to as Part 3) is intended to address the key management issues associated with currently available implementations.

Part 2 of the *Recommendation for Key Management* first identifies the concepts, functions and elements common to effective key management systems; second, describes key management policy and practice documentation that are needed by organizations that use cryptography; and third, identifies the security planning requirements and documentation necessary to effective institutional key management. Appendices provide examples of key management infrastructures and supplemental documentation and planning materials.

Non-governmental organizations may voluntarily choose to follow this practice.

1.1 Scope

SP 800-57 Part 2, *Best Practices for Key Management Organization* (hereafter referred to as Part 2), 1) identifies concepts, functions, and elements common to effective key management systems; 2) describes key management policy and practice documentation that is needed by organizations that use cryptography; and 3) identifies security planning requirements and documentation necessary to effective institutional key management. Appendices provide examples of key management infrastructures and supplemental documentation and planning materials. This document identifies applicable laws and directives concerning security planning and management and suggests approaches to satisfying those laws and directives with a view to minimizing the impact of management overhead on organizational resources and efficiency. Part 2 also acknowledges that planning and documentation requirements associated with small-scale or single-system organizations will not need to be as elaborate as those required for large and diverse government agencies that are supported by a number of information technology systems. However, any organization that employs cryptography to provide security services needs to have key management policy, practices and planning documentation.

Part 2 of this Recommendation recognizes that some key management functions, such as provisioning and the revocation of keys, are sufficiently labor-intensive that they act as an impediment to the adoption of cryptographic cybersecurity mechanisms – particularly in large network operations. Nevertheless, responsible cryptographic key management is essential to the effective use of cybersecurity mechanisms for protecting information technology systems against attacks that threaten the confidentiality of the information processed, stored, and communicated; the integrity of information and systems operation; and the timely availability of critical information and services. Improved tools for the automation of many key management services

are needed to improve the security, performance, and usability of key management systems, but the characteristics identified in SP 800-57 as essential to secure and effective key management are valid, independent of performance and usability concerns.

1.2 Audience

The primary audience for Part 2 is the set of federal government system owners and managers who are setting up or acquiring cryptographic key establishment and management capabilities. However, consistent with the Cybersecurity Enhancement Act of 2014 (PL 113-274), this Recommendation is also intended to provide direct cybersecurity support to the private sector as well as government-focused guidance consistent with OMB Circular A-130 (OMB 130[1]). Since guidelines and best practices for the private sector are strictly voluntary, the requirement terms (**should**/**shall** language) used for some recommendations do not apply outside the federal government. For federal government organizations, the terms **should** and **shall** have the following meaning in this document:

1. **shall**: This term is used to indicate a requirement of a Federal Information Processing Standard (FIPS) or NIST Recommendation. Note that **shall** may be coupled with **not** to become **shall not**.

2. **should**: This term is used to indicate an important recommendation. Ignoring the recommendation could result in undesirable results. Note that **should** may be coupled with **not** to become **should not**.

1.3 Background and Rationale

Regardless of the key management method employed, some secret or private keys will need to be made available to some set of the entities that use cryptography. Trust in the source of these keys is essential to any confidence in the cryptographic mechanisms being employed. Access to the private or secret keys by entities that are not intended to use them invalidates any assumptions regarding the confidentiality or integrity of information believed to be protected by the associated cryptographic mechanisms. Although organizations may generate keys for and distribute keys to members, the only way to completely protect information being stored under a cryptographic key is for the entity responsible for storing the information to control the generation and key storage process. The only way to completely protect information being shared between any two or more entities using a cryptographic mechanism is for the underlying private or secret keys to be generated and passed to the intended recipient of the information by a completely secure (often manual) process. This approach is impractical for most organizations. Organizations usually have the right to access any information that is present in systems belonging to that organization. As a result, policies generally permit the organization to acquire or generate the private or secret keys on which the security of cryptographic mechanisms depends. Trust between an organization and the source of the private or secret keys used by its staff and associates must be established by agreement, documented by policy, and implemented within a key management infrastructure.

At the device or software application level, keying material needs to be provided, changed, and protected in a manner that enables cryptographic operation and preserves the integrity of

[1] OMB A-130, *Managing Information as a Strategic Resource*.

cryptographic processes and their dependent services. FIPS 140 [2] provides guidance on implementing key establishment and entry functionality into a cryptographic module. A variety of other government publications specify key establishment schemes and processes in specific applications, including:

a) SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*;

b) SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*;

c) SP 800-56C, *Recommendation for Key Derivation Methods in Key-Establishment Schemes*;

d) SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*;

e) SP 800-132, *Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*;

f) SP 800-133, *Recommendation for Cryptographic Key Generation*; and

g) SP 800-135, *Recommendation for Existing Application-Specific Key Derivation Functions.*

Technical mechanisms alone are not sufficient to ensure the protection of sensitive information. SP 800-57 Part 2, specifies key management planning requirements for cryptographic product development, acquisition, and implementation. In federal government systems, technical mechanisms are required to be used in combination with a set of procedures that implement a clearly understood and articulated protection policy. Part 2 provides a framework and general guidance to support establishing cryptographic key management policies, procedures, and the key management infrastructure within an organization. This Part 2 also provides a basis for satisfying the key management aspects of statutory and policy security planning requirements for federal government organizations.

In acknowledgement of the heterogeneous nature of the cryptographic user community, SP 800-57 Part 2, presents a significant degree of flexibility with respect to the complexity of management infrastructures and the amount of documentation required to support key management. As previously noted, planning and documentation requirements associated with small scale or single-system organizations will obviously not be as elaborate as those required for large and diverse government agencies supported by a number of information technology systems. However, any organization that employs cryptography to provide security services is likely to require policy, practices and planning documentation.

In order for key management practices and procedures to be effectively employed, support for these practices and procedures at the highest levels of the organization is a practical necessity. The executive level of the organization needs to establish policies that identify executive-level key management roles and responsibilities for the organization. The key management policies need to support the establishment of, or access to, the services of a key management infrastructure and the employment and enforcement of key management practices and procedures.

[2] FIPS 140, *Security Requirements for Cryptographic Modules*.

1.4 Organization

Part 2 of the *Recommendation for Key Management* is organized as follows:

- Section 2 introduces key management concepts that must be addressed in key management policies, practice statements and planning documents by any organization that uses cryptography to protect its information.
- Section 3 provides guidance for the development of organizational key management policy statements and key management practices statements. Key management policies and practices documentation may take the form of separate planning and implementation documents or may be included in an organization's existing information security policies and procedures.[3]
- Section 4 identifies key management information that needs to be documented for all federal applications of cryptography.
- Appendix A provides key management infrastructure (KMI) examples.
- Appendix B provides key management inserts for organizational security plans.
- Appendix C provides a key management specification checklist for cryptographic product development.
- Appendix D is a table of references.
- Appendix E identifies Revision 1 changes from the original SP 800-57 Part 2 document.

1.5 Glossary of Terms and Acronyms

The definitions provided below are consistent with Part 1. Note that the same terms may be defined differently in other documents.

1.5.1 Glossary

Access control	As used in this Recommendation, the set of procedures and/or processes that only allow access to information in accordance with pre-established policies and rules.
Accountability	A property that ensures that the actions of an entity may be traced uniquely to that entity.
Approved	FIPS-Approved and/or NIST-recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) specified elsewhere and adopted by reference in a FIPS or NIST Recommendation.
Archive	See *Key management archive*.

[3] Agency-wide security program plans are required by OMB guidance on implementing the *Government Information Security Reform Act*.

Authentication	A process that provides assurance of the source and integrity of information in communications sessions, messages, documents or stored data. In a general information security context: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (as defined in SP800-53[4]).
Authentication code	A cryptographic checksum based on an **approved** security function (e.g., a cryptographic algorithm) and a symmetric key to detect both accidental and intentional modifications of data (also known as a message authentication code).
Authority	The aggregate of people, procedures, documentation, hardware, and/or software necessary to authorize and enable security-relevant functions.
Authorization	(noun) Access privileges granted to an entity; conveys an "official" sanction to perform a security function or activity. (verb) The process of verifying that a requested action or service is approved for a specific entity.
Availability	Timely, reliable access to information by authorized entities.
Backup	A copy of information (e.g., keying material) to facilitate recovery of that material, if necessary.
Central oversight authority	The key management infrastructure (KMI) entity that provides overall KMI data synchronization and system security oversight for an organization or set of organizations.
Certificate	See *Public key certificate*.
Certificate class	A CA-designation (e.g., "class 0" or "class 1") indicating how thoroughly the CA checked the validity of the certificate. Per X.509 rules, the "class" **should** be encoded in the certificate as a CP extension: the CA can put there some OID which designates the set of procedures applied for the issuance of the certificate. These OID are CA-specific and can be understood only by referring to the Certification Practice Statement.
Certificate policy	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements.
Certificate revocation list (CRL)	A list of revoked public key certificates by certificate number that includes the revocation date and (possibly) the reason for their revocation.

[4] SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

Certification authority (CA)	The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy.
Certification path	An ordered list of certificates (containing an end-user subscriber certificate and zero or more intermediate certificates) that enables the receiver to verify that the sender and all intermediates certificates are trustworthy. Each certificate in the path must have been signed by the private key corresponding to the public key that precedes it in the path, and the first certificate in the path must have been issued by a *Trust anchor*.
Certification practice statement	A statement of the practices that a certification authority employs in issuing and managing public key certificates.
Ciphertext	Data in its encrypted form.
Client node	A recipient of the key distribution services needed to implement a key establishment scheme.
Communicating group	A set of communicating entities that employ cryptographic services and need cryptographic keying relationships (see below) to enable cryptographically protected communications.
Compliance audit	A comprehensive review of an organization's adherence to governing documents such as whether a certification practice statement satisfies the requirements of a certificate policy and whether an organization adheres to its certification practice statement.
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keying material and other security-related information).
Compromised key list (CKL)	A list of named keys that are known or suspected of being compromised.
Confidentiality	The property that sensitive information is not disclosed to unauthorized entities.
Cross-certification	Used by one CA to certify another CA other than a CA immediately adjacent (superior or subordinate) to it in a CA hierarchy.
Cryptanalysis	1. Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. 2. The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Examples include: • The transformation of plaintext data into ciphertext data, • The transformation of ciphertext data into plaintext data, • The computation of a digital signature from data, • The verification of a digital signature, • The computation of an authentication code from data, • The computation of a shared secret that is used to derive keying material.
Cryptographic keying relationship	A relationship among two or more entities that is in effect when the entities share one or more symmetric keys for secure communication.
Cryptographic key management system (CKMS)	Policies, procedures, devices, and components designed to protect, manage, and distribute cryptographic keys and metadata. A CKMS performs cryptographic key management functions on behalf of one or more entities.
Cryptographic module	The set of hardware, software, and/or firmware that implements **approved** security functions (including cryptographic algorithms and key generation) that are contained within the cryptographic security boundary of the module.
Cryptoperiod	The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.
Data integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored.
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
De-registration (of a key)	The removal of records of keying material that was registered by a registration authority.
Destruction	The process of overwriting, erasing, or physically destroying a key so that it cannot be recovered. See SP 800-88.[5]

[5] SP 800-88, *Guidelines for Media Sanitization.*

Digital signature	The result of a cryptographic transformation of data that, when properly implemented, provides the services of: 1. Origin (i.e., source) authentication, 2. Data integrity authentication, and 3. Support for signer non-repudiation.
Distribution	See *Key distribution*.
Emergency key revocation	A revocation of keying material that is effected in response to an actual or suspected compromise of keying material.
Encrypted keying material	Keying material that has been encrypted using an **approved** security function with a key encrypting key in order to disguise the value of the underlying plaintext key.
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key.
Entity	An individual (person), organization, device or process.
Establishment	See *Key establishment*.
Initialization vector (IV)	As used in this Recommendation, a vector used in defining the starting point of a cryptographic process (e.g., key wrapping).
Integrity	In the general information security context: guarding against improper modification; includes ensuring information non-repudiation and authenticity (as defined in SP800-53). In a cryptographic context: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner since it was created, transmitted or stored.
Interconnection Security Agreement	A security document that specifies the technical and security requirements for establishing, operating, and maintaining an interconnection.
Internet Key Exchange (IKE)	The protocol used to set up a security association in the Internet Protocol Security (IPsec) protocol suite.
Kerberos	A network authentication protocol that is designed to provide strong authentication for client/server applications by using symmetric-key cryptography.

Key agreement	A (pair-wise) key-establishment procedure in which the resultant secret keying material is a function of information contributed by both participants so that neither party can predetermine the value of the secret keying material independently from the contributions of the other party. Key agreement includes the creation (i.e., generation) of keying material by the key-agreement participants. A separate distribution of the generated keying material is not performed. Contrast with *Key transport*.
Key-center environment	As used in this Recommendation, a key-center environment is an environment in which keys or components of the keys necessary to support cryptographically protected exchanges within one or more communicating groups are obtained from a common central source.
Key certification	Key certification is a process that permits keys or key components to be unambiguously associated with their certificate sources (e.g., digital signatures that associate public-key certificates to be unambiguously associated with the certification authorities from which they were issued).
Key certification hierarchy	A key center or certification authority may delegate the authority to issue keys or certificates to subordinate centers or authorities that can, in turn, delegate that authority to their subordinates.
Key derivation	As used in this Recommendation, a method of deriving keying material from a pre-shared key and possibly other information. See SP 800-108.[6]
Key distribution	The transport of keying material from one entity (the sender) to one or more other entities (the receivers). The sender may have generated the keying material or acquired it from another source as part of a separate process. The receiver may be the intended user of the keying material or a conduit for passing the keying material to an intended user. The keying material may be distributed manually or using automated key transport mechanisms.
Key distribution center (KDC)	A key center that generates keys for distribution to subscriber entities.
Key encrypting key (KEK)	A cryptographic key used to encrypt other keys. Compare to *Key wrapping key*.
Key establishment	The process that results in the sharing of a key between two or more entities, either by manual distribution, using automated key transport or key agreement mechanisms or by key derivation using an already-shared key between or among those entities. Key establishment may include the creation of a key.

[6] SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions.

Key generation	The generation of keying material either as a single process using a random bit generator and an **approved** set of rules, or as created during key agreement.
Keying material	The data (e.g., keys and IVs) necessary to establish and maintain cryptographic keying relationships.
Keying material installation	The installation of keying material for operational use in a cryptographic module.
Key management	The activities involved in the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, use and destruction.
Key management infrastructure (KMI)	The framework and services that provide for the generation, production, establishment, control, accounting, and destruction of cryptographic keying material. It includes all elements (hardware, software, other equipment, and documentation); facilities; personnel; procedures; standards; and information products that form the system that establishes, manages, and supports cryptographic products and services for end users. The KMI may handle symmetric keys, asymmetric keys or both.
Key management plan	Documents how current and/or planned key management products and services will be supplied by the key management infrastructure and used by the cryptographic application to ensure that lifecycle key management support is available.
Key management policy	A high-level statement that identifies a high-level structure, responsibilities, governing standards and guidelines, organizational dependencies and other relationships, and security policies.
Key management product	A symmetric or asymmetric cryptographic key, a public-key certificate and other items (such as certificate revocation lists and compromised key lists) that are obtained by a trusted means from some source. These products can be used to validate the authenticity of keys or certificates. Software that performs either a security or cryptographic function (e.g., keying material accounting and control, random number generation, cryptographic module verification) is also considered to be a cryptographic product.
Key management practice statement	A document or set of documentation that describes in detail the organizational structure, responsible roles, and organization rules for the functions identified in the key management policy (see IETF RFC 3647[7]).

