

NIST Special Publication 800-152

A Profile for U.S. Federal Cryptographic Key Management Systems

Elaine Barker
Miles Smid
Dennis Branstad

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-152>

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

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

NIST Special Publication 800-152

A Profile for U. S. Federal Cryptographic Key Management Systems

Elaine Barker
*Computer Security Division
Information Technology Laboratory*

Miles Smid
*G2, Inc.
Annapolis Junction, MD*

Dennis Branstad
*NIST Consultant
Austin, TX*

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-152>

October 2015



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further its statutory responsibility under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *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 800-152
Natl. Inst. Stand. Technol. Spec. Publ. 800-152, 146 pages (October 2015)
CODEN: NSPUE2

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-152>

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

Comments on this publication may be submitted to:

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

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

This Profile for U. S. Federal Cryptographic Key Management Systems (FCKMSs) contains requirements for their design, implementation, procurement, installation, configuration, management, operation, and use by U. S. Federal organizations. The Profile is based on NIST Special Publication (SP) 800-130, *A Framework for Designing Cryptographic Key Management Systems (CKMS)*.

Keywords

access control; confidentiality; cryptographic key management system; disaster recovery; federal cryptographic key management system; integrity; metadata; security assessment; security functions; security policies; source authentication.

Acknowledgements

The National Institute of Standards and Technology (NIST) acknowledges and greatly appreciates contributions by all those who participated in the creation, review, and publication of this document. NIST also thanks the many public and private sector contributors whose constructive comments significantly improved its quality and usefulness. Many useful suggestions on Cryptographic Key Management that were made during the workshops held at NIST in 2009, 2010, 2012, and 2014 have been incorporated into this document.

Executive Summary

The National Institute of Standards and Technology (NIST) Cryptographic Key Management project covers major aspects of managing the cryptographic keys that protect sensitive, unclassified federal information. Associated with each key is specific information (e.g., the identifier associated with its owner, its length, and acceptable uses) called metadata. The computers, software, modules, communications, and roles assumed by one or more authorized individuals when managing and using cryptographic key management services are collectively called a Cryptographic Key Management System (CKMS).

This Profile for U. S. Federal Cryptographic Key Management Systems (FCKMSs) has been prepared to assist CKMS designers and implementers in selecting the features to be provided in their “products,” and to assist federal organizations and their contractors when procuring, installing, configuring, operating, and using FCKMSs. Other organizations may use this Profile as desired.

An FCKMS can be owned and operated by a federal organization or by a private contractor that provides key management services for federal organizations or other contractors performing federal information-processing services.

This Profile can also be used by agencies and organizations to understand their FCKMSs, and to adopt, adapt and migrate their FCKMSs to comply with the Profile requirements over time. NIST does not expect that these requirements would be implemented immediately, but that agencies would use these requirements when creating or procuring FCKMSs or FCKMS services for their Enterprise Architectures.

This Profile is based on [NIST Special Publication 800-130](#), *A Framework for Designing Cryptographic Key Management Systems*. The Framework specifies topics that should be considered by a CKMS designer when selecting the capabilities that a CKMS will have and the cryptographic key management services it will support. This Profile replicates all of the Framework requirements that must be satisfied in a CKMS and its design documentation, and includes additional information about installing, configuring, operating and maintaining an FCKMS.

The Framework and this Profile could be used by other organizations that have security requirements similar to those specified in these documents or could be used as a model for the development of other profiles.

Table of Contents

1	Introduction.....	1
1.1	Profile Terminology	2
1.2	Scope of this Profile	3
1.3	Audience.....	4
1.4	Organization.....	4
2	Profile Basics.....	6
2.1	Profile Topics and Requirements, Augmentations, and Features	6
2.2	Rationale for Cryptographic Key Management	7
2.3	Keys, Metadata, Trusted Associations, and Bindings	8
2.4	FCKMS Functions.....	9
2.5	CKMS Design	9
2.6	CKMS Profile	10
2.7	FCKMS Profile	10
2.8	Differences between the Framework and This Profile.....	10
2.9	Example of a Distributed CKMS Supporting a Secure E-Mail Application	10
2.10	Modules, Devices, and Components	11
3	Federal CKMS Goals	13
3.1	Providing Key Management to Networks, Applications, and Users.....	13
3.2	Maximize the Use of COTS Products in an FCKMS	13
3.3	Conformance to Standards	14
3.4	Ease-of-use.....	14
3.4.1	Accommodate User Ability and Preferences	15
3.4.2	Design Principles of the User Interface	15
3.5	Performance and Scalability	16
3.6	Intellectual Property Rights	17
4	Security Policies.....	18
4.1	Information Management Policy.....	18
4.2	Information Security Policy.....	19
4.3	CKMS and FCKMS Security Policies.....	19
4.4	FCKMS Module Security Policy	23
4.5	Cryptographic Module Security Policy	24
4.6	Other Related Security Policies	25

