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

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

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

List of Figures