[7] RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

Key pair	A public key and its corresponding private key; a key pair is used with a public key algorithm.
Key processing facility	A KMI component that performs one or more of the following functions: • The acquisition or generation of public key certificates, • The initial establishment of keying material (including generation and distribution), • The maintenance of a database that maps user entities to an organization's certificate/key structure, • Key archiving or key recovery, • The maintenance and distribution of key compromise lists and/or certificate revocation lists, and • The generation of audit requests and the processing of audit responses as necessary for the prevention of undetected compromises.
Key recovery	Mechanisms and processes that allow authorized entities to retrieve or reconstruct keying material from key backups or archives.
Key recovery agent (KRA)	A role that assists in the access of stored key information for recovery, metadata modification or deletion.
Key revocation	A process whereby a notice is made available to affected entities that keying material **should** be removed from operational use prior to the end of the established cryptoperiod of that keying material.
Key specification	A specification of the data format, cryptographic algorithms, physical media, and data constraints for keys required by a cryptographic device and/or application.
Key translation center (KTC)	A key center that receives keys from one entity wrapped using a symmetric key shared with that entity, unwraps the wrapped keys and rewraps the keys using a symmetric key shared with another entity.
Key transport (automated)	A key-establishment procedure whereby one entity (the sender) selects a value for secret keying material and then securely distributes that value to one or more other entities (the receivers). Contrast with *Key agreement*.
Key wrapping	A method of providing both confidentiality and integrity for keying material using a symmetric key, Compare with *Key encrypting key*, which only provides confidentiality
Key wrapping algorithm	A cryptographic algorithm approved for use in wrapping keys.

Key wrapping key	A symmetric key that is used with a key-wrapping algorithm to protect the confidentiality and integrity of keying material.
Least privilege	A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.
Manual key distribution	A non-automated means of transporting cryptographic keys by physically moving a device or document containing the key or key component.
Mesh	In meshed key management architecture, each of several key processing facilities may interact with some other key processing facility in what is termed a *mesh*, but no concept of dominance is implied by the interaction.
Message authentication	A process that provides assurance of the integrity of messages, documents or stored data.
Multiple-center group	As used in this Recommendation, a set of two or more key centers that have agreed to work together to provide cryptographic keying services to their subscribers.
Non-repudiation	A service using a digital signature that is used to support a determination of whether a message was actually signed by a given entity. In a general information security context, assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information (as defined in SP800-53).
Password	A string of characters (letters, numbers and other symbols) that are used to authenticate an identity, to verify access authorization or to derive cryptographic keys.
Peers	Entities at the same tier in a key management hierarchy (e.g., all peers are client nodes).
Plaintext	Intelligible data that has meaning and can be understood without the application of decryption.

Private key	A cryptographic key, used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public. The private key has a corresponding *public key*. Depending on the algorithm, the private key may be used to: 1. Compute the corresponding public key, 2. Compute a digital signature that may be verified by the corresponding public key, 3. Decrypt keys that were encrypted by the corresponding public key, or 4. Compute a shared secret during a key agreement transaction.
Public key	A cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and that may be made public. The public key has a corresponding *private key*. The public key may be known by anyone and, depending on the algorithm, may be used to: 1. Verify a digital signature that is signed by the corresponding private key, 2. Encrypt keys that can be decrypted using the corresponding private key, or 3. Compute a shared secret during a key agreement transaction.
Public key certificate	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity (e.g., using an X.509 certificate). Additional information in the certificate could specify how the key is used and its validity period.
Public-key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys, a *public key* and a *private key*. The two keys have the property that determining the private key from the public key is computationally infeasible.
Public key infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates. A PKI is one example of a *Key management infrastructure*.
Registration authority (RA)	An entity that is responsible for the identification and authentication of certificate subjects on behalf of an authority, but that does not sign or issue certificates (e.g., an RA is delegated certain tasks on behalf of a CA).
Rekey	The replacement of one key by another key that is totally unrelated to the old key but has the same format.

Relying party	An entity that relies on received information for authentication purposes.
Revocation	See *Key revocation*.
Revoked key notification (RKN)	A report (e.g., a list) of one or more keys that have been revoked and the date(s) of revocation, possibly along with the reason for their revocation. CRLs and CKLs are examples of RKNs; along with Online Certificate Status Protocol (OCSP) responses (see RFC 6960[8]).
Security policy	Defines the threats that a system needs to address and provides high-level mechanisms for addressing those threats.
Separation of duties	A security principle that divides critical functions among different staff members in an attempt to ensure that no single individual has enough information or access privilege to perpetrate damaging fraud.
Service agent	An intermediate distribution or service facility. Some key management infrastructures may be sufficiently large or support sufficiently organizationally complex organizations, making it impractical for organizations to receive keying material directly from a common key processing facility.
Suspension	The process of temporarily changing the status of a key or certificate to invalid (e.g., in order to determine if it has been compromised or to indicate that the owner is unavailable for valid activity using that certificate). The certificate may subsequently be revoked or reactivated.
Symmetric key	A single cryptographic key that is used by one or more entities with a symmetric key algorithm.
Symmetric key algorithm	A cryptographic algorithm that employs the same secret key for an operation and its complement (e.g., encryption and decryption).
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission function, image, or reputation), agency assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of data, and/or denial of service (as defined in SP800-53).
Token	A portable, user-controlled, physical device (e.g., smart card or memory stick) used to store cryptographic information and possibly also perform cryptographic functions.

[8] RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Updates*.

Transport Layer Security protocol (TLS)	An authentication and security protocol that is widely implemented in browsers and web servers. TLS is defined by RFC 2246, RFC 3546, and RFC 5246. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. SP 800-52[9] specifies how TLS is to be used in government applications.
Trust anchor	An authoritative entity for which trust is assumed and not derived. In a public key infrastructure (PKI), the trust anchor is a certification authority (CA) that may be the issuer of the first certificate in a *certification path*. "Trust anchor" also refers to the public key of this CA.
Unauthorized disclosure	An event involving the exposure of information to entities not authorized access to the information.
User	An entity that uses a cryptographic key.
Wrapped keying material	Keying material that has been encrypted using an **approved** security function that also provides integrity protection using a key wrapping key in order to disguise the value of the underlying plaintext key.
X.509 certificate	The X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. Most commonly (including in this document), an X.509 certificate refers to the X.509 public-key certificate.
Zeroization	See *Destruction*.

1.5.2 Acronyms

The following abbreviations and acronyms are used in this document:

CA	Certification Authority
CIO	Chief Information Officer
CKL	Compromised Key List
CKMS	Cryptographic Key Management System
CN	Client Node
COA	Central Oversight Authority
CPS	Certification Practice Statement
CP	Certificate Policy

[9] SP 800-52, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

297	CRL	Certificate Revocation List
298	CSN	Central Service Node
299	FIPS	Federal Information Processing Standard
300	KMI	Key Management Infrastructure
301	IPsec	Internet Protocol Security
302	IKE	Internet Key Exchange
303	ISA	Interconnection Service Agreement
304	IV	Initialization Vector
305	KMP	Key Management Policy
306	KMPS	Key Management Practice Statement
307	KPF	Key Processing Facility
308	MOA	Memorandum of Agreement
309	MOU	Memorandum of Understanding
310	NIST	National Institute of Standards and Technology
311	OMB	Office of Management and Budget
312	Part 1	SP 800-57, Part 1
313	Part 2	SP 800-57, Part 2 (this document)
314	Part 3	SP 800-57, Part 3
315	PKI	Public Key Infrastructure
316	RA	Registration Authority
317	RKN	Revoked Key Notification
318	SA	Service Agent
319	S/MIME	Secure/Multipurpose Internet Mail Exchange
320	SP	Special Publication
321	TLS	Transport Layer Security

2 Key-Management Concepts

This section introduces key-management concepts that must be addressed in key-management policies, practice statements and planning documents by any organization that uses cryptography to protect its information.

2.1 Key Establishment

Key establishment is the process that results in the sharing of a key between two or more entities. This process could be by a manual distribution, using automated key-transport or key-agreement mechanisms or by key derivation using an already-shared key between or among those entities. Key establishment may include the creation of a key.

Key distribution is the transport of keying material from one entity (the sender) to one or more other entities (the receivers). The sender may have generated the keying material or acquired it from another source as part of a separate process. The receiver may be the intended user of the keying material or a conduit for passing the keying material to an intended user. The keying material may be distributed manually or using automated key-transport mechanisms.

Manual distribution is a method of transporting keys from the entity that generates the keys to the entities that will use them. This may be done using trusted couriers, face-to-face meetings or similar trusted mechanisms. The keys may be provided on electronic devices (e.g., flash drives or key loaders). Historically, the keys were often printed on paper, but this is discouraged because of the difficulty of entering long keys into a cryptographic module without error. Manual distribution is often the only means of providing the initial key that establishes a cryptographic relationship.

Automated key transport is a key-establishment procedure whereby one entity (the sender) selects a value for secret keying material and then securely distributes that value to one or more other entities (the receivers) using online protocols. The selection process is based on the output of a random bit generator and criteria for the generation of keying material from that output.

Automated key agreement is a (pair-wise) key-establishment procedure using online protocols in which the resultant secret keying material is a function of information contributed by both participants so that neither party can predetermine the value of the secret keying material independently from the contribution of the other party. Key agreement includes the creation of keying material between the key-agreement participants.

Key derivation is a method of deriving keying material using an algorithm and a pre-shared key that is used specifically for key derivation (i.e., a key-derivation key). In order for two or more entities to derive the same keying material, they must have the same key-derivation key (KWK) and any other information that may be included in the process (e.g., a counter or context-specific information such as the identifiers for the entities that share the KWK).

2.2 Key-Management Functions

Each of the functions that comprise key management need to be addressed by an organization's key-management policy. This is true for organizations already using cryptography as well as for the case of establishing key management in an organization that does not currently acquire, distribute, and manage keying material. Key management policies and practices will need to be documented (see Section 3). Roles and responsibilities need to be defined for management of at least the following functions:

- The generation or acquisition of keying material,
- The secure distribution of private or secret keys,
- The establishment of cryptoperiods,
- Procedures for routine supersession of keys at the end of a cryptoperiod,
- Procedures for the emergency revocation of compromised keying material and the distribution of replacement keys,
- The storage of and accounting for backup keying material and archived keys for recovery and checking the integrity of stored information following the end of the cryptoperiod in which it was protected, and
- The destruction of private or secret keying material that is no longer required.

2.3 Key-Management Infrastructures (KMIs)

This section identifies common key management infrastructure elements and suggests functions of and relationships among the organizational elements. The complexity of and allocation of roles within a key-management infrastructure will depend on 1) the cryptographic algorithms employed, 2) the operational and communications relationships among the organizational elements being served, 3) the purposes for which cryptography is employed, and 4) the number and complexity of cryptographic relationships required by an organization. The key management infrastructure itself will depend on all these factors, plus the key establishment approach to be taken (e.g., the key-establishment scheme[10] used).

The structure, complexity, and scale of actual KMIs may vary considerably according to the needs of individual organizations. However, the elements and functions identified here need to be present in most organizations that require cryptographic protection. This subsection describes the common KMI organizational elements, functions, and requirements. Examples of real-world KMIs are provided in Appendix A.

A KMI is designed to incorporate a set of functional elements that collectively provide unified and seamless protection policy enforcement and key management services. Several distinct functional elements are identified for the generation, establishment, and management of cryptographic keys: a central oversight authority, key processing facility(ies), (optional) service agents, client nodes and (optional) tokens. It should be noted that organizations may choose to combine the functionality of more than one element into a single component. Figure 1 illustrates functional KMI relationships.

[10] See SP 800-56A, SP 800-56B, SP 800-56C, SP 800-108, SP 800-132, SP 800-133, and SP 800-135.

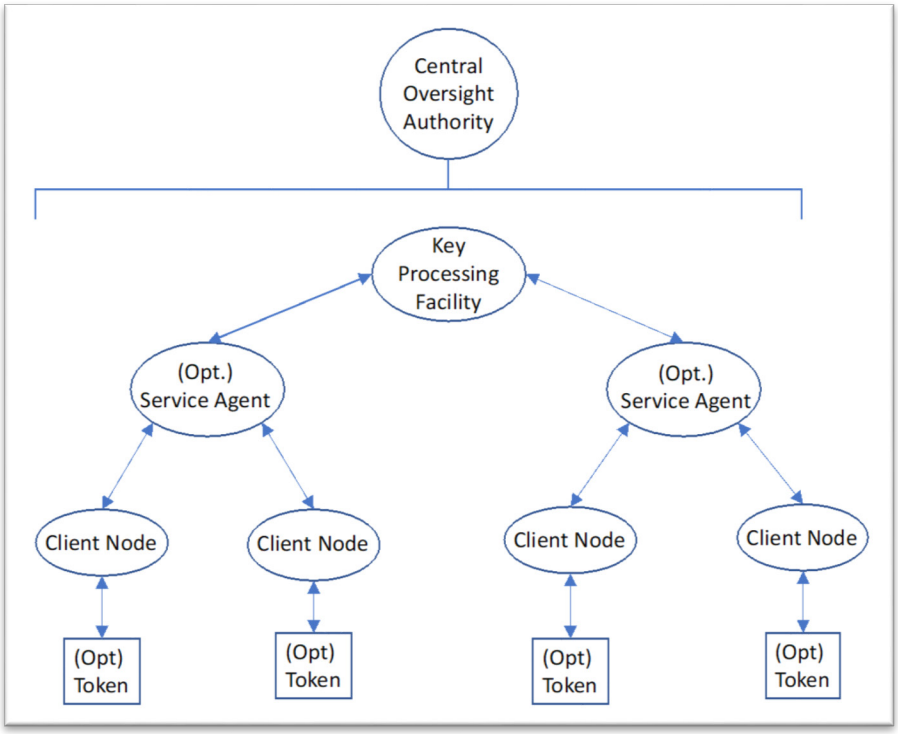

Figure 1: KMI Components

2.3.1 Central Oversight Authority (Facility)

As used in this Recommendation, the KMI's central oversight authority is the entity that provides overall KMI data synchronization and system security oversight for an organization or set of organizations. The central oversight authority 1) coordinates protection policy and practices (procedures) documentation, 2) may function as a holder of data provided by service agents, and 3) serves as the source for common and system-level information required by service agents (e.g., keying material and registration information, directory data, system policy specifications, and system-wide key compromise and revocation information). As required by survivability or continuity of operations policies, central oversight facilities may be replicated at an appropriate remote site to function as a system back up.

2.3.2 Key-Processing Facility(ies)

Key-processing facilities[11] typically provide one or more of the following services:

- Generation and/or distribution of keying material,
- Acquisition or generation of public-key certificates (where applicable),

[11] Where public key cryptography is employed, the organization operating the key processing facility will generally perform most PKI registration authority, repository, and archive functions. The organization also performs at least some PKI certification authority functions. Actual X.509 public-key certificates may be obtained from a government source (certification authorities generating identification, attribute, or encryption certificates) or a commercial external certification authority (usually a commercial infrastructure/CA that supplies/sells X.509 certificates). Commercial external certification authority certificates **should** be cross-certified by a government root CA.

- Storage, backup, archiving, and recovery of keying material,
- Maintenance of a database that maps user entities to an organization's certificate or key structure,
- Maintenance and distribution of revoked key reports (see Section 2.6), and
- Generation of audit requests and the processing of audit responses as necessary for the prevention of undetected compromises.

