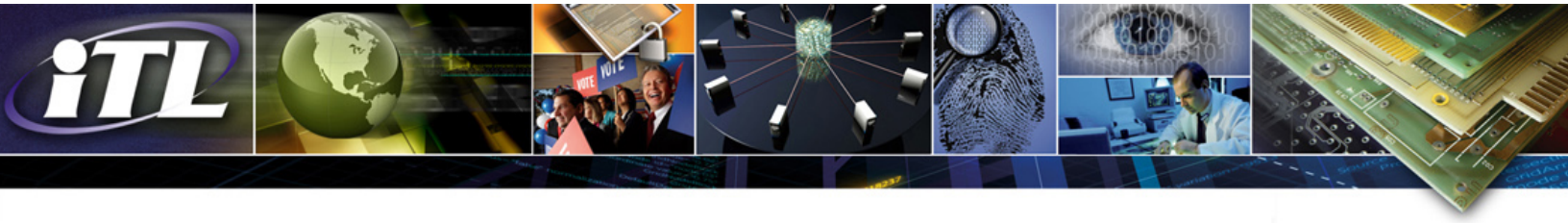


ITL BULLETIN FOR JANUARY 2014

A PROFILE OF THE KEY MANAGEMENT FRAMEWORK

FOR THE FEDERAL GOVERNMENT

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

The Computer Security Division within the Information Technology Laboratory has recently provided a draft of NIST Special Publication (SP) 800-152, *A Profile for U. S. Federal Cryptographic Key Management Systems*, for public comment. The draft and instructions for providing comments are available at this website.

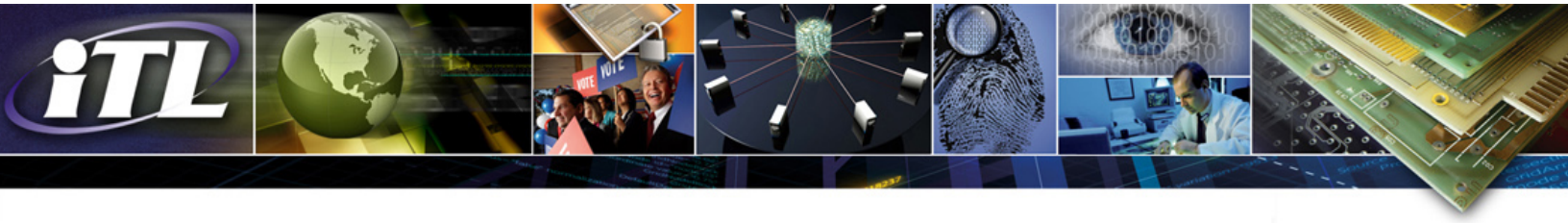
NIST SP 800-152 is based on NIST SP 800-130, *A Framework for Designing Cryptographic Key Management Systems (CKMS)*, which is referenced in this article as the "Framework." SP 800-130 describes the topics to be considered and the documentation requirements to be addressed when designing a CKMS.

A CKMS is responsible for managing the cryptographic keys to be employed for protecting stored and transmitted sensitive information by its users. Typically, each user has a device to perform the computational actions required to cryptographically protect the information. This device could be, for example, a personal computer, a tablet, or a smart phone. In order to interact with other users of the CKMS, each device needs to include a CKMS module that is responsible for interacting with other CKMS modules in the CKMS to perform the general CKMS functionality needed for the device, and a cryptographic module to perform the actual cryptographic operations.

A CKMS could be set up so that its CKMS modules have the same or similar capabilities. An example of this model might be an email application that cryptographically protects the emails sent between CKMS users.

A CKMS could also be set up so that one CKMS module has a "master" relationship with the other CKMS modules in the CKMS. In this case, an example might be a "master" CKMS module that is used by a Key Distribution Center that provides all keys to other CKMS modules in the CKMS.

A CKMS designer determines the type of CKMS to be developed and the capabilities to be incorporated into the specific design. The Framework document specifies CKMS topics that need to be considered during the design and requires that the CKMS designer document the capabilities to be incorporated into the design.



However, the Framework does not address the specific requirements for a CKMS user organization, such as a federal agency; a profile of the Framework is required for this purpose. SP 800-152 is a profile of the Framework that is intended for CKMSs used by the federal government for protecting sensitive, unclassified information, and is referenced herein as the "Profile." Other public and private sectors, such as the healthcare and financial sectors, may use this Profile for their own CKMSs or may develop a profile document of their own, perhaps using SP 800-152 as a model.

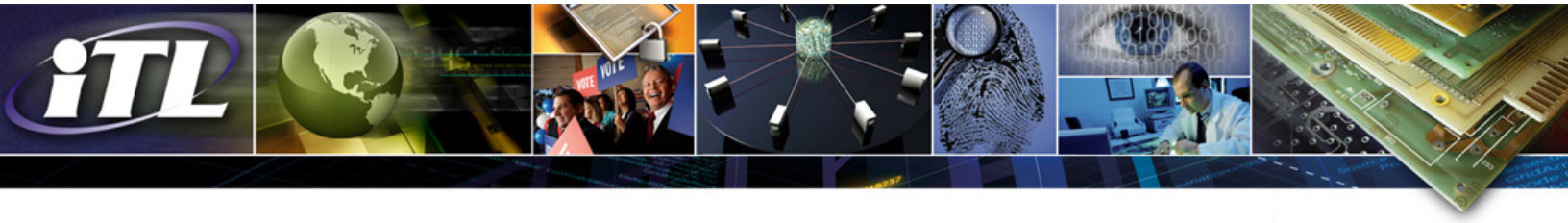
SP 800-152 provides a foundation for designing and implementing federal CKMSs. While the Framework specifies requirements for documenting the design of any CKMS, SP 800-152 provides specific details to be incorporated in the design, such as the use of NIST-approved cryptographic algorithms and Federal Information Processing Standard (FIPS) 140-validated cryptographic modules. However, SP 800-152 goes beyond the Framework by specifying requirements for testing, procuring, installing, managing, operating, maintaining, and using federal CKMSs, including interoperability considerations.

The Profile specifies requirements for a "base" Federal CKMS (FCKMS) with the minimum requirements for all FCKMSs that could be further augmented to meet the needs of federal organizations and their contractors. The Profile recommends augmentations to be considered, as well as suggesting features that may be useful, now or in the future. It is anticipated that some federal organizations may develop a more customized profile document to meet their specific needs, using SP 800-152 as a base.

SP 800-152 is intended to address key management for all the current environments in use today, including key management in the cloud and mobile applications. While SP 800-152 cannot address all issues relating to these environments, it needs to be flexible enough to serve as a basis for developing further guidance for a variety of such environments. Comments are requested during the public-comment period about how well the Profile document serves as a basis for providing more detailed guidance for key management in these environments.

The Profile document also addresses the requirements and guidance in several security documents developed by NIST in the last few years, including FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The security categories in FIPS 199 are based on the potential impact on an organization if certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS 200 uses the security categories in FIPS 199 to specify and define three information system impact levels: low, moderate, and high.

SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides baseline security controls for each FIPS 200 impact level. However, no current guidance exists on the minimum amount of security protection required for each impact level when cryptographic mechanisms are used. The draft of SP 800-152 proposes a mapping between each impact level and a minimum security strength to be provided using NIST-approved algorithms and key lengths, as well as a minimum cryptographic module security level for each impact level. Comments are requested during the public-comment period about the proposed mappings. Once the mappings are solidified, SP 800-53 and any related documents will be modified to reflect these mappings.



An open workshop is planned at NIST for March 4-5, 2014, to discuss the document. Information on the workshop is available at this website.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov