Cryptographic Key Management Workshop

March 4-5, 2014

Session 1: Introduction
(SP 800-152, Sections 1-3)

Dennis K. Branstad, NIST

NIST IT Security Responsibility

- Develop security guidelines, standards, and **requirements for unclassified U.S. Federal** Information Systems.

Cryptographic Key Management Project

- Goal: Develop **Security Requirements, Recommendations, and Suggestions** for Automated Federal Cryptographic Key Management Systems (FCKMSs).
- Task 1: Develop a **Framework** for Designing Cryptographic Key Management Systems (CKMSs).
- Task 2: Develop a **Profile** for U.S. Federal Cryptographic Key Management Systems (FCKMSs).

Presentation Terminology

- **Framework:** Generally means a description of a topic's building blocks and how they **fit together** in various designs; NIST SP 800-130 is a Framework for Designing a CKMS.
- **Profile:** Generally provides a high-level view of **the Requirements for a topic,** including specifications of standards for **a Sector of Users**.
- **Sector**: A **category (e.g., Federal, Financial, Health) of Users** of the products.

Presentation Caveats

- FCKMS Profile is presently a **draft document.**
- My presentation often **summarizes** Profile specifications and doesn't duplicate details.
- Our primary workshop goal is to obtain your suggestions for **improving the current draft document.**
- Interested parties should study the current draft and then later **obtain and use the final Profile.**
- The final Profile **will be reviewed** by potential Federal users and revised before publication.

Framework Requirements: The Foundation of the Profile

- Explanation: The Framework **specifies CKMS design and documentation requirements.**
- **CKMS design documents** can be reviewed before procuring a CKMS to be configured and used as an FCKMS.
- Framework requirements are the **foundation of** many of the **Profile's** requirements.
- One CKMS Framework is the basis for all **Profiles.**
- One Profile for each **Sector of users (e.g., the Federal Sector).**

NIST SP 800-130: A Framework for CKMS Design

- Specifies the **Topics** that a Designer must consider while **designing CKMS products**.
- Specifies **Requirements** for CKMS Designers for **selecting and documenting** the capabilities of automated key management products.
- Specifies **tests** that the Designer and potential customers can use when **evaluating and procuring** CKMSs.

FCKMS Profile Terminology

- CKMS: A Cryptographic Key Management System **designed and implemented for one or more Sectors** that satisfies the Framework requirements.
- Configurable CKMS: A **CKMS that can be configured to meet** the needs of a **service-providing organizations**.
- FCKMS is a **CKMS** that has been designed, implemented, and configured for the **U. S. Federal Sector.**
- **FCKMS** must satisfy all CKMS Framework requirements and all FCKMS Profile requirements.

Federal Profile Audience

- **CKMS designers** and implementers;
- **Federal CKMS** procurers, installers, configuration personnel, administrators, managers, operators, and users;
- **Federal employees** and Federal contractors;
- Members of the public sector who are authorized to use the services of a Federal CKMS when **interacting with Federal organizations** and their contractors.

NIST SP 800-152: A Profile for U. S. FCKMSs

- Requires the **procurement and use** of CKMS products that meet all **Framework and Federal Profile** requirements.
- FCKMS **service-providing** organizations procure, install, configure and operate an FCKMS for Federal **service-using** organizations.

Profile Assistance to Users

- **Assists FCKMS service-using organizations** in selecting or creating appropriate policies for managing their sensitive and valuable information and the cryptographic keys that are used to protect their data.
- **Assist users** within FCKMS service-using organizations to know what key management services **are available** and how they can be initiated and used.

CKMS VS FCKMS

- A CKMS design is created and documented by a **CKMS designer,** and a CKMS is built by implementers of the design.
- An **FCKMS is a CKMS** that is procured, installed, configured, managed, and operated by an **FCKMS service provider** (e.g., agency, contractor).
- **FCKMS service-users** obtain and use the key management services provided by one or more FCKMS service-providers that have been configured to satisfy their special needs.

FCKMS Scope

- **An FCKMS includes** all:
  - Federal computers, devices, modules, software, facilities, management personnel, testers, and maintenance personnel;
  - Users who are **authorized to** create, process, protect, manage, and use keys that protect Federal information; and
  - **Cryptographic keys and** certain information about the keys and their acceptable usage, called **metadata**.

FCKMS Objectives

- **Provide Key Management Services** for one or more U.S. Federal Organizations (e.g., Agencies, Contractors), Applications, and Users.
- **Protect Cryptographic Keys and their associated Metadata** at a level commensurate with the sensitivity level, value, and perceived risks to the information being cryptographically protected.

FCKMS Objectives 2

- Optimize the usage of FCKMS **Standards and COTS products,**
- Optimize the **Scalability and Performance of FCKMS Products and Services**, and
- Optimize **“Easy-to-use” Interfaces** that:
  - **Accommodate** user **ability and preferences,**
  - **Accommodate** user support of organizational **information management and security policies,** and
  - **Support** a user in **doing the right things** and not doing the wrong things.

Federal Profile Structure

- The Profile specifies **Requirements (PRs)**, **recommended Augmentations (PAs)**, and **suggested Features (PFs)** for FCKMSs used to protect unclassified Federal information.
- Requirements are **mandatory** for all FCKMSs.
- Recommended Augmentations and suggested Features are **optional,** but should be implemented and used, based on the special needs of the FCKMS service-users.

