Session 3: The Security Architecture

March 4, 2014
Miles E. Smid
The process of planning, designing, and constructing a secure FCKMS.

The protection of cryptographic keys and metadata at creation, at rest, during distribution, when in use, and when destroyed.

Will cover mostly Profile Requirements (PRs).
*Key and Metadata Protection (Section 6)*

- Unauthorized Disclosure and Modification
  - Encryption/decryption
  - Digital signatures and cryptographic authentication codes
  - Physical Security

- Unauthorized Access and Use (Access Control)
  - Identification/Authentication Systems (source, receiver and use)
  - Physical Security
Key Types, Lengths and Strengths

(Section 6.1.1)

• **PR:6.1** A Federal CKMS **shall** support all the key types and lengths specified in the CKMS design.
**Key Protections**  
*(Section 6.1.2)*

- **PR:6.2** A Federal CKMS *shall* physically or cryptographically protect all symmetric and private keys from unauthorized disclosure, use, and modification.

- **PR:6.3** A Federal CKMS *shall* support the protection of keys at a level that is commensurate with the impact level of the data to be protected by the keys.

- **PA:6.1** A Federal CKMS *should* cryptographically protect all keys against unauthorized disclosure and modification when outside of a cryptographic module.
**Key Assurance**
*(Section 6.1.3)*

- **PR:6.4** A Federal CKMS **shall** verify the integrity of all keys when received or before initial use.

- **PR:6.5** A Federal CKMS **shall** obtain the following assurances (as appropriate) before the initial operational use of a key: a) Domain parameter validity, b) Public-key validity, c) Private-key possession, or d) Secret key possession.

- **PA:6.2** A Federal CMS **should** support assuring a receiver of a transported key that it came from an authenticated and authorized source.
• **PR:6.8** and **PR:6.9** are similar to the protection requirements for keys.

• **PR:6.10** A Federal CKMS **shall** verify the integrity of all metadata when received or before the initial use of its key.

• **PR:6.11** A Federal CKMS **shall** maintain the association between a key and its metadata.

• **PA:6.5** A Federal CKMS **should** provide a cryptographic binding between a key and its metadata elements.

• **PA:6.6** A Federal CKMS **should** support a source authentication of the metadata elements for all cryptographic keys.
A F/CKMS is implemented by means of key and metadata management functions (e.g., generate key, register owner, associate key with metadata, encrypt/decrypt key, store key, recover key, and revoke key).

Twenty-eight examples are given.

**PR:6.14** A Federal CKMS **shall** support all key and metadata management functions that are specified in its CKMS design.

**PR:6.15** A Federal CKMS **shall** support the verification of the integrity of the request.
**Interoperability Requirements**

*Section 6.4 and Section 6.6.4*

• Profile does not automatically require interoperability.

• When interoperability is deemed to be required, then the Profile does establish requirements.

• E.g., **PR:6.42** When secure interoperability is required, a Federal CKMS **shall** support establishing a key and associated metadata between entities.

• E.g., **PR:6.61+** When interoperability is required, a Federal CKMS **shall** support one or more approved key-establishment protocols.
The Access Control System
(Section 6.7.1)

• **PR:6.62** A Federal CKMS **shall** control access to, and the initiation of, all its key and metadata management services and functions, granting access to and permission to initiate a requested service of function only after verifying the identity and authorization of the requesting entity to perform the requested service of function.

• **PR:6.63** A Federal CKMS **shall** protect the integrity of all keys and their metadata, and the confidentiality of secret and private keys and their sensitive metadata when outside a cryptographic module.
Calling Entity

Function Calls and Responses

ACS

Crypto Service Requests and Responses

Cryptographic module

Protected Storage

Secure Channel

Crypto Service Requests and Responses
KeyManagementFunctionCall:
- entity ID
- entity authenticator
- function name
- key identifier KI

Response:
- function output or
- function denied

Entity IDs and Passwords:
- ID1, PW1
- ID2, PW2
- ... 
- IDn, PWn

Key Management Functions:
- Sym enc
- Sym dec
- SK sign
- PK verify
- Com HMAC
- Verify HMAC
- ...

Keys and Metadata:
- KI1, K1, M1
- KI2, K2, M2
- KI3, K3, M3
- ...
- Kli, Ki, Mi

CryptoServiceRequest:
- encrypt
- decrypt
- sign
- verify
- HMAC
Compromise Recovery
(Section 6.8)

• **PR:6.65** A Federal CKMS **shall** create and maintain a compromise-recovery plan for recovering from actual and suspected compromises of its security and availability.

• **PR:6.66** A Federal CKMS **shall** perform the following when a compromise is detected or suspected:
  – Evaluate compromise,
  – Mitigate compromise,
  – Institute corrective measures, and
  – Return to a secure operating state.
Key and Metadata Compromise (Section 6.8.1, 6.8.2, and 6.8.3)

- **PR:6.67** A Federal CKMS shall revoke compromised keys.
- **PR:6.69** A Federal CKMS shall revoke the key associated with compromised sensitive metadata.
- **PR:6.70** A Federal CKMS shall support reporting and investigation a compromise of sensitive metadata.
- **PR:6.72** A Federal CKMS shall provide a notification when a key is revoked, including the reason for the revocation.
*Computer System Compromise Recovery (Section 6.8.5)*

- **PR:6.74** A Federal CKMS *shall* support replacing modified system software with valid backup copies after the detection of an unauthorized modification to any of its computer system’s software.

- **PR:6.75** A Federal CKMS *shall* support reporting any detected or suspected computer operating system compromise, installing available upgrades, and performing tests to verify that the problem has been fixed.
Network Security Controls and Compromise Recovery
(Section 6.8.6)

- **PR:6.77** If the security of a network security-control device has been compromised, a Federal CKMS **shall**:
  - Repair or replace the device,
  - Test the repaired or replaced device, and
  - Return the FCKMS to a secure state.