An organization may use more than one key-processing facility to provide these services (e.g., for purposes of inter-organizational interoperation). Key-processing facilities can be added to meet new requirements or deleted when no longer needed and may support both public key and symmetric key-establishment techniques.

A key-processing facility may be distributed such that intermediary redistribution facilities maintain stores of keying material that exist in physical form (e.g., magnetic media, smart cards) and may also serve as a source for non-cryptographic products and services (e.g., software downloads for KMI-reliant users, usage documents, or policy authority).

Secret and private keys that are electronically distributed to end users **shall** be wrapped (i.e., encrypted and their integrity protected) for the end user or for intermediary redistribution services before transmission. Public keys and non-cryptographic products that are electronically distributed to end users **shall** be integrity protected.

Some key-processing facilities may generate and produce human-readable key information and other key-related information that require physical (i.e., manual) distribution. Keys that are manually distributed **shall** either 1) be cryptographically protected in the same manner as those intended for electronic distribution or 2) receive physical protection and be subject to controlled distribution (e.g., registered mail) between the key processing facility and the end user.

Part 1, Section 2.3.1 provides general guidance for key distribution. Newly deployed key-processing facilities **should** be designed to support legacy and existing system requirements and **should** be designed to support future network services as they become available.

2.3.3 Service Agents

Some key-management infrastructures may be large enough or support sufficiently complex organizations that it is impractical for organizations to receive keying material directly from a common key-processing facility. Intermediate distribution or service facilities, called *service agents*, may be employed to perform key-distribution processes.

Service agents support an organization's KMI(s) as single points of access for client nodes, when required by the infrastructure. When used, all transactions initiated by client nodes are either processed by a service agent or forwarded to a key-processing facility; when services are required from multiple key-processing facilities, service agents coordinate services among the key-processing facilities to which they are connected. A service agent that supports a major organizational unit or geographic region may either access a central or inter-organizational key-processing facility or employ local, dedicated processing facilities as required to support survivability, performance, or availability, requirements (e.g., a commercial external certification authority).

Service agents may be employed by users to order keying material and services, retrieve keying material and services, and manage cryptographic material and public-key certificates. A service agent may provide cryptographic material and/or certificates by utilizing specific key-processing facilities for key and/or certificate generation.

Service agents may provide registration, directory, and support for data-recovery services (i.e., using key recovery), as well as provide access to relevant documentation, such as policy statements and infrastructure devices. Service agents may also process requests for keying material, and assign and manage KMI user roles and privileges. A service agent may also provide interactive help-desk services as required.

2.3.4 Client Nodes

Client nodes are interfaces for human users, devices, and applications to access KMI functions, including the requesting of certificates and keying material. Client nodes may include cryptographic modules, software, and the procedures necessary to provide user access to the KMI. Client nodes interact with service agents (when used) or directly with key-processing facilities (when service agents are not used) to obtain cryptographic key services. Client nodes provide interfaces to end user entities (e.g., human users or devices) for the establishment of keying material, for the generation of requests for keying material, for the receipt and forwarding (as appropriate) of revoked key notifications (RKNs), for the receipt of audit requests, and for the delivery of audit responses.

Client nodes typically initiate requests for keying material in order to synchronize new or existing user entities with the current key structure and receive wrapped keying material for distribution to end-user cryptographic devices (in which the content – the plaintext keying material – is not usually accessible to human users or user-node interface processes). A client node can be a FIPS 140-validated workstation executing KMI security software or a FIPS 140-compliant special purpose device. Actual interactions between a client node and a service agent or a key-processing facility (in the event that a service agent is not used) depend on whether the client node is a device, a human user, or a functional security application.

2.3.5 Tokens

Tokens may be used by human users to interface with their systems that include the KMI's client node. These tokens typically contain information and keys that allow the user to interact with their systems by authenticating the user's identity to the system and providing keys for protecting communications. Examples of such tokens are the government's Personal Identification Verification (PIV) cards and Common Access Cards (CAC).

2.3.6 Hierarchies and Meshes

Multiple key-processing facilities may be organized so that subscribers from different domains may interact with each other. Two common constructions are hierarchies and meshes.

In a KMI hierarchy, as shown in Figure 2, multiple layers of key-processing facilities may be used, each with its own service agent(s) and client nodes, if appropriate (not shown in the figure). Each layer (except the top layer) is "dominated" in some way by a higher-level key-processing facility.

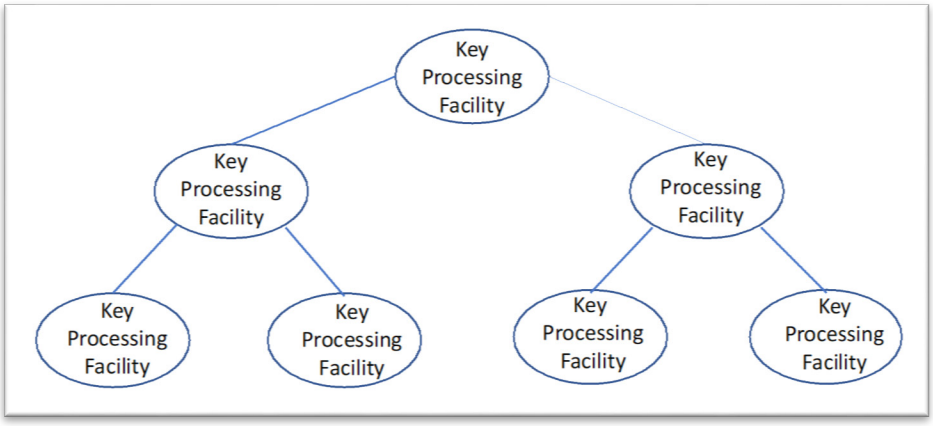

Figure 2: KMI Hierarchy

In a meshed KMI architecture, as shown in Figure 3, each key-processing facility may interact with some other key-processing facilities in the mesh, but no concept of dominance is implied by the architecture.

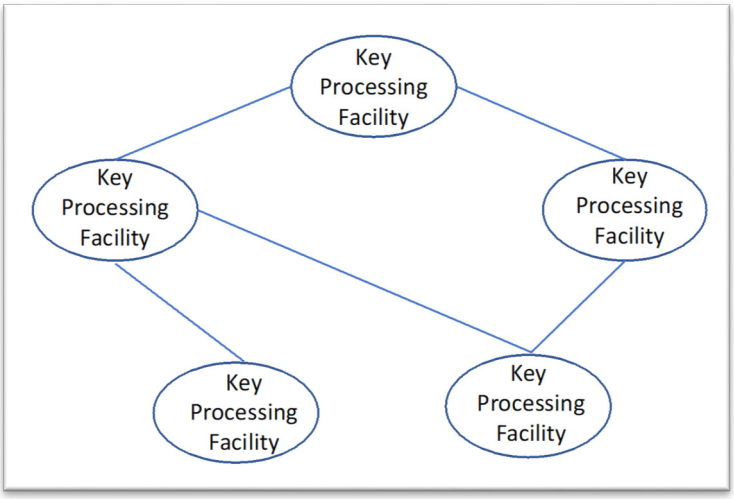

Figure 3: KMI Mesh Architecture

2.3.7 Centralized vs. Decentralized Infrastructures

Key-management infrastructures (KMIs) can be either centralized or decentralized in nature. For a PKI, the public key does not require protection, so decentralized key management can work efficiently for both large-scale and small-scale cases. The management of symmetric keys, particularly for large-scale operations, often employs a centralized structure.

Centralized key-management structures tend to be more structurally rigid than decentralized key-management structures, but the choice of how to establish keys, store and account for them, maintain an association of keys with the information protected under those keys, and dispose of keys that are no longer needed is a decision to be made by an organization's security management team. SP 800-57 Part 1 provides specific guidance regarding constraints associated with each key-

management function across the life cycle of keying material. This section provides general key-management design recommendations.

2.3.8 Cryptoperiods

In general, the keys used to protect bulk information should have relatively short periods of use. The use of long-term keys to protect this type of information increases the probability that the key that protects the data will be exposed to unauthorized entities and increases the amount of information that is compromised by such exposure. The short-term keys used during communication are often termed "session keys."

2.3.9 Available Automated Key Management Schemes and Protocols

The Internet Engineering Task Force has developed a significant body of work describing key-management schemes, protocols, and syntax. Though RFC 4107[12] has not been updated since 2005 and was largely overtaken by SP 800-57 Part 1, it remains an internationally recognized standard and includes advice and examples that are still useful. RFC 4107 notes in its Section 2 that automated key management involves the derivation of one or more short-term session keys. The RFC states that a key-derivation function may make use of long-term keys to incorporate authentication into the process. RFC 4107 does not prescribe the manner in which the long-term key is distributed to or established among the peers or the type of key used (pre-shared symmetric secret value, RSA public key, DSA public key, and others). Under RFC 4107, manual key management is used to distribute such values and can also be used to distribute long-term session keys. RFC 4107 notes that automated key management and manual key management provide very different features. The protocol associated with an automated key-management technique confirms the liveness of the peer, protects against replay, authenticates the source of the short-term session key, associates protocol state information with the short-term session key, and ensures that a fresh short-term session key is generated. RFC 4107 also notes that an automated key-management protocol can improve interoperability by including negotiation mechanisms for cryptographic algorithms.

Examples of automated key-management systems include IPsec IKE and Kerberos. S/MIME and TLS also include automated key-management functions. The design of key-management schemes is technically very challenging. The most frequent sources of vulnerabilities that result in an adversary defeating cryptographic mechanisms are vulnerabilities in key management (e.g., a failure to change session keys frequently or at all, protocol weaknesses, insecure storage, or insecure transport).

Some examples of IETF standards and guidelines for cryptographic key management include:

- RFC 4107, *Guidelines for Key Management*
- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4535, *GSAKMP: Group Secure Association Key Management Protocol*
- RFC 4758, *Cryptographic Token Key Initialization*

[12] RFC 4107, *Guidelines for Key Management*.

- RFC 4962, *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management*
- RFC 5083, *Cryptographic Message Syntax (CMS) Authenticated Enveloped-Data Content Type*
- RFC 5272, *Certificate Management Over CMS (CMC)*
- RFC 5275, *CMS Symmetric Key Management and Distribution*
- RFC 5652, *Cryptographic Message Syntax (CMS)*
- RFC 6030, *Portable Symmetric Key Container (PSKC)*
- RFC 6031, *Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type*
- RFC 6063, *Dynamic Symmetric Key Provisioning Protocol (DSKPP)*
- RFC 6160, *Algorithms for Cryptographic Message Syntax (CMS)*
- RFC 6402, *Certificate Management Over CMS (CMC) Updates*

2.4 General KMI Design Requirements

Regardless of the key-management structure, any key-management system design **should** describe how it provides cryptographic keys to the entities that will use those keys to protect sensitive data. The key-management system design documentation **should** specify the use of each key type, where and how keys can be generated, how they can be protected in storage and during delivery, and the types of entities to whom they can be delivered.

SP 800-152 contains requirements for the design, implementation, and procurement of a cryptographic key management system (CKMS). A key-management system can be designed to provide services for a single individual (e.g., in a personal data-storage system), an organization (e.g., in a secure VPN for intra-office communications), or a large complex of organizations (e.g., in secure communications for the U.S. Government). A key-management system can be owned or rented. However, regardless of the design or source for the key-management system, the recommendations of SP 800-57 Part 1 **shall** be followed.

2.5 Trust

Because the compromise of a cryptographic key compromises all of the information and processes protected by that key, it is essential that clients be able to trust that keys and/or components of keys come from a trusted source and that they've been protected both in storage and in transit from modification or exposure. In the case of secret keys, the exposure of a key by any member of a communicating group or on any link between any pair in that group exposes all of the information shared by the group that was protected by the same key. As a result, it is important to avoid accepting a key from an unauthenticated source,[13] to protect all keys and key components in transit, and to protect stored keys for as long as any information protected under those keys requires protection. Cryptographic confidentiality and integrity mechanisms are most commonly used to

[13] Note that, in TLS, unauthenticated clients do send keys to servers. This is permitted where the server is only serving publicly-available information and the TLS session is used to (1) ensure the client of the integrity and source of the information and (2) protect the privacy of the client so that others cannot see what information the client has chosen to access.

establish anchors that enforce trust policies and practices. A *trust anchor* is an authoritative entity for which trust is assumed and not derived. For example, in a public key infrastructure (PKI), the trust anchor is a certification authority (CA) that may be the issuer of the first certificate in a certification path. "Trust anchor" also refers to the public key of this CA.

2.6 Revocation and Suspension

Key revocation is used in cases where the authorized use of a key needs to be terminated prior to the end of the established cryptoperiod of that key. Keys may be routinely revoked at the end of the period that had been established for their authorized use, or they may be revoked on an emergency basis if there is reason to believe that they may have been disclosed to or otherwise accessed by unauthorized entities. In either case, a cryptographic key should be revoked as soon as feasible after its use is no longer authorized. Entities that have been, that are, or that would be using the key (e.g., relying parties) need to be notified that the key has been revoked. Methods for notifying these entities in the PKI world include the publication of certificate revocation lists (CRLs) and/or compromised key lists (CKLs), and the use of online status mechanisms, such as the Online Certificate Status Protocol (OCSP). These methods often include the reason for the revocation (e.g., a key has been compromised or the key's owner(s) is no longer authorized to use it) and the date and time when they were revoked.

Irrespective of whether symmetric or asymmetric keys are used, a means of revoking keys is required. This Recommendation will use the term *revoked key notification* (RKN) to refer to a mechanism to revoke keys that may include the revocation reason and an indication when the revocation was requested. The inclusion of the revocation reason can be useful in risk decisions regarding the trust to associate with information that was received or stored using those keys.

A key may also be suspended from use for a variety of reasons, such as an unknown status of the key or due to the key owner being temporarily away. In the case of the public key, suspension of the companion private key is communicated to the relying parties. This may be communicated as an "on hold" revocation reason code in a CRL and in an Online Certificate Status Protocol (OCSP) response.

3 Key-Management Policy and Practices

A key-management policy is a set of rules that are established to describe the goals, responsibilities, and overall requirements for the management of the cryptographic keying material used to protect private or critical facilities, processes, or information. Key management policies are also referenced in SP 800-130[14] and SP 800-152.[15]

Key management policies (KMP) are implemented through a combination of security mechanisms and procedures. An organization uses security mechanisms (e.g., safes, alarms, random number generators, encryption algorithms, signature, and authentication algorithms) as tools to implement a policy. However, key-management mechanisms will produce the desired results only if they are properly configured and maintained.

Key-management practice statements (KMPS) document the procedures that system administrators and users follow when establishing and maintaining key-management mechanisms using cryptographic systems. The procedures documented in the KMPS describe how the security requirements in the KMP are met and are directly linked to the key-management mechanisms employed by an organization (see PKI 01).

U. S. Government agencies that use cryptography are responsible for defining the KMP that governs the lifecycle for the cryptographic keys as specified in Section 6.3 of SP 800-152 and in Part 1, Sections 7 and 8. A KMPS is then developed, based on the KMP and the actual applications supported.

Policy and practices documentation requirements associated with small scale or single-system cryptographic applications will obviously not be as elaborate as those required for large and diverse government agencies that are supported by a number of information technology systems. However, any organization that employs cryptography to provide security services is likely to require some level of policy, practices and planning documentation.

3.1 Key Management Policy (KMP)

Each organization that manages cryptographic systems that are intended to protect sensitive information **should** base the management of those systems on an organizational policy statement. The KMP[16] is a high-level document that describes the authorization and protection objectives and constraints that apply to the generation, establishment, accounting, storage, use, and destruction of cryptographic keying material. Section 4 of SP 800-130, and Section 4 of SP 800-152 describe the relationship of cryptographic key-management system security policies in the context of the organization's overall information management policy, information security policy, and other related security policies.