4.7	Interrelationships among Policies	25
4.8	Personal Accountability.....	26
4.9	Anonymity, Unlinkability, and Unobservability.....	27
4.9.1	Anonymity.....	28
4.9.2	Unlinkability	28
4.9.3	Unobservability	29
4.10	Laws, Rules, and Regulations.....	29
4.11	Security Domains.....	29
4.11.1	Conditions for Data Exchange	30
4.11.2	Assurance of Protection.....	30
4.11.3	Equivalence and Compatibility of FCKMS Security Policies	31
4.11.4	Third-Party Sharing.....	32
4.11.5	Multi-level Security Domains.....	32
4.11.6	Upgrading and Downgrading	33
4.11.7	Changing FCKMS Security Policies.....	34
5	Roles and Responsibilities	35
6	Cryptographic Algorithms, Keys, and Metadata.....	37
6.1	Cryptographic Algorithms and Keys.....	37
6.1.1	Key Types, Lengths and Strengths.....	37
6.1.2	Key Protections	38
6.1.3	Key Assurance	38
6.2	Key Metadata.....	39
6.2.1	Metadata Elements.....	39
6.2.2	Required Key and Metadata Information	43
6.3	Key Lifecycle States and Transitions	44
6.4	Key and Metadata Management Functions.....	45
6.4.1	Generate a Key	46
6.4.2	Register an Owner.....	47
6.4.3	Activate a Key	47
6.4.4	Deactivate a Key	48
6.4.5	Revoke a Key	48
6.4.6	Suspend and Re-Activate a Key.....	49
6.4.7	Renew a Public Key Certificate	49

6.4.8	Key Derivation or Key Update	51
6.4.9	Destroy a Key and Metadata	51
6.4.10	Associate a Key with its Metadata	52
6.4.11	Modify Metadata	52
6.4.12	Delete Metadata.....	53
6.4.13	List Key Metadata	53
6.4.14	Store Operational Key and Metadata Outside a Cryptographic Module.....	54
6.4.15	Backup of a Key and its Metadata	54
6.4.16	Archive Key and/or Metadata.....	54
6.4.17	Recover a Key and/or Metadata	55
6.4.18	Establish a Key	56
6.4.19	Enter a Key and Associated Metadata into a Cryptographic Module	56
6.4.20	Output a Key and Associated Metadata from a Cryptographic Module.....	57
6.4.21	Validate Public-Key Domain Parameters	58
6.4.22	Validate a Public Key	58
6.4.23	Validate a Public Key Certification Path	58
6.4.24	Validate a Symmetric Key	59
6.4.25	Validate Possession of a Symmetric Key.....	59
6.4.26	Validate a Private Key (or Key Pair).....	59
6.4.27	Validate the Possession of a Private Key	59
6.4.28	Perform a Cryptographic Function using the Key.....	60
6.4.29	Manage the Trust Anchor Store	60
6.5	Cryptographic Key and/or Metadata Security: In Storage	61
6.6	Cryptographic Key and Metadata Security: During Key Establishment.....	62
6.6.1	Key Transport.....	62
6.6.2	Key Agreement.....	63
6.6.3	Key Confirmation	63
6.6.4	Key-Establishment Protocols.....	64
6.7	Restricting Access to Key and Metadata Management Functions	64
6.7.1	The Access Control System (ACS).....	64

6.7.2 Restricting Cryptographic Module Entry and Output of Plaintext Keys	65
6.7.3 Controlling Human Input	65
6.7.4 Multiparty Control	66
6.7.5 Key Splitting	66
6.8 Compromise Recovery	67
6.8.1 Key Compromise	67
6.8.2 Metadata Compromise	69
6.8.3 Key and Metadata Revocation	70
6.8.4 Cryptographic Module Compromise	70
6.8.5 Computer System Compromise Recovery	71
6.8.6 Network Security Controls and Compromise Recovery	72
6.8.7 Personnel Security Compromise Recovery	73
6.8.8 Physical Security Compromise Recovery	74
7 Interoperability and Transitioning	76
8 Security Controls	81
8.1 Physical Security Controls	81
8.2 Operating System and Device Security Controls	82
8.2.1 Operating System Security	82
8.2.2 Individual FCKMS Device Security	85
8.2.3 Malware Protection	85
8.2.4 Auditing and Remote Monitoring	87
8.3 Network Security Control Mechanisms	89
8.4 Cryptographic Module Controls	91
8.5 Federal CKMS Security-Control Selection and Assessment Process	91
9 Testing and System Assurances	94
9.1 CKMS and FCKMS Testing	94
9.2 Third-Party Testing	94
9.3 Interoperability Testing	95
9.4 Self-Testing	96
9.5 Scalability Testing	96
9.6 Functional and Security Testing	96
9.7 Environmental Testing	98

9.8	Ease-of-Use Testing	98
9.9	Development, Delivery, and Maintenance Assurances	99
9.9.1	Configuration Management	99
9.9.2	Secure Delivery	100
9.9.3	Development and Maintenance Environmental Security	100
9.9.4	Flaw Remediation Capabilities	101
10	Disaster Recovery	103
10.1	Facility Damage	103
10.2	Utility Service Outage	106
10.3	Communication and Computation Outage	106
10.4	FCKMS Hardware Failure	107
10.5	System Software Failure	108
10.6	Cryptographic Module Failure	109
10.7	Corruption and Loss of Keys and Metadata	110
11	Security Assessment	112
11.1	Full Security Assessment	112
11.1.1	Review of Third-Party Testing and Verification of Test Results	113
11.1.2	Architectural Review of System Design	114
11.1.3	Functional and Security Testing	115
11.1.4	Penetration Testing	115
11.2	Periodic Security Review	116
11.3	Incremental Security Assessment	116
11.4	Security Maintenance	117
12	Technological Challenges	119
Appendix A: References		121
Appendix B: Glossary		125

List of Figures

Figure 1:	FCKMS and its FCKMS Modules	11
Figure 2:	CKMS Security Policy Configurations	20
Figure 3:	An FCKMS Network	24