Profile (NIST SP 152) Uses

- **Assist CKMS designers and implementers** in selecting and supporting appropriate security algorithms, cryptographic key types, key metadata, and protocols for protecting sensitive U.S. Federal information; and
- **Assist FCKMS service-providers** in comparing, selecting, testing, procuring, installing, configuring, managing, operating, and maintaining their FCKMS.

FCKMS Scope

- All **hardware and software** that generates, protects, and uses cryptographic keys and their metadata,
- The **roles** (e.g., managers, operators, auditors, and users) performed by individuals authorized to manage, protect, and use an FCKMS, and
- The **physical facilities and utility services** needed to physically protect and support operation of an FCKMS.

FCKMS Requirements, Augmentations and Features

- The **Federal Profile specifies**: Requirements (PRs), recommended Augmentations (PAs), and suggested Features (PFs), collectively called **RAFs**, for Federal CKMSs.
- **Allows** FCKMS designers, implementers, and service providers **flexibility** in accommodating present and future needs of Federal organizations with diverse security needs.

Keys, Metadata, Trusted Associations, and Bindings

- **Keys**: Primary parameters of cryptographic **algorithms.**
- **Key Metadata**: Auxiliary parameters of a key used to **control** the key management system.
- **Trusted Association**: Cryptographic or physically protected connection between a **key and its metadata**.
- **Binding**: A **cryptographic-based association** between a key and its metadata.

Components and Modules

- **Components**: Electronic and software building blocks of Cryptographic Modules, FCKMS Modules, and User Computers.
- **Cryptographic Module**: An electronic or software entity that performs cryptographic functions and conforms to FIPS 140-2.
- **FCKMS Module**: An electronic or software entity that is part of an FCKMS and performs key management functions and services; uses a cryptographic module.

Steps from a CKMS Design to an Operational FCKMS

- CKMS **designer identifies a potential target market** for CKMS products;
- CKMS designer **creates a target CKMS security policy** for use in selecting product capabilities;
- CKMS **designer designs** a CKMS product **and documents** its capabilities per the Framework;
- CKMS **implementer/vendor implements** the CKMS design and **performs tests** to demonstrate the product's capabilities to users;

Steps from a CKMS Design to an Operational FCKMS 2

- An **FCKMS service-using organization** selects or establishes information management and security policies that it desires to support.
- The FCKMS using-organization **selects** or creates an **FCKMS service-providing organization** to use.
- The FCKMS service-providing organization **reviews** CKMS designs, third-party test results, and **procurement test results** of CKMS candidates.

Steps from a CKMS Design to an Operational FCKMS 3

- FCKMS **service-using organizations specify policies** for using and protecting keys & metadata.
- **FCKMS is procured**, tested, installed, configured, staffed, operated, and maintained **by the service-provider** for its service-using organizations and all their authorized employees/users.

Profile Requirement Example

- **PR: 1.1** A Federal CKMS **shall** satisfy all Framework requirements (**FR's**) and Profile requirements (**PR**s).
  - Explanation: Profile Requirements must be satisfied in **all Federal CKMSs** (i.e., FCKMSs) and are denoted by the word "**shall**."
  - NOTE: Profile Requirements will be discussed throughout the Workshop by presenters and participants.

Profile Requirements Table (Example with 4 PR entries)

PR: 2.1		A Federal CKMS **shal**l support **NIST-approved** cryptographic algorithms, schemes and modes of operation in accordance with [SP 800-131A].
PR: 2.2		In a Federal CKMS, information rated at a **Low impact level shall** be protected with cryptographic algorithms and keys that provide at least **112 bits of security** strength.
PR: 2.3		In a Federal CKMS, information rated at a **Moderate impact level shall** be protected with cryptographic algorithms and keys that provide at least **128 bits of security** strength.
PR: 2.4		In a Federal CKMS, information rated at a **High impact level shall** be protected with cryptographic algorithms and keys that provide at least **192 bits** of security strength.

Profile Augmentation Example

- **PA: 1.1** A Federal CKMS **should** support Profile augmentations (**PA**s) that are specified by one or more of its FCKMS-using organizations.
  - Explanation: Profile Augmentations are **optional recommendations** for FCKMSs and are denoted by the word "**should.**"

Profile Augmentation Table (Example with 1 PA entry)

PA: 3.1		A Federal CKMS **should** support user interfaces that: a) Require **minimal user interactions** with the FCKMS, b) Are commensurate with the range of **experience and capability** of its expected users; c) Support a user when providing an identifier and **identity verification,** d) Support a **user initiating and controlling** the generation and protection of cryptographic keys and associated metadata, and e) Provide one or more **security service-control interfaces.**

Profile Feature Example

- **PF: 1.1** A Federal CKMS **could** support Profile features (**PF**s) that are specified by one or more of its FCKMS-using organizations.
  - Explanation: Profile features are **optional suggestions** for Federal CKMSs and are denoted by the word "**could**."

Profile Feature Table (Example with 1 PF entry)

PF 3.2		A Federal CKMS **could** provide fully **automatic services** to a user or an application, based on **organizational policy.**

Workshop Participant Discussion

- Questions?
- Suggestions?