3.1.1 Policy Content

The policy document or documents that comprise the KMP include high-level key management structure and responsibilities, governing standards and guidelines, organizational dependencies and other relationships, and security objectives. Most currently available guidance for KMP

[14] SP 800-130, *A Framework for Designing Cryptographic Key Management Systems.*
[15] SP 800-152, *A Profile for US Federal Cryptographic Key Management Systems.*
[16] In a purely PKI environment, the KMP may be a certificate policy (CP) in conformance to RFC 3647, the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

development is focused primarily on the use of asymmetric algorithms and X.509 certificate-based key establishment and transport environments. Though some interpretation is required[17] in applying KMP templates to organizations that employ symmetric algorithms for key establishment, most of the guidance applies to these environments as well. Note that in a purely public key infrastructure (PKI) environment, the KMP is usually a stand-alone document known as a certificate policy (CP).[18] Also, note that certificate issuance organizations also publish CPs.[19] The scope of a KMP may be limited to the management of certificates in a single PKI certification authority (CA) and its supporting components,[20] or to a symmetric point-to-point or single key-center environment.[21] Alternatively, the scope of a KMP may include certificate management in a hierarchical PKI, bridged PKI, or multiple-center symmetric-key environments.

The KMP is used for a number of different purposes. The KMP is used to guide the development of KMPSs for each CA or symmetric key-management group that operates under its provisions. CAs from other organizations' PKIs may review the KMP before cross-certification, and managers of symmetric-key KMIs may review the KMP before joining new or existing multiple-center groups. Auditors and accreditors will use the KMP as the basis for their reviews of CA and/or symmetric-key KMI operations. Application owners that are considering a PKI certificate source **should** review a KMP/CP to determine whether its certificates are appropriate for their applications.

3.1.2.1 General Policy Content Requirements

Although detailed formats are specified for some environments (e.g., see Appendix A for a PKI CP format), the policy documents into which key-management information is inserted may vary from organization to organization. In general, the information **should** appear in top-level organizational information systems policies and practices documents. The policy need not always be elaborate. A degree of flexibility may be desirable with respect to actual organizational assignments and operations procedures in order to accommodate organizational and information infrastructure changes over time. However, the KMP needs to establish a policy foundation for the full set of key management functions.

3.1.2.1.1 Security Objectives

A KMP **should** state the security objectives that are applicable to and expected to be supported by the KMI. The security objectives **should** include the identification of:

(a) The nature of the information to be protected (e.g., financial transactions, confidential information, critical process data);

[17] For example, the use of key-encrypting keys for key wrapping, compromised key lists rather than certificate revocation lists, and message authentication codes rather than digital signatures.

[18] Examples include *Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate* Policy (Treasury CP), *Reference Certificate* Policy (NISTIR 7924), the *United States Department of Defense X.509 Certificate Policy* (DoD Cert Policy), and the *CNSS Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy* (CNSSI 1300).

[19] For example, the *CertiPath X.509 Certificate Policy* (CP X509 CP).

[20] This is generally the case when a single CA serves an enterprise or a CA participates in a mesh. (PKI 01).

[21] Note that multiple CAs and/or single symmetric point-to-point or multiple-center groups may operate under a single KMP.

(b) The classes of threats against which protection is required (e.g., the unauthorized modification of data, the replay of communications, the fraudulent repudiation of transactions, the disclosure of information to unauthorized parties);

(c) The FIPS 199[22] impact level that is determined by the consequences of a compromise of the protected information and/or processes (including the sensitivity and perishability of the information);

(d) The cryptographic protection mechanisms to be employed (e.g., message authentication, digital signatures, encryption);

(e) The protection requirements for cryptographic processes and keying material (e.g., tamper-resistant processes, confidentiality of keying material); and

(f) Applicable statutes, and executive directives and guidance to which the KMI and its supporting documentation **shall** conform.

The statement of security objectives will provide a basis and justification for other provisions of the KMP.

3.1.2.1.2 Organizational Responsibilities

The KMP **should** identify the required KMI management responsibilities and roles, including organizational contact information. The following classes of organizational responsibilities **should** be identified:

(a) Identification of an Individual Having Ultimate Responsibility for Key Management Within the Organization (e.g., keying material manager) – Since the security of all material that is cryptographically protected depends on the security of the keying material employed, the ultimate responsibility for key management **should** reside at the executive level. The individual responsible for keying material management functions **should** report directly to the organization's Chief Information Officer (CIO).[23] The individual responsible for keying material management **should** have the capabilities and trustworthiness commensurate with the responsibility for maintaining the authority and integrity of all formal, electronic transactions and the confidentiality of all information that is sufficiently sensitive to warrant cryptographic protection.

(b) Identification of Infrastructure Entities and Roles - The key management policy document **should** identify organizational responsibilities for critical KMI roles. The following roles (where applicable to the type and complexity of the infrastructure being established) **should** be assigned and their responsibilities specified:

- Central oversight authority (may be the keying material manager),
- Oversight for relationships with certification authorities (CAs),
- Oversight for relationships with registration authorities (RAs),
- Compliance auditor (ensures compliance with regulations and internal controls), and

[22] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

[23] When an organization does not have a CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

- Oversight for operations (e.g., key processing facility (ies), service agents).

(c) Basis for and Identification of Essential Key Management Roles – The KMP **should** also identify responsible organization(s), organization (not individual) contact information, and any relevant statutory or administrative requirements for the following functions, at a minimum:

- Key generation or acquisition;
- Agreements with partner organizations regarding the cross-certification of keying material and/or key establishment, as appropriate;
- Key establishment;
- Establishment of cryptoperiods;
- Establishment of and accounting for keying material;
- Protection of secret and private keys and related materials;
- Emergency and routine revocation of keying material (e.g., revocation due to compromise of a key);
- Auditing of keying material and related records;
- Destruction of revoked or expired keys;
- Key recovery;
- Compromise recovery;
- Contingency planning;
- Disciplinary consequences for the willful or negligent mishandling of keying material; and
- Generation, approval, and maintenance of key management policies and practice statements.

3.1.2.1.3 Sample KMP Format

The sample format provided in this subsection is designed to be compatible with the standard format for PKI certificate policies (Appendix A). The sample format differs somewhat from that for PKI certificate policies (CPs) because some key management characteristics of and requirements for KMIs that accommodate symmetric keys differ from those for purely PKI-based KMIs. The sample KMP format below includes the general information called for in Subsections 3.1.2.1.1 and 3.1.2.1.2 above, plus some additional material that may be required in some administrative environments. As stated above, variations among organizational structures and needs will necessarily result in variations in the form and content of policy documentation. The sample KMP format is provided as a general guide rather than as a mandatory template.

(a) *Introduction* -

The *Introduction* identifies and introduces the provisions of the policy document and indicates the security objectives and the types of entities and applications for which the

KMP is targeted. This section has the following subsections: 1) Overview, 2) Identification, 3) Community and Applicability, and 4) Contact Details.

Overview - This subsection introduces the KMP.

Objectives – This subsection states the security objectives applicable to and expected to be supported by the KMI. The *Objectives* subsection **should** include the elements of information called for in Section 3.1.2.1.1 above (Security Objectives). (Note that in the case of a CP for a purely PKI environment, the *Overview* is followed by an *Identification* subsection that provides any applicable names or other identifiers, including ASN.1 object identifiers, for the set of policy provisions.)

Community and Applicability - This subsection identifies the types of entities that establish keys or distribute certificates. In the general case of the KMI, this will include the responsible entities identified in the "Identification of Infrastructure Entities and Roles" element of Section 3.1.2.1.2 above (Organizational Responsibilities). (Note that in the case of a KMI that includes a PKI CA, this subsection **should** identify the types of entities that issue certificates or that are certified as subject CAs, the types of entities that perform RA functions, and the types of entities that are certified as subject end entities or subscribers.) This subsection may also contain:

- A list of applications for which the issued certificates and/or identified key types are suitable. (Examples of applications in this case are: electronic mail, retail transactions, contracts, travel orders, etc.)
- A list of applications to which the use of the issued certificates and/or identified key types is restricted. (This list implicitly prohibits all other uses for the certificates or key types.)
- A list of applications for which the use of the issued certificates and/or identified key types is prohibited.

Contact Details - This subsection includes the organization, telephone number, and mailing and/or network address of the keying material manager. This is the authority responsible for the registration, maintenance, and interpretation of the KMP (see Section 3.1.2.1.2).

(b) *General Provisions* –

The *General Provisions* section of the KMP identifies any applicable policies regarding a range of legal and general practices topics. This section may contain subsections covering 1) obligations, 2) liability, 3) financial responsibility, 4) interpretation and enforcement, 5) fees, 6) publication and repositories, 7) compliance auditing, 8) confidentiality, and 9) intellectual property rights. Each subcomponent may need to separately state the provisions applying to each KMI entity type (e.g., central oversight authority, key processing facility, service agent, client node, PKI CA, PKI repository, PKI RA, PKI subscriber, key recovery agent (KRA) and/or PKI relying party[24]). Note that many of the general provisions require input from and/or review by procurement elements of the organization.

[24] Specific provisions regarding subscribers and relying parties are only applicable in the Liability and Obligations subcomponents.

Obligations - This subsection contains, for each entity type, any applicable policies regarding the entity's obligations to other entities. Such provisions may include: 1) keying material manager and/or central oversight authority obligations, 2) key processing facility obligations, 3) service agent obligations, 4) CA and/or RA obligations (PKI), 4) User obligations (including client nodes and PKI subscribers and relying parties), 5) KRA obligations and 6) keying material repository obligations.

Liability - This subsection contains, for each entity type, any applicable policies regarding the apportionment of liability (e.g., warranties and limitations on warranties, kinds of damages covered and disclaimers, loss limitations per certificate or per transaction, and other exclusions (e.g., acts of God).

Financial Responsibility - For key and/or certificate providers (e.g., key processing facilities, PKI CAs, key or certificate repositories, PKI RAs), this section contains any applicable policies regarding financial responsibilities, such as 1) an indemnification statement 2) fiduciary relationships (or lack thereof) among the various entities; and 3) administrative processes (e.g., accounting, audit).

Interpretation and Enforcement - This subsection contains any applicable policies regarding the interpretation and enforcement of the KMP or KMPS, addressing such topics as 1) governing law; 2) dispute resolution procedures; and 3) other technical contract issues, such as the severability of provisions, survival, merger, and notice.

Fees - This subsection contains any applicable policies regarding interagency reimbursement or fees charged by key and/or certificate providers (e.g., reimbursement for key-center management, certificate issuance or renewal fees, a certificate access fee, revocation or status information access fee, key recovery fee, reimbursement for information desk services, fees for other services such as policy information, refund policy).

Publication and Repositories - This subsection contains any applicable policies regarding 1) a key and/or certificate source's obligations, where keys are not locally generated, to publish information regarding its practices, its products (e.g., keys, certificates), and the current status of such products; 2) the frequency of publication; 3) access control on published information (e.g., policies, practice statements, certificates, key and/or certificate status, RKNs); and 4) requirements pertaining to the use of repositories operated by private-sector CAs or by other independent parties.

Compliance Audit[25] - This subsection addresses any high-level policies regarding 1) the frequency of compliance audits for KMI entities, 2) the identity/qualifications of the compliance auditor, 3) the auditor's relationship to the entity being audited, 4) topics covered under the compliance audit,[26] 5) actions taken as a result of a deficiency found during a compliance audit, and 6) the dissemination of compliance audit results.

Confidentiality Policy - This subsection states policies regarding 1) the types of information that **shall** be kept confidential by KMI entities, 2) the types of information that

[25] Note that a compliance auditor (who audits the procedures against the practice statements and policies) is different than an auditor that looks at the information recorded by an operational system (e.g., key generation, key recovery, etc.) as defined in Section 2.

[26] May be by reference to audit guidelines documents.

are not considered confidential, 3) the dissemination of reasons for the revocation of certificates and symmetric keys, 4) the release of information to third parties (e.g., legal entities), 5) information that can be revealed as part of civil discovery (e.g., material that may be subject to FOIA or subpoena in civil actions), 6) the disclosure of keys or certificates by KMI entities at subscriber/user request; and 7) any other circumstances under which confidential information may be disclosed.

Intellectual Property Rights - This subsection addresses policies concerning the ownership rights of certificates, practice/policy specifications, names, and keys.

(c) *Identification and Authentication* –

The *Identification and Authentication* section describes circumstances and identifies any applicable regulatory authority and guidelines regarding the authentication of a certificate applicant or key requestor[27] prior to the issuing of key(s) or certificate(s) by a keying material source. This section also includes policies regarding the authentication of parties requesting re-keying, key recovery or revocation. Where applicable, this section also addresses KMI naming practices, including name ownership recognition and name dispute resolution. This section of the KMP has the following subsections:

- Initial Registration,
- Routine Re-keying,
- Re-keying After Revocation,
- Key Recovery, and
- Revocation Request.

(d) *Operational Requirements* –

The *Operational Requirements* section specifies policies regarding the imposition of requirements on KMI entities with respect to various operational activities. This section may address the following topics:

- Request for actions needed to establish shared-key relationship (e.g., a symmetric key to be shared between two entities),
- Initial issuance of key wrapping keys and/or certificate issuance,
- Validity checking and acceptance of keys and certificates,
- Key and/or certificate suspension and revocation,
- Security audit requirements,
- Key backup and archiving,
- Records archiving,
- Key changeover (i.e., re-keying and key derivation),
- Key recovery,

[27] An entity that requests a new key for use; distinct from a key recovery requestor.

- Compromise and disaster recovery, and
- Key service termination (e.g., key center, CA, key storage).

Within each topic, separate consideration may need to be given to each type of KMI component.

(e) *Minimum Baseline Security Controls* –

This section states the policies regarding the management, operational, and technical security controls (e.g., physical, procedural, and personnel controls) used by KMI components to securely perform 1) key generation, 2) entity identity authentication, 3) key establishment and/or certificate issuance, 4) key and/or certificate revocation, 5) auditing, and 6) key storage and recovery (i.e., to and from backups and archives).

For federal government systems, based on the FIPS 199 impact level, the appropriate minimum baseline of security controls contained in SP 800-53[28] **shall** be implemented and described in this section of the KMP.

(f) *Cryptographic Key, Message Interchange, and/or Certificate Formats* –

This section is used to state policies specifying conformance to specific standards and/or guidelines regarding 1) key management architectures and/or protocols, 2) key management message formats, 3) certificate formats and/or 4) RKN formats.

(g) *Specification and Administration* –

This section of the policy document specifies:

- The organization(s) that has change-control responsibility for the KMP,
- Publication and notification procedures for new KMP versions, and
- KMPS approval procedures.

3.1.3 Policy Enforcement

In order to be effective, key management policies **shall** be enforced, and policy implementation **should** be evaluated on a regular basis. Each organization will need to determine its requirements based on the sensitivity of information being exchanged or stored; the communications volume associated with sensitive or critical information and processes; the storage required for operational, backed-up and archived keys; provisions for key recovery; personnel resources; the size and complexity of the organization or organizations supported; the variety and numbers of cryptographic devices and applications; the types of cryptographic devices and applications; and the scale and complexity of protected communications facilities.

3.2 Key Management Practices Statement (KMPS)

The key management practices statement (KMPS) establishes a trust root for the KMI and specifies how key management procedures and techniques are used to enforce the KMP. For example, a KMP might state that secret and private keys **shall** be protected from unauthorized disclosure. The corresponding KMPS might then state that secret and private keys **shall** be either cryptographically wrapped or physically protected, and that it is the responsibility of the network systems

[28] SP 800-53: *Recommended Security Controls for Federal Information Systems*.

administrator to ensure that the keys are properly safeguarded. (The KMPS would also identify and provide contact information for the network systems administrator.) Note that the practices information contained in a KMPS is more prescriptive and specific than policy material contained in a KMP, so it will be subject to more frequent change. Several KMPSs may implement a KMP for a single organization, one for each organizational key management domain (e.g., one for each of several CAs).

3.2.1 Alternative KMPS Formats

As in the case of the policy documentation, the plans, practices, and/or procedures documents into which KMPSs are inserted will vary from organization to organization. In general, the nature and complexity of the KMPS will vary with an organization's existing documentation requirements and the size and complexity of an organization's key management infrastructure.

Each KMPS applies to a single KMI or a single domain of that KMI. The KMPS may be considered the overall operations manual for the KMI. Specific portions of the KMPS may be extracted to form a KMI operations guide, a CA operations guide, a service agent manual, a key distribution center manual, a key translation center manual, a key storage and recovery manual, an RA manual, a PKI users' guide, or other application or role-specific documentation. Auditors and accreditors may use the KMPS to supplement the KMP during reviews of KMI operations.

3.2.1.1 Stand-Alone KMPS

While it is recommended that organizations create stand-alone practices documents, the key management practice information may be included in pre-existing top-level organizational information security policies and/or security procedures documents. A stand-alone KMPS may follow the general RFC 3647 format described for the KMP in Section 3.1.2.1.3 above (Sample KMP Format), or it may follow a proprietary format. If the general outline of the sample KMP format is followed, the authors of the KMP will need to keep in mind the basic differences in character between a KMP and a KMPS. While the KMP is a high-level document that describes a security policy for managing keys, the KMPS is a highly detailed document that describes how a KMI implements a specific KMP. The KMPS identifies any KMPs that it implements and specifies the mechanisms and procedures that are used to support each KMP. Where the KMP specifies organizational roles and states requirements for mechanisms and procedures, the KMPS identifies more specific roles and responsibilities, and describes the mechanisms and procedures in detail. (Note that descriptive material can sometimes be included by reference to other procedures, guidelines, and/or standards documents.) The KMPS **should** include sufficient operational detail to demonstrate that the KMP can be satisfied by this combination of mechanisms and procedures.

3.2.1.2 Certification Practices Statement

A certification practices statement (CPS) is a PKI-specific document. In a purely PKI environment, the RFC 3647-specified CPS may serve as the KMPS for a CA. In such cases, the CPS will follow the RFC 3647 format summarized in Appendix A.

3.2.1.3 Information Technology System Security Plans

All government organizations are required by OMB Circular A-130 to develop security plans for their information technology systems. The use of the format offered in "Information Technology Systems Security Plans" (Section 4 below) will assist in the development of a security plan that

945 incorporates key-management information.[29] Appendix B suggests key-management inserts for a
946 Security Plan Template.

947 ### 3.2.2 Common KMPS Content

948 Regardless of the KMPS format employed, the KMPS needs to include a minimum set of
949 information. This subsection identifies the kinds of information that **should** be included in all
950 KMPSs, when appropriate.

951 #### 3.2.2.1 Association of KMPS with the KMP

952 The KMPS **should** identify the KMI to which it applies and the KMP that its content implements.

953 #### 3.2.2.2 Identification of Responsible Entities and Contact Information

954 The KMPS **should** identify the organizational entities that perform the various functions identified
955 in the Organizational Responsibilities section (Section 3.1.2.1.2). The individuals assigned to
956 perform each key management role **should** be identified (e.g., by title). Contact information
957 **should** include the entity's identity (e.g., a title), organization, business address, telephone number,
958 and electronic mail address.

959 #### 3.2.2.3 Key Generation or Acquisition

960 The KMPS **should** prescribe key generation and acquisition functions. Key generation and/or
961 acquisition **should** be accomplished in accordance with the guidelines contained in the key
962 establishment sections of Part 1 (Section 8.1.5). The scope of key acquisition includes out-of-band
963 procedures for acquiring initial keying material and replacement keying material (e.g., initial key
964 wrapping keys for communication with key centers and service agent's procedures for emergency
965 replacement of compromised keys). The KMPS generally identifies:

966 • Any management organization, roles, and responsibilities associated with key generation
967 and/or acquisition,

968 • Any standards and guidelines governing key generation/acquisition facilities and
969 processes, and

970 • Any documents required for authorization, implementation, and accounting functions.

971 For organizations that employ public-key cryptography, the KMPS **should** identify the certificate
972 issuance elements of the CA (and its hardware, software, and human/organizational components
973 as appropriate), as well as registration entities.

974 Operating procedures and quality control procedures for key generation and/or acceptance of
975 acquired keying material may appear either in the KMPS or in separate documents referenced by
976 the KMPS. Documentation of the key generation process **should** also be included in order to
977 establish a chain of evidence to support the establishment of the trusted source of keying material
978 (e.g., a trust root for public key certificates or a symmetric key processing center.

979

980

[29] Note also that SP-800-37 also requires Information Technology Security Plans as part of Certification and Accreditation documentation.

3.2.2.4 Key Agreement

Key agreement, as defined in Part 1 (Section 2.1), involves participation by more than one entity in the creation of shared keying material. Public key techniques are normally employed to accomplish key agreement. KMPSs may prescribe the organizational authority and procedures for authorizing and implementing key agreement between or among partner organizations. Within the context of a KMI, key agreement will commonly be implemented by *client nodes*, using key agreement keys or key pairs received from *key processing facilities*.

3.2.2.5 Cross-Certification Agreements

Organizations that have distinct public key certification hierarchies or meshes (see Section 2.3.6), but require secure communications between their domains may agree to cross-certify their organizations' CAs. Similarly, in centralized symmetric key management structures, key processing facilities may function as key distribution *centers* (see Appendix A.2).[30] Where entities within different organizations need to communicate securely with each other, the key processing facilities that serve them will need to establish formal agreements to work together to provide cryptographic services to their subscribers. In both cases, a formal *cross-certification agreement* is required. KMPSs (also known as CPSs in PKIs) may prescribe the organizational authority and procedures for authorizing and implementing the cross-certification of keying material between or among partner organizations. Within the context of the KMI, any authorization for cross-certification **should** come from the central oversight authority or its organizational equivalent. Cross-certification will normally be implemented in the key processing facility or its equivalent.

3.2.2.6 Key Establishment, Suspension and Revocation Structures

The KMPS **should** prescribe the organizational authority and procedures for the design and management of the organizational structure and information flow necessary to meet the organization's key establishment, suspension,[31] and revocation[32] requirements. The KMPS **should** include or reference guidelines for maintaining the continuity of operations and maintaining both the assurance and integrity of the revocation process. The KMPS **should** include guidelines for the emergency replacement of keys, compromise lists, and revocation lists as well as timely and the reliable routine establishment of keying material. Both the initial key establishment and subsequent changes to key establishment, suspension and revocation procedures **should** be authorized by the central oversight authority and implemented by the key processing facility (or their equivalents) as described in the KMI discussion (see Section 2.3.2). Additionally, a prescription of the audit and control of the key establishment process is necessary in order to maintain confidence in the integrity of the source of keying material.

3.2.2.7 Establishment of Cryptoperiods

The KMPS **should** prescribe cryptoperiods[33] for the keying material employed by an organization. Cryptoperiods **should** be approved by the central oversight authority, or its organizational

[30] These centers may establish formal agreements to share a common identity as a *multiple center group*.

[31] The validity of keys or certificates may be temporarily suspended for administrative or security reasons.

[32] Note that both public key certificates and symmetric keys may be revoked for a variety of reasons (administrative reasons, expiration of the key's assigned crypto period, or compromise).

[33] If a key is retained indefinitely for operational use (e.g., for encryption, decryption, or signing), the probability that it will become known through cryptanalysis, technical probing, malware, carelessness, or other methods increases over time. Depending on the criticality, volume, or perishability of the information being protected, longer or shorter

equivalent, and **should** be implemented by the CA or key processing facility and client nodes (or their equivalents), as described in the KMI discussion (see Section 2.3). Recommendations for establishing cryptoperiods are provided in Section 5.3 of Part 1.

3.2.2.8 Tracking of and Accounting for Keying Material

For keys distributed from a CA or other key processing center rather than established at client nodes using key agreement or other automated key establishment techniques, the KMPS **should** prescribe the organizational authority and procedures for any distribution of, local creation of, and accounting for keying material required at each phase of the key management lifecycle (see Part 1, Sections 7 and 8). General accountability recommendations are provided in Section 9 of Part 1. Responsibilities and procedures **should** be identified for the central oversight authority, CA or other key processing facility, service agent, and client node entities of the KMI (or their equivalents). For keys distributed from a CA/key processing center rather than established at client nodes using key agreement or other automated key establishment techniques, any relevant accounting forms and database structures **should** be specified as required for:

- Keying material requests,
- Keying production authorization,
- The authorization of the distribution of specific material to specific organizational destinations for use in specific devices,
- Physical or automated establishment of keys or related cryptographic materials,
- Receipts for keys or related cryptographic material,
- Reporting of the receipt of keys not accompanied by authorized transmittal information,
- Backup and archiving of keying material,
- Requesting the recovery of backed up or archived keying material, and
- The destruction of keys or related cryptographic materials.

3.2.2.9 Protection of Keying Material

The KMPS **should** prescribe the responsibilities, facilities, and procedures for the protection of secret and private keys and related cryptographic materials, including public key certificates. This includes requirements for cryptographic materials both in transit and in storage. Requirements **should** be specified for the central oversight authority, CA or other key processing facility, service agent, and client node entities of the KMI (or their equivalents). General recommendations for the protection of keying material at different lifecycle stages (provided in Part 1, Sections 7 and 8) **should** be included or referenced in the KMPS.

Note that where keys and key establishment security mechanisms are integral to a FIPS 140-compliant cryptographic module or application, reference to FIPS 140 and any local physical security procedures may provide an adequate specification of protection practices.

operational lifetimes may be established for cryptographic keying material. Some private-sector organizations neither change key variables nor make provision for users to change cryptographic keys. This is not recommended if the information has any privacy or security value. Ideally, a user's organization controls cryptoperiod determinations for the keys that protect their information.

3.2.2.10 Suspension and Revocation of Keying Material

The KMPS **should** prescribe the roles, responsibilities, and procedures for the suspension, and emergency[34] and routine[35] revocation of keying material. The KMPS **should** also prescribe the roles, procedures, and protocols employed at the key processing facility for the generation of RKNs for prematurely lost or destroyed certificates and keys, or for compromised certificates and keys.

The KMPS **should** also specify the roles, procedures, and protocols employed by service agent and client node entities, or their organizational equivalents, for the timely and secure reporting of potential compromises. The KMPS **should** identify the key types and reasons for which suspension and revocation actions are taken (e.g., suspension: key owner is on leave or a key compromise is suspected; revocation: key compromise or the key owner is leaving the organization); suspension and revocation are not necessary for ephemeral keys. General recommendations for key revocation are provided in Part 1, Section 8.3.5 and **should** be included or referenced in the KMPS.

3.2.2.11 Auditing

The KMPS **should** prescribe the roles, responsibilities, facilities, and procedures for the routine auditing of keying material and related records, including their generation, access and destruction. The KMPS **should** also describe audit reporting requirements and procedures. Auditing **should** occur wherever keys are handled (generated, stored, recovered, or destroyed). Note that audit requirements will depend on the sensitivity of the information (including what is to be audited, the frequency of audits, and the frequency of reviews of different elements of the audit log). Note also that audits will generally be conducted in facilities that distribute or receive keys (e.g., CAs or other key processing centers) rather than for cryptographic devices that use automatically established keys. Conditions and procedures **should** also be included for unscheduled audits that are triggered by the observed and/or suspected unauthorized access, production, loss, or compromise of keys or related cryptographic material. General audit recommendations are provided in Part 1, Section 9.2 and SP 800-152, Section 8.4.

Note that where keys and key establishment security mechanisms are integral to a FIPS 140-compliant cryptographic module or application, and the keys are relatively short-term and employed for protection within a client node or between communicating pairs of client nodes, it may not be practical or necessary to document or audit those keys.

3.2.2.12 Keying Material Destruction

The KMPS **should** prescribe the roles, responsibilities, facilities, and procedures for any routine destruction of revoked or expired keys required at all KMI elements. Key destruction conditions and procedures may also be included. Part 1 (Sections 8.3.4 and 8.4) and SP 800-152 (Section 6.4.9) include recommendations that **should** be included or referenced in the KMPS. Note that the destruction of keying material is not accomplished until all copies are destroyed (including backups). Keying material in archives may need to be retained for later retrieval, but **should** be destroyed when no longer needed.

[34] An example of emergency revocation is revocation due to the known or suspected compromise of a key or key processing center.

[35] An example of routine revocation is revocation due to the expiration of the period for which the key's use is authorized.

3.2.2.13 Key Backup, Archiving and Recovery

OMB Guidance to Federal Agencies on Data Availability and Encryption, 26 November 2001, states that agencies **must** address information availability and assurance requirements through appropriate data recovery mechanisms such as cryptographic key recovery. The KMPS **should** prescribe, for each KMI element, any roles, responsibilities, facilities, and procedures necessary for all organizational elements to backup, archive and recover critical keying material, with the necessary integrity mechanisms intact, in the event of the loss or expiration of the operational copy of cryptographic keys under which the data is protected. Key backup, archive and recovery are normally the responsibility of the central oversight authority, or its organizational equivalent, although mechanisms to support recovery may be included in other components of a KMI. Part 1, Appendix B contains general key recovery recommendations that **should** be included in or referenced by the KMPS. Examples of key recovery policies include the *Key Recovery Policy for The Department of the Treasury Public Key Infrastructure (PKI)*, *Federal Public Key Infrastructure Key Recovery Policy*, and *Key Recovery Policy for External Certification Authorities*.

3.2.2.14 Compromise Recovery

For all KMI elements, the KMPS **should** prescribe any roles, responsibilities, facilities, and procedures required for recovery from the compromise of cryptographic keying material at any phase in its lifecycle. Compromise recovery includes 1) the timely and secure notification of users of compromised keys that the compromise has occurred and 2) the timely and secure replacement of the compromised keys. Emergency key revocation and the generation and processing of RKNs are elements of compromise recovery, but compromise recovery also includes:

- The recognition and reporting of the compromise,
- The identification and/or establishment of replacement keying material,
- Recording the compromise and compromise recovery actions (may use existing audit mechanisms and procedures), and
- The destruction and/or de-registration of compromised keying material, as appropriate.

Part 1 (Sections 9.3.4 and 10.2.9) and SP 800-152 (Section 6.8) contain recommendations regarding compromise recovery that **should** be included in or referenced by the KMPS.

3.2.2.15 Policy Violation Consequences

The KMPS **should** prescribe any roles, responsibilities, and procedures required for establishing and carrying out disciplinary consequences for the willful or negligent mishandling of keying material. The consequences **should** be commensurate with the potential harm that can result from the violation of the organization's policy, its mission, and/or other affected organizations. While the procedures apply to all KMI elements, the responsibility for establishing and enforcing the procedures rests at the central oversight authority or its organizational equivalent. Consequences prescribed in a KMPS **shall** be enforced if they are to be effective. Note also that it is necessary to correlate compromise records and the associated audit logs to the disciplinary actions that are taken as a result of violations of policies or procedures.

3.2.2.16 Documentation

The KMPS **should** prescribe any roles, responsibilities, and procedures required for the generation, approval, and maintenance of the KMPS. The generation, approval, and maintenance of KMPSs are normally the responsibilities of the central oversight authority or its organizational equivalent. The generation and maintenance of audit records are also normally the responsibilities of the central oversight authority or its organizational equivalent. The generation and maintenance of registration, de-registration, revocation and compromise lists, revoked key notifications, and accounting documentation **should** be accomplished at the key processing facility(ies), service agent(s), and client nodes (or their organizational equivalents), as required by the KMPS.

4 Key Management Planning for Cryptographic Components

Federal government organizations are required by statutory and administrative rules and guidelines to protect the confidentiality and integrity of sensitive information and processes. If cryptography is used to satisfy this requirement, developers, integrators, and managers need to ensure that each cryptographic implementation satisfies all system security, compatibility, and interoperability requirements that are associated with the system into which it is being integrated.

For any cryptographic device employed by the federal government, there **should** be a specification of the keying material that the device requires, an identification of whether the keying material is internally or externally generated, a specification of keying material input/output interfaces, and a description of interfaces to any required validation process. Development of the specification **should** be initiated before any cryptographic procurement is initiated. Algorithms, key lengths, cryptoperiods, key sources, input/output interfaces (where applicable) and keying material access and handling requirements **should** also be specified. For devices using modules that are validated under FIPS 140, most of these requirements are specified in the security policy posted with the validation information for each module. Note that all cryptographic modules used by federal agencies **shall** be validated in accordance with FIPS 140. These specifications are required by system developers as well as by the managers of systems into which cryptographic components are integrated. They are also required by program managers who are responsible for the security of system implementations.

Program managers who oversee the implementation of cryptography in federal systems are responsible for ensuring that the systems include all mechanisms, interfaces, policies, and procedures that are necessary to generate or otherwise establish, acquire, distribute, replace or update, account for, and protect keying material that is required for system cryptographic operations in accordance with the recommendations presented in Part 1 and the policies and practices identified in this Part 2 document (SP 800-57).

The development of new cryptographic systems, including key management systems, **should** ideally be conducted following the processes described in SP 800-160.[36]

All cryptographic purchasing plans, development activities, and applications integration plans **should** involve key management planning. In the case of planning for the acquisition and use of existing cryptographic devices or software, key management planning **should** begin during the initial discussion stages for cryptographic applications or implementation efforts. The planning **should** be evolutionary in nature, maturing as the cryptographic application matures, and **should** be consistent with NIST key management guidance. Key management plans **should** ensure that the key management products and services that are proposed for the cryptographic device or application are provided with adequate security, and are supportable and operationally suitable in accordance with the FIPS 140 security policy for any associated module.

Processes for purchases of cryptographic products and services **should** include plans and provisions for the acquisition of keying material from trusted sources, secure paths for the transport of keying material, and/or FIPS 140-compliant automated key establishment mechanisms (see SP

[36] SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.*

800-56A and SP 800-56B). Key management requirements **shall** be included in service agreements associated with cryptographically protected services.

For cryptographic development efforts, a key specification and acquisition process **should** begin as soon as the algorithm and, if appropriate, the media and format have been identified. For the application of existing cryptographic products for which no key management plan exists, the process **should** begin as soon as the product is selected for the application. In both cases, the specification and acquisition process **should** be an initial step in the evolution of a key management plan.

For the application of existing cryptographic products for which a key management plan already exists, the existing plan **should** be reviewed in the context of the application's environment, and requirements **should** be amended as necessary. Such a review process **should** begin as soon as the product is selected for the application.

The types of key management products and services that are produced for a specific cryptographic device and/or for suites of devices used by organizations (e.g., algorithms, modes of operation, key sizes) **should** be standardized to the maximum possible extent, and new cryptographic application development efforts **should** comply with NIST key management recommendations. Accordingly, NIST criteria for the security, accuracy, and utility of key management products and services in electronic and physical forms **should** be met (e.g., FIPS 140, SP 800-53, and SP 800-57 Part 1). The methods used in the design, evaluation, programming, generation, production, establishment, quality assurance, and inspection procedures for key management products and services **should** be structured to satisfy such criteria.

Where the criteria for security, accuracy, and utility can be satisfied with any of the organization's existing suite of key management products and services, one of those products and services **should** be used. Where the application of current key management products and services results in reduced security, accuracy, utility, or added cost to a cryptographic application, then an organization may initiate efforts to develop and implement other key management products and services types, variations, and, as necessary, production processes. However, such efforts **should** conform as closely as possible to established key management recommendations.

4.1 Key Management Planning Documents

The document that describes the management of all key management products and services used by a cryptographic product (cryptographic engine, cryptographic device, cryptographic application, or user entity) throughout its lifetime is the key management specification. Key management specifications are generally produced by developers or (where developers have failed to produce adequate capabilities) by integrators.[37] Organizational key management plans (e.g., key management appendices to system security plans) document the capabilities that cryptographic applications require from the organization's key management infrastructure (KMI). The purpose of these organizational key management plans is to ensure that any lifecycle key management services are supportable by and available from the KMI in a secure and timely manner. If a KMP exists for an organization, the key management specification needs to be in conformance with the KMP. The KMPS **should** support both the KMPS and the key management specification.

[37] Note that a significant part of the information required is available in the Security Policy associated with each module validation.

4.2 Key Management Planning Process

When developing a key management specification for a cryptographic product, the unique key management products and services needed from the KMI to support the operation of the cryptographic product need to be defined. The specification of cryptographic mechanisms, including key management mechanisms, **shall** necessarily take into account the organization's resource limitations and procedural environment. For example, an organization that lacks the physical protection facilities, adequate vetting of support personnel, and procedures and resources required for managing controlled unclassified information, might find it difficult to satisfy the policies and procedures required for cryptography that is generally required for the protection of controlled unclassified information. Before either approving or rejecting specifications required for controlled unclassified information, the organization **should** consider the resource and operational implications of the decision. A contrasting example is that of an organization that must exchange information that is assigned a *moderate* or *high* FIPS 199 information security risk level specifying a FIPS 140 Level 1 cryptographic module. Such a decision could adversely affect the organization's ability to be permitted to continue to engage in mission-critical processing and communications partnerships.

The planning process must account for both the availability of critical resources and for assurance requirements implied by the organization's critical mission functions.

4.3 Key Management Planning Information Requirements

The level of key management planning detail required for cryptographic applications can be tailored, depending upon the scope and complexity of the application. Obviously, if an organization's cryptographic support requirements are limited to e-mail security for a small number of employees, extensive planning documentation is neither feasible nor cost-effective (unless such security documentation is justified by a very high level of sensitivity associated with the organization's email). On the other hand, cryptographic security for a collection of networks that support thousands, or tens of thousands of users require the kind of extensive documentation described in Section 3 and Appendix B. Regardless of the size and complexity of a cryptographic application, documentation of some basic key management characteristics and requirements is strongly recommended. Some basic information that needs to be documented for all applications is provided in the following subsections.

4.3.1 Key Management Products and Services Requirements

The key management product and service requirements describe the types, quantities, cryptoperiod (lifetime), algorithms, and additional information that define the cryptographic application's keying material requirements.[38] If additional keys (e.g., certificates or tokens) are required, key management documentation **should** describe a rough order of magnitude for the quantities required. If keys or certificates already issued (or planned to be issued) by the KMI are adequate for the cryptographic application described in the key management specification, then the key management specification **should** so state. Otherwise, any new or additional key, certificate, or token features (e.g., new certificate extensions or formats) **should** be described.

[38] For example, cryptographic applications using public key certificates (i.e., X.509 certificates) **should** describe the class of certificates as identified by the CA, and whether certificates and tokens already issued to subscribers will be used for the cryptographic application, or whether the cryptographic application will require additional certificates and tokens.

The requirement information for the cryptographic application's key management products and services may be included in table format. The following information **should** be included[39]:

- The types of key management products and services (e.g., keys, certificates, tokens for various purposes);
- The quantity of key management products and services required (per device to be keyed);
- The projected quantity of devices to be employed in the application;
- For each key management product and service used by the cryptographic application, the algorithm(s) employed to provide for each key management product and service provided by the cryptographic application (the applicable FIPS or SP);
- The keying material format(s) (reference existing key specifications, if applicable);
- Cryptoperiods to be enforced (may be a general recommendation or a recommendation specific to an application or organization);
- PKI certificate classes (as applicable);
- Tokens or software modules to be used (as applicable);
- Dates when keying material is needed (initial plans and plan revisions);
- The projected duration of the need (for applications or organizations)[40]; and
- The title or identity of the anticipated keying material manager (as applicable).

The description of the key management products and services format generally references an existing key specification. If the format of the keying material is not already specified elsewhere, then the format and medium **should** be specified.

4.3.2 Changes to Key Management Product Requirements and Transition Planning

Cryptanalytic capabilities and processing power available for application to cryptanalysis eventually overtake the protection afforded by cryptographic algorithms. Most often, the cryptanalytic advances require transition from a key size currently in use to a larger key size, but they can also result in the need to move from one algorithm employed in key management (e.g., for key wrapping) to another. Examples include past requirements to transition from DES and SHA-1 to stronger algorithms, and the postulated need to transition from logarithmic and elliptic curve algorithms to algorithms more resistant to Shor's algorithm and quantum computing. Regardless of the basis for transition and whether the transition involves just key size or a new algorithm, it is important to begin planning for transition as soon as possible after becoming aware of the need. Changes to either algorithm or key size most often require changes to code and protocols, not just to configuration settings for code and protocols. Frequently, firmware or hardware changes are required. This always takes longer than expected and is more complicated than expected. The transition period can be measured in decades, and during the period between when a cryptographic attack becomes practical and when the consequent transition is completed,

[39] Note that some of this material may be included by reference (e.g., a distribution of cryptography by the using organization's KMI).

[40] This can affect the strength of the mechanism, affect when the system must be replaced, etc. It should be crosschecked with the projected duration of the need.

all information protected by the vulnerable cryptography is subject to disclosure, alteration, or both.

4.3.3 Key Management Products and Services Ordering

For keys distributed from a CA or other key processing center rather than established at client nodes using automated key establishment techniques, a description of the procedures for ordering keying material within a specified KMI is required. Details **should** be included that are sufficient to permit a determination of the requirements for long-term support by the KMI.

4.3.4 Keying Material Distribution

For keys distributed from a CA or other key processing center rather than established at client nodes using automated key establishment techniques, describe the distribution method for key management products and services within the cryptographic application. The distribution information will normally include how the key management products are protected during distribution (e.g., key wrapping) and how they are distributed (e.g., by courier), the physical form of the product (electronic, PROM, disk, paper, etc.) and how they are identified during the distribution process.

4.3.5 Keying Material Storage

Documentation **should** address keying material storage (e.g., the media used and storage location) and the method for identifying keying material during its storage life (e.g., by key name and date). The storage capacity capabilities for key management products and services **should** be included.

4.3.6 Access Control

Documentation **should** address how access to the cryptographic application will be authorized, controlled, and validated for the request, generation, handling, establishment, storage, and/or use of key management products and services. Any use of passwords, tokens, personal identification numbers (PINs), or biometrics **shall** be included (with their expiration dates, where applicable). For PKI cryptographic applications, access privileges based on roles and the use of tokens **shall** be described.

4.3.7 Accounting

There needs to be a description of the accounting for key management products and services used by the cryptographic application. The use of logs to support the tracking of key management products and services, including the generation/establishment, storage, use and/or destruction of keying material **should** be described. The use of appropriate access privileges to support the control of key management products and services used by the cryptographic application **should** also be described in addition to the directory capabilities used to support PKI cryptographic applications, if applicable. There **should** be an identification of circumstances under which human and automated tracking actions are performed and where two-person control is required, if applicable. Note that some of this material may, under some circumstances, be included by reference (e.g., reference to Department of Defense (DoD) Cryptographic Material System (CMS) documentation where the keying material is distributed by a DoD KMI).

4.3.8 Compromise Management and Recovery

How protected communications and stored information content can be restored in the event of the compromise of keying material needs to be described. The recovery process description **should** include the methods for re-keying. The methods for revoking keys **should** be described in detail, including the methods for rekeying and/or issuing new certificates.

4.3.9 Key Recovery

Key recovery addresses how currently unavailable keying material can be recovered. Keying material that is in active memory or stored in normal operational storage may sometimes be lost or corrupted (e.g., from a system crash or power fluctuation). Some of the keying material is needed to continue operations and cannot easily be replaced. For example, keys may need to be retained to permit retrieval of encrypted information from archives. This requirement may persist as long as the archived information needs to be retained.

An assessment needs to be made of which keying material needs to be preserved for possible recovery at a later time. The decision employing a key recovery capability **should** be made on a case-by-case basis. The factors involved in a decision for or against key recovery **should** be carefully assessed. The trade-offs are concerned with continuity of operations versus the risk of possibly exposing the keying material and the information it protects if control of the keying material is lost. If it is determined that a key needs to be recovered, and the key is still active (e.g., the cryptoperiod of the key has not expired, and the key has not been compromised), then the key may be replaced in order to limit the exposure of the data protected by the lost key (see Section 8.2.3 of SP 800-57 Part 1). Issues associated with key recovery and discussions about whether or not different types of cryptographic material need to be recoverable are provided in Appendix B of Part 1.

A key recovery process description **should** include a discussion of the generation (e.g., whether or not the material was centrally-generated), storage, and access for long-term storage keys. The process of transitioning from the current to future long-term storage keys **should** also be included.

4.3.10 KMI Enhancement (optional)

The use of validated key management modules in products and services provided by an organization's KMI is required for federal agencies and highly encouraged for others. Such use reduces the documentation requirements and facilitates both systems integration and logistics support. It also encourages the feedback of locally specific requirements to the KMI planning process. However, a cryptographic application may identify requirements that are currently not supported by the appropriate KMI. If applicable, it would be useful to identify and address required improvements to the KMI in order to achieve the needed cryptographic application functionality. This will assist in identifying requirements for current and/or planned capability increments for the KMI. Even if a cryptographic application can be fully supported by the current or planned KMI, improvements to the KMI **should** also be identified if they improve the functionality of the cryptographic application or reduce user workload. The identified requirements can be analyzed for potential upgrades to the KMI, based on available cost, schedule, and performance constraints.

Appendix A: KMI Examples

This appendix contains examples of KMIs: a PKI used for the distribution of asymmetric key pairs and two classes of key centers used for the establishment of symmetric keys.

A.1 Public Key Infrastructure (PKI)

One form of a KMI is that of a public-key infrastructure (PKI) (shown in Figure 4). Comparing the PKI components against the KMI components in Figure 1, the PKI's certification authority (CA) is the KMI's key processing facility, and the PKI's registration authority (RA) is the KMIs service agent.

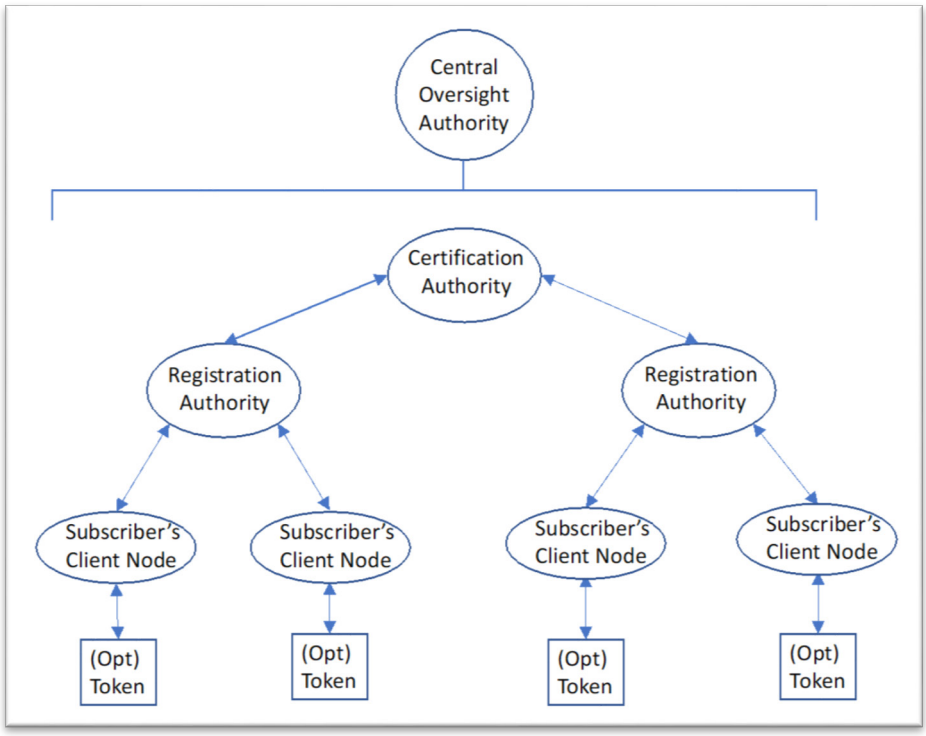

Figure 4: PKI Components

A.1.1 Central Oversight Authority

In a PKI, the central oversight authority may be called a policy management authority or just a policy authority.

A.1.2 Certification Authority (CA)

The key management facility for a PKI is the certification authority (CA), whose responsibility is to create, sign, publish and manage public key certificates. Depending on the CA design, the CA may also generate asymmetric key pairs (e.g., for key establishment). See SP 800-15[41] and *Certificate Policy for the Federal Bridge Certification Authority (FBCA)* for more information about the responsibilities of a CA.

[41] SP 800-15, *MISPC Minimum Interoperability Specification for PKI Components*.

A.1.3 Registration Authority (RA)

A PKI's registration authority (RA) is an entity that enters into an agreement with a CA to collect and verify the identity of prospective subscribers of the CA's services and other information that will be included in the subscriber's certificates. RAs register subscribers, approve certificate issuance, and perform key recovery operations. Not all RAs are authorized to perform all RA functions. An RA designated to perform key recovery operations may be referred to as a key recovery authority (KRA).

A.1.4 Subscriber's Client Node and Token

Subscribers interface with the PKI and with others (called relying parties) using their client nodes. A subscriber is the entity whose name appears as the subject of a certificate. If tokens are used, they are associated with a particular subscriber. Typically, either the client node or the subscriber's token contains the keying material to be used by the subscriber.

A.1.5 PKI Hierarchical Structures and Meshes

A hierarchical PKI, is one in which all of the end entities and relying parties use a single "root CA" as their trust anchor. If the hierarchy has multiple levels, the root CA certifies the public keys of intermediate CAs (also known as subordinate CAs). These CAs then certify end entities' (subscribers') public keys or may, in a large PKI, certify other CAs. In this architecture, certificates are issued in only one direction, and a CA never certifies another CA that is "superior" to itself. Typically, only one superior CA certifies each CA. Certification path building in a hierarchical PKI is a straightforward process that simply requires the relying party to successively retrieve issuer certificates until a certificate that was issued by the trust anchor is located.

A widely used variation on the single-rooted hierarchical PKI is the inclusion of multiple CAs as trust anchors. In this case, certificates for end entities are validated using the same approach as with any hierarchical PKI. The difference is that a certificate will be accepted if it can be verified back to any of the set of trust anchors.

In a typical mesh style PKI (see Section 2.3.6); each end entity trusts the CA that issued its own certificate(s). Thus, there is no “root CA” for the entire PKI. The CAs in this environment have peer relationships; they are neither superior nor subordinate to one another. In a mesh, cross-certification between peer CAs may go in both directions.

A.2 Key Centers

Key Centers are often used in environments using symmetric keys. Two example architectures are that of a key distribution center and a key translation center.

A.2.1 Key Distribution Center (KDC) Architecture

A key distribution center (KDC) generates keying material as needed, either in response to a request or as determined by policy. Figure 5 shows a typical KDC architecture.

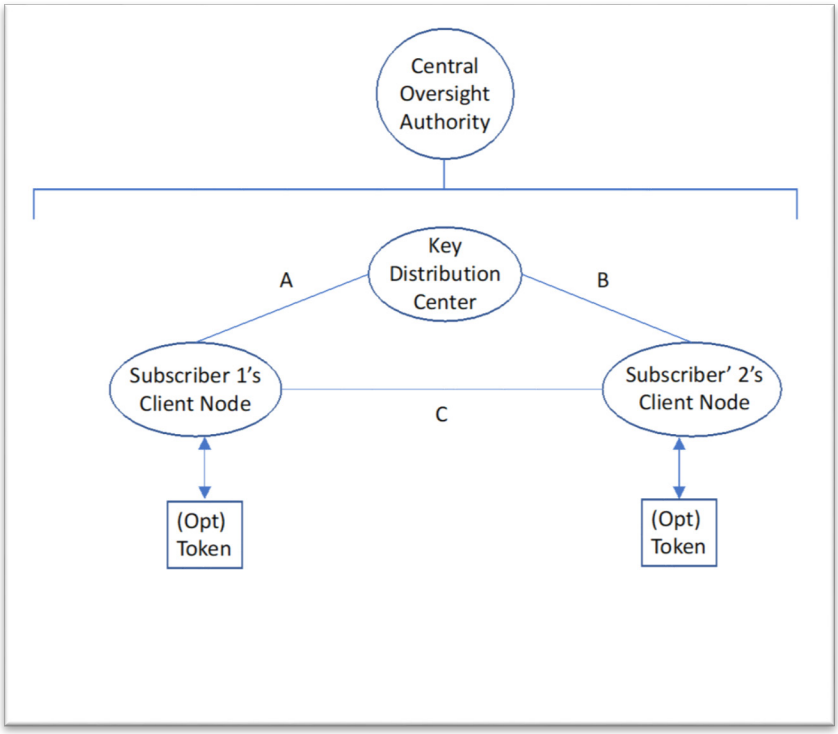

Figure 5: KDC Components

A.2.1.1 Key Distribution Center (KDC)

A KDC generates keys, either upon request or of its own volition, and distributes them to one or more of its subscribers. KDCs mostly generate symmetric keys. Subscribers share a key-wrapping key with the KDC that is used to protect the generated keys during communication. The KDC will use cryptographic techniques to authenticate requesting users and their authorization to request keys. Kerberos is a real-world example of a KDC.

A key generated by a KDC may be sent directly to one or more subscribers (using paths A and B in Figure 5) or multiple keys may be sent to one subscriber (e.g., Subscriber 1) who forwards them to another subscriber (e.g., using path A, followed by path B).

A.2.1.2 Subscriber Client Node and Token

Subscribers may request keys from a KDC (e.g., Subscriber 1 uses path A) only for their own use or may request keys to be shared with other KDC subscribers (Subscriber 2 in the figure). Alternatively, a KDC may voluntarily generate and distribute keys to its subscribers, either to be shared among two or more subscribers or to be used solely by a single subscriber. These keys may be stored by the client node or on the subscriber's token (if used).

A.2.2 Key Translation Center (KTC) Architecture

A KTC is used to translate keys for future communications between KTC subscribers. The architecture is shown in Figure 6 and is similar to the KDC architecture shown in Figure 5, except that a KTC is used instead of a KDC. Subscribers share a key-wrapping key with the KTC that is used to protect the generated keys during communication.

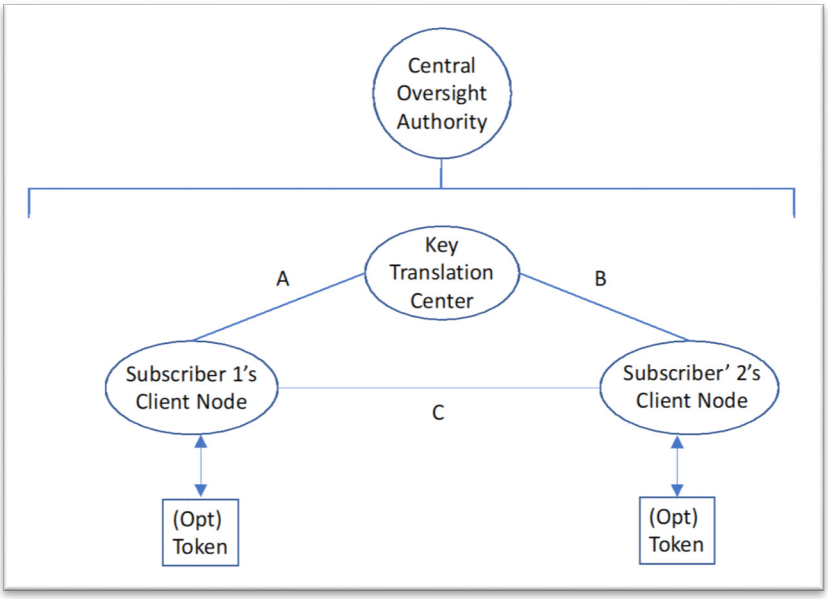

Figure 6: KTC Components

A.2.2.1 Subscriber Client Node and Token

When a KTC subscriber (e.g., Subscriber 1) needs to securely communicate with one or more other KTC subscribers (e.g., Subscriber 2) but does not share a key with them, then Subscriber 1 may generate keying material, wrap it using a key-wrapping key (KWK) shared with the KTC and send the wrapped keying material (using path A) to the KTC for "translation" into a form that can be understood by the other subscriber(s) (e.g., Subscriber 2). Depending on how the architecture is implemented, the translated keys may be returned to Subscriber 1 for forwarding to the other intended subscriber(s) (using path A, followed by path C) or may be sent directly to the other intended parties (using path B).

A.2.2.2 Key Translation Center (KTC)

KTCs receive keying material from their subscribers for "translation" into a form usable by other KTC subscribers. When a request for translation is received from a KTC subscriber (e.g., Subscriber 1 via path A), the KTC unwraps the received keying material using the KWK shared with Subscriber 1, re-wraps the key(s) using the KWK(s) shared with each of the other intended subscribers (e.g., Subscriber 2) and sends them either directly to each subscriber (using path B) or to the requesting subscriber for forwarding to the other intended subscriber(s) (using path A followed by path B).

Appendix B: Key Management Inserts for Security Plan Templates

This appendix identifies a system security plan template and key management material that **should** be included in system security plans. The template information has been extracted from SP 800-18.[42]

Note that the following sample has been provided only as one example; this example is for a PKI. Organizations may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility.

Although the information identified in the key management appendix outline described at item 16 below may be distributed among other template elements rather than in a separate appendix, all of the information described in the key management appendix **shall** be included in the security plan for systems that employ cryptography.

1. Information System Name/Title

- The unique identifier and name given to the system.

2. Information System Categorization

- An identification of the appropriate FIPS 199 categorization.

3. Information System Owner

- The name, title, agency, address, email address, and phone number of the person who owns the system.

4. Authorizing Official

- The name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts

- A list of other critical personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility

- The name, title, address, email address, and phone number of the person who is responsible for the security of the system.

7. Information System Operational Status

- An indication of the operational status of the system. If more than one status is selected, list which each status is assigned to each part of the system.

[42] SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems.*

8. Information System Type

- An indication of whether the system is a major application or a general support system.

9. General System Description/Purpose

- A description of the function or purpose of the system and the information processes.

10. System Environment

- A general description of the technical system, including the primary hardware, software, and communications equipment.
- Key management-specific information that needs to be included in this section, including the identification of any cryptographic mechanisms employed (including key sources) and the location of any keys stored for future use as well as backed-up and archived cryptographic keys.

11. System Interconnections/Information Sharing

- A list of interconnected systems and system identifiers (if appropriate); provide the system, name, organization and system type (e.g., major application or general support system); indicate if there is an ISA/MOU/MOA on file, the date of any agreement to interconnect, the FIPS 199 category, the certification and accreditation status, and the name of the authorizing official.

12. Related Laws/Regulations/Policies

- A list of any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

13. Minimum Security Controls

- A thorough description of how the minimum controls in the applicable Low, Moderate or High baseline are being implemented or planned to be implemented. The controls **should** be described by control family and indicate whether it is a system control, hybrid control, common control, scoping guidance is applied, or a compensating control is being used.
- Key management-specific information, including key backup, archiving and recovery procedures in support of the recovery of encrypted files; controls for the validation of digital signatures and other integrity keying materials (e.g., certification authority and controls for determining completeness/correctness); key management procedures for key establishment (including generation and distribution), storage, and disposal; and applicable cryptographic standards and guidelines for all cryptographic mechanisms employed. This information may be included in a key management appendix.

14. Information System Security Plan Completion Date

- The completion date of the plan.

15. Information System Security Plan Approval Date

- The date that the system security plan was approved and an indication of whether the approval documentation is attached or on file.

16. Key Management Appendix

- **The Identification of the Keying Material Manager**: The keying material manager **should** report directly to the organization's chief executive officer, chief operations executive, or chief information systems officer. The keying material manager is a critical employee who **should** have been determined to have the capabilities and trustworthiness commensurate with responsibility for maintaining the authority and integrity of all formal electronic transactions and the confidentiality of all information that is sufficiently sensitive to warrant cryptographic protection.
- **The Identification of the Management Entity(ies) Responsible for Certification Authority (CA) and Registration Authority (RA) Functions and Interactions:** Where applicable: where public key cryptography is employed, either the keying material manager or his/her immediate superior **should** be designated as the organization's manager responsible for CA and RA functions. This section **shall** include references to any cloud computing or other shared services employed.
- **Key Management Organization:** The identification of job titles, roles, and/or individuals responsible for the following functions:
  a. Key generation or acquisition;
  b. Agreements with partner organizations regarding cross-certification of any PKI keying material;
  c. Key establishment and revocation structure design and management;
  d. Establishment of cryptoperiods;
  e. Establishment of and accounting for keying material;
  f. Protection of secret and private keys and related materials;
  g. Emergency and routine revocation of keying material;
  h. Auditing of keying material and related records;
  i. Destruction of revoked or expired keys;
  j. Key recovery;
  k. Compromise recovery;
  l. Contingency planning;
  m. Disciplinary consequences for the willful or negligent mishandling of keying material; and
  n. Generation, approval, and maintenance of key management practices statements.
- **Key Management Structure:** A description of the key certification, distribution and revocation procedures for encryption, signature, and other cryptographic

processes implemented within the organization. A description of the procedures for modifying the revocation sequence and for establishing cryptoperiods.

- **Key Management Procedures** (when appropriate)

  a. **Key Establishment:** Where applicable, a brief description of the procedures to be followed for key establishment. This section includes references to applicable standards and guidelines. Some procedures may be presented by reference. Note that not all organizations that employ cryptography will necessarily generate keying material.

  b. **Key Acquisition:** An identification of the source(s) of keying material. A description of the ordering procedures and examples of any forms employed in ordering keying material (e.g., by online request or paper request).

  c. **Cross-Certification Agreements** (applicable only to PKIs)**:** A description of the cross-certification procedures and examples of any forms employed in establishing and/or implementing cross-certification agreements.

  d. **Distribution of and Accounting for Keying Material:** A description of the procedures and forms associated with requests for keying material, the acknowledgement and disposition of the requests, the receipting for keying material, creating and maintaining keying material inventories, reporting the destruction of keying material, and reporting the acquisition or loss of keying material under exceptional circumstances.

  e. **Emergency and Routine Revocation of Keying Material:** A description of the rules and procedures for the revocation of keying material under both routine and exceptional circumstances, such as a notice of unauthorized access to operational keying material.

  f. **Protection of Secret and Private Keys and Related Materials:** The methods and procedures employed to protect keying material under various circumstances, such as during the pre-operational, operational, and revoked phase of a key's lifecycle.

  g. **Destruction of Revoked or Expired Keys:** The procedures and guidelines for identifying the circumstances, responsibilities, and methods for the destruction of keying material.

  h. **Auditing of Keying Material and Related Records:** A description of the circumstances, responsibilities, and methods for the auditing of keying material records.

  i. **Key Recovery:** Specification of the circumstances and process for authorizing key recovery and an identification of the guidelines and procedures for key recovery operations.

  j. **Compromise Recovery:** The procedures for recovering from the exposure of sensitive keying material to unauthorized entities.

  j. **Disciplinary Actions**: A specification of the consequences for willful or negligent mishandling of keying material.

k. **Change Procedures:** A specification of the procedures for effecting changes to key management planning documentation.

APPENDIX C: Key Management Specification Checklist for Cryptographic Product Development

The following key management-related information for cryptographic products development may be needed to determine and resolve potential impacts to the key management infrastructure or other keying material acquisition processes in a time frame that meets user requirements. Yes/no responses **should** be provided to the following questions as well as additional information for each "yes" response. To the extent practical, SP 800-160,[43] **should** be followed in the development of cryptographic products.

1. Are unique key management products and services required by the cryptographic product for proper operation?
2. Are there any cryptographic capabilities to be supported by the KMI that are not fully configurable in the cryptographic product?
3. Does the cryptographic module implement a software download capability for importing updated cryptographic functions?
4. Does the cryptographic module use any non-keying material KMI products or services (such as CKL/CRLs, seed key conversion, etc.)?
5. Does the cryptographic module design preclude the use of any **approved** cryptographic algorithm?

[43] SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

APPENDIX D: References

The following publications are provided for reference. The provided publication dates refer to the last available version of the document as of the publication of this revision of SP 800-57 Part 2. When later revisions of these referenced documents are available, those versions should be referenced instead.

CC	Evaluation Criteria for IT Security, International Organization for Standardization, ISO-IEC 15408-1, December 2009. https://www.iso.org/standard/50341.html
CertiPath KR	*CertiPath Key Recovery Policy*, Certipath, December 2013 https://www.certipath.com/downloads/20131216%20CertiPath%20KRP%20v.1.5.pdf
CNSSI 1300	*Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25*, CNSSI No. 1300, Committee on National Security Systems, October 2009. https://www.hsdl.org/?view&did=18451
CP X509 CP	*CertiPath X.509 Certificate Policy*, Certipath, Version 3.26, November 2014. https://www.certipath.com/downloads/CertiPath%20CP-v.3.26_final.pdf
DoD Policy	*X.509 Certificate Policy for the United States Department of Defense*, Department of Defense, Version 10.5, January 2013. https://iase.disa.mil/pki-pke/Documents/unclass-dod_cp_v10-5.pdf
DoD KRP	*Key Recovery Policy for External Certification Authorities*, Department of Defense, Version 1.0, June 2003. https://iase.disa.mil/pki-pke/Documents/unclass-eca_krp_v1-4_jun03_signed.pdf
FBP	*X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.31, Federal Bridge Certification Authority, General Services Administration, June 2017. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA-Certificate-Policy-v2.31-06-29-17.pdf
FedPKIKRP	*Federal Public Key Infrastructure Key Recovery Policy*, Version 1.0, October 6, 2017. https://www.idmanagement.gov/fpki/

FIPS 140	Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, December 2002. https://doi.org/10.6028/NIST.FIPS.140-2
FIPS 199	Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, February 2004. https://doi.org/10.6028/NIST.FIPS.199
FISMA	Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, 17 December 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html
NISTIR 7924	Second Draft NIST Internal Report (NISTIR) 7924, *Reference Security Policy*, National Institute of Standards and Technology, May 2014. https://csrc.nist.gov/publications/detail/nistir/7924/draft
OMB130	OMB Circular A-130, *Managing Information as a Strategic Resource*, 28 July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
PDD63	Presidential Decision Directive 63, *Critical Infrastructure Protection*, May 1998. https://www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865
PL106	Electronic Signatures in Global and National Commerce Act, Public Law 106-229, 30 June 2000. https://www.gpo.gov/fdsys/pkg/PLAW-106publ229
PL 113-274	Cybersecurity Enhancement Act of 2014, Public Law 113-274, December 2014. https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf
PKI	SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, February 2001. https://doi.org/10.6028/NIST.SP.800-32
PKI 01	Housley, R and Polk, T; *Planning for PKI*; Wiley Computer Publishing; New York; 2001.
RFC3647	*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, Internet Engineering Task Force, Network Working Group, Request for Comments 3647, The Internet Society; November 2003.

https://datatracker.ietf.org/doc/rfc3647/

RFC 4107 *Guidelines for Key Management*, Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 4107, June 2005. https://doi.org/10.17487/RFC4107

RFC 4158 *Internet X.509 Public Key Infrastructure: Certification Path Building*, Request for Comments 4158, September 2005.

https://doi.org/10.17487/RFC4158

RFC 4210 *Internet X.509 Public Key Infrastructure Protocol (KMP),* Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 4210, September 2005. https://doi.org/10.17487/RFC4210

RFC 4535 *GSAKMP: Group Secure Association Key Management Protocol*, Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 4535, June 2006. https://doi.org/10.17487/RFC4535

RFC 4758 *Cryptographic Token Key Initialization Protocol (CT-KIP),* Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 4758, November 2006. https://doi.org/10.17487/RFC4758

RFC 4962 *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management*, Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 4962, July 2007. https://doi.org/10.17487/RFC4962

RFC 5083 *Cryptographic Message Syntax (CMS) Authenticated Enveloped-Data Content Type*, Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 5083, November 2007. https://doi.org/10.17487/RFC5083

RFC 5272 *Certificate Management Over CMS (CMC),* Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 5272, June 2008. https://doi.org/10.17487/RFC5272

RFC 5275 *CMS Symmetric Key Management and Distribution*, Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 5275, June 2008. https://doi.org/10.17487/RFC5275

RFC 5652 *Cryptographic Message Syntax (CMS),* Internet Engineering Task Force, Network Working Group, Standards Track, Request for Comments 5652, September 2009. https://doi.org/10.17487/RFC5652

RFC 5990 *Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS),* Internet Engineering Task Force, Standards Track, Request for Comments 5990, September 2010.

https://doi.org/10.17487/RFC5990

RFC 6030 *Portable Symmetric Key Container (PSKC)*, Internet Engineering Task Force, Standards Track, Request for Comments 6030, October 2010. https://doi.org/10.17487/RFC6030

RFC 6031 *Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type*, Internet Engineering Task Force, Standards Track, Request for Comments 6061, December 2010. https://doi.org/10.17487/RFC6031

RFC 6063 *Dynamic Symmetric Key Provisioning Protocol (DSKPP)*, Internet Engineering Task Force, Standards Track, Request for Comments 6063, December 2010. https://doi.org/10.17487/RFC6063

RFC 6160 *Algorithms for Cryptographic Message Syntax (CMS)*, Internet Engineering Task Force, Standards Track, Request for Comments 6160, April 2011. https://doi.org/10.17487/RFC6160

RFC 6402 *Certificate Management Over CMS (CMC) Updates*, Internet Engineering Task Force, Standards Track, Request for Comments 6402, November 2011. https://doi.org/10.17487/RFC6402

RFC 6960 *X.509 Internet Public Key InfrastructureOnline Certificate Status Protocol – OCSP, Updates*, Internet Engineering Task Force, Standards Track, Request for Comments 6960, June 2013. https://doi.org/10.17487/RFC6960

RMF *Risk Management Framework*, National Institute of Standards and Technology, November 30, 2016

https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

SP 800-15 Special Publication 800-15, MISPC Minimum Interoperability Specification for PKI Components, Version 1, January 1998. https://doi.org/10.6028/NIST.SP.800-15

SP800-18 Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, National Institute of Standards and Technology, February 2006. https://doi.org/10.6028/NIST.SP.800-18r1

SP800-23 Special Publication 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, National Institute of Standards and Technology, August 2000.

https://doi.org/10.6028/NIST.SP.800-23

SP800-37 Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, National Institute of Standards and Technology, June 2014.

https://doi.org/10.6028/NIST.SP.800-37r1

SP800-53 Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, April 2013 (updated 1/22/2015).

https://doi.org/10.6028/NIST.SP.800-53r4

SP-800-53A Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls for Federal Information Systems and Organizations: Building Effective Assessment Plans*, National Institute of Standards and Technology, December 2014 (updated 12/18/2014).

https://doi.org/10.6028/NIST.SP.800-53Ar4

SP 800-56A Special Publication 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, National Institute of Standards and Technology, May 2013. https://doi.org/10.6028/NIST.SP.800-56Ar2

(Draft SP 800-56A Revision 3, August 2017, is available at: https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/draft).

SP 800-56B Special Publication 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, National Institute of Standards and Technology, September 2014.

https://doi.org/10.6028/NIST.SP.800-56Br1

SP 800-56C Special Publication 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*, National Institute of Standards and Technology, November 2011.

https://doi.org/10.6028/NIST.SP.800-56C

(Draft SP 800-56C Revision 1, August 2017, is available at: https://csrc.nist.gov/publications/detail/sp/800-56c/rev-1/draft).

SP 800-57 Pt1 Special Publication 800-57 Part 1 Revision 4, *Recommendation for Key Management, Part 1: General*, National Institute of Standards and Technology, January 2016.

https://doi.org/10.6028/NIST.SP.800-57pt1r4

SP 800-57 Pt3 Special Publication 800-57 Part 3 Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, National Institute of Standards and Technology, January 2015.

https://doi.org/10.6028/NIST.SP.800-57pt3r1

SP 800-88 Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014.

https://doi.org/10.6028/NIST.SP.800-88r1

SP 800-108 Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, National Institute of Standards and Technology, October 2009.

https://doi.org/10.6028/NIST.SP.800-108

SP 800-130 Special Publication 800-130, *A Framework for Designing Cryptographic Key Management Systems*, National Institute of Standards and Technology, August 2013.

https://doi.org/10.6028/NIST.SP.800-130

SP 800-132 Special Publication 800-132, *Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*, National Institute of Standards and Technology, December 2010.

https://doi.org/10.6028/NIST.SP.800-132

SP 800-133 Special Publication 133, *Recommendation for Cryptographic Key Generation*, National Institute of Standards and Technology, December 2012.

https://doi.org/10.6028/NIST.SP.800-133

SP 800-135 Special Publication 800-135 Revision 1, *Recommendation for Existing Application-Specific Key Derivation Functions*, National Institute of Standards and Technology, December 2011.
https://doi.org/10.6028/NIST.SP.800-135r1

SP 800-152 Special Publication 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*, National Institute of Standards and Technology, October 2015.

https://doi.org/10.6028/NIST.SP.800-152

SP 800-160 Special Publication 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, November 2016 (updated 3/21/2018).

https://doi.org/10.6028/NIST.SP.800-160v1

SP 800-171 Special Publication 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, National Institute of Standards and Technology, December 2016 (updated 2/20/2018).

https://doi.org/10.6028/NIST.SP.800-171r1

SP 800-175A Special Publication 800-175A, *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*, National Institute of Standards and Technology, August 2016.

https://doi.org/10.6028/NIST.SP.800-175A

Treasury CP *Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy*, Version 2.9, United States Department of the Treasury, March 15, 2017.

http://pki.treas.gov/docs/treasury_x509_certificate_policy.pdf

Treasury KR *Key Recovery Policy For The Department of the Treasury Public Key Infrastructure (PKI)*, Version 1.0, United States Department of the Treasury, August 24, 2009.

http://pki.treas.gov/docs/dot_krp.pdf

X.509 *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, International Telecommunications Union Telecommunication Sector, ITU-T X.509, October 14, 2016.

http://handle.itu.int/11.1002/1000/13031

1647

Appendix E: Revisions

The original version of this document was published in August 2005. Several editorial corrections and clarifications were made, and the following more substantial revisions were made in 2018 (Revision 1):

1. The Authority section has been updated.
2. Consistent with the Cybersecurity Enhancement Act of 2014 (PL 113-274), Section 1 now states that this Recommendation is intended to provide direct cybersecurity support to the private sector as well as the government-focused guidance consistent with OMB Circular A-130 (OMB 130). The revision states explicitly that the recommendations are strictly voluntary for the private sector, and that requirement terms (**should/shall** language) used for some recommendations do not apply outside the federal government.
3. The Glossary section was updated to improve consistency with recent publications. The terms *accountability, certificate revocation list, client node, communicating group, compliance audit, compromised key list, cryptographic keying relationship, cryptographic key management system, de-registration (of a key), emergency key revocation, encrypted keying material, internet key exchange, Kerberos, key agreement, key-center environment, key certification hierarchy, key derivation, key distribution center, key generation, keying material, key recovery agent, key wrapping key, manual key distribution, mesh, message authentication, multiple-center group, peer, rekey, revocation, revoked key notification, service agent, suspension, transport layer security, token, trust anchor, and user* were added. The *association, asymmetric key algorithm, cryptographic key component, data key, data encrypting key, data origin authentication, dual control, encrypted key, integrity detection, integrity restoration, key de-registration, key registration, label, random number generator, secret key, security services, and subject certification authority* terms were deleted. The definitions for *authentication, authentication code, certification practice statement, confidentiality, digital signature, encrypted keying material, key processing facility, key transport, key update, key wrapping, non-repudiation, password, private key, public key,* and *X.509 certificate* were updated.
4. The acronyms section was revised to add *CKMS, IKE, IPsec, Part 1, Part 2, Part 3, RKN, S/MIME,* and *TLS*; and delete *PRNG* and *RNG*.
5. Section 2 was updated to introduce a more comprehensive set of key management concepts that must be addressed in key management policies, practice statements and planning documents by any organization that uses cryptography to protect its information. The revised section reflects guidance provided by SP 800-130 and SP 800-152, and broadens the applicability of its recommendations to cover both decentralized and centralized key management structures. The example centralized infrastructure design was replaced with explanatory material that reflects SP 800-130 and SP 800-152 and applies to both centralized and decentralized key management structures.

6. In section 3.1.2.1.2, the requirement that the keying material manager also be the certification authority was deleted.
7. The original Section 4 (*Information Technology System Security Plans*), which provided documentation requirements for General Support Systems and Major Applications, was deleted as out of date.
8. The original Section 5, *Key Management Planning for Cryptographic Components*, was updated as Section 4.
9. The original Appendix A, *Notional Key Management Infrastructure*, was removed as outdated and bound strictly to hierarchical structures. It was replaced with a *KMI Examples* Appendix A that describes both PKI and Center environments.
10. The original Appendix B was deleted. It is not necessary to repeat material from the IETF RFC 3647 standard.
11. The original Appendix C, *Evaluator Checklist*, was removed due to SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*, and SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*, now being available to provide the guidance covered in that appendix. Further, as stated in SP 800-53A, security control assessments and privacy control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, such assessments are the principal vehicle used to verify that implemented security controls and privacy controls are meeting their stated goals and objectives.
12. The original Appendix D became Appendix C, and the original Appendix E became Appendix D.