- **PR:6.78** If network passwords are compromised, a Federal CKMS **shall**:
  - Replace compromised passwords
  - Notify affected entities
  - Perform damage assessment, and
  - Take corrective actions.
**Personnel Security Compromise Recovery**

(Section 6.8.7)

- **PR:6.79** A Federal CKMS shall perform an assessment of the potential consequences of personnel security compromises before the FCKMS initially becomes operational.

- **PR:6.80** A Federal CKMS shall develop procedures for recovering from a personnel security compromise.

- **PR:6.81** A Federal CKMS shall perform an audit of its personnel security actions after a compromise is detected, and issue revisions to reduce the likelihood of similar compromises.
**Physical Security Compromise Recovery**  
*(Section 6.8.8)*

- **PR:6.82** A Federal CKMS **shall** support the notification of an appropriate authority of any actual or suspected physical security compromise and initiating mitigation actions by that authority.

- **PR:6.83** A Federal CKMS **shall** control physical access to FCKMS devices and restrict access to only authorized entities.

- **PR:6.84** A Federal CKMS **shall** support the evaluation of each new individual before being authorized to perform a role involving the recovery from a security compromise.
Disaster Recovery Overview
(Section 10)

• 10.1 Facility Damage
• 10.2 Utility Service Outage
• 10.3 Communication and Computation Outage
• 10.4 FCKMS Hardware Failure
• 10.5 System Software Failure
• 10.6 Cryptographic Module Failure
• 10.7 Corruption of Keys and Metadata
• **PR:10.1** The components of a Federal CKMS shall be located in physically secure and environmentally protected facilities.

• **PR:10.2**: A Federal CKMS shall have redundancy to ensure operational continuity when high-availability is required.

• **PR:10.3** A Federal CKMS shall support recovery procedures in the event of the damage or loss of an FCKMS capability.

• **PR:10.4** A Federal CKMS shall be operated in facilities that provide levels of protection and availability that are commensurate with the impact level of the information being protected.
**Facility Damage (Section 10.1)**

- **PR:10.5** When a primary facility is damaged, and a backup is available, a Federal CKMS **shall** activate its backup.

- **PR:10.6** A Federal CKMS **shall** be tested annually to determine that facility-damage detection and recovery mechanisms and procedures work as required.

- **PR:10.7** The procedures for maintaining and testing the environmental, physical, and disaster recovery capabilities **shall** be evaluated every five years and upgraded as needed.

- **PR:10.8** Damaged or lost FCKMS devices **shall** be reported to FKMS management personnel.
Utility Service Outage
(Section 10.2)

• **PR:10.9** A Federal CKMS shall be protected with sufficient utility services to support all primary and backup fixed facilities during both normal operation and emergencies.

• **PR:10.10** A Federal CKMS shall conform to applicable Federal and industry standards for utility assurance and satisfy the CKMS design requirements for utility services for all primary, backup, and archive facilities.
• **PR:10.11** When high reliability and availability of the FCKMS services is required, a Federal CKMS **shall** have alternative communications computation, and electrical services available that can be activated as needed.
• **PR:10.12** A Federal CKMS shall perform initial and periodic tests of backup and recovery capabilities of its critical FCKMS modules and devices.

• **PR:10.13** A Federal CKMS shall test backup and recovery of services requiring high availability at least annually.
• **PR:10.14** A Federal CKMS shall use software that has passed correctness and integrity tests.

• **PR:10.15** A Federal CKMS shall perform backups of its software after the current secure-state of the FCKMS software is verified.

• **PR:10.16** A Federal CKMS shall reload its software from the latest FCKMS secure-state backup after a software failure is detected or suspected.

• **PR:10.17** A Federal CKMS shall verify that it is in a secure-state following the initial loading of its software and before becoming operating.

• **PR:10.18** A Federal CKMS shall ensure that all software errors are analyzed and repaired before it is returned to a secure state.
Cryptographic Module Failure (Section 10.6)

- No requirements listed.
- See FIPS 140-2.
- **PA:10.13** Repeat Power-up self tests after error detection already required by FIPS 140-2.
Corruption of Keys and Metadata (Section 10.7)

- **PR:10.19** A Federal CKMS **shall** support:
  - Detecting corrupted keys and metadata,
  - Reporting corrupted keys or metadata to the FCKMS,
  - Preventing the use of corrupted key and/or metadata,
  - Recovering or replacing corrupted keys and metadata.

- **PR:10.20** A Federal CKMS **shall** train CKMS personnel to perform key recovery and replacement.
Circles are Federal Entities; Rectangles are FCKMS Modules; Colors are FCKMS Policies; lines are policy-authorized interactions;
• Entity 1 supports three FCKMS systems, each with its own security policy: green (for external key storage), blue (for key establishment), and red (for key establishment).

• Entity 2 supports only the blue FCKMS security policy for both key establishment and internal key storage.

• Entity 3 supports only the red FCKMS security policy for both key establishment and external key storage.

• Entity 4 supports only the blue FCKMS security policy for key establishment.
• Is the scope of this document too large?
  — Much of the SP deals with general security topics that are not specific to CKMS or FCKMS.
  — For example, security policies, system backup, disaster recovery, operating system security, and personnel management.
  — These topics are well understood by USG agencies.
  — These topics may be better covered in other documents.

• Are some of the requirements too specific for all systems?

• Are any of the requirements too vague to be objectively tested, implemented, used, and verified?
• Are any useful terms left undefined?
  — E.g., High Availability
• Are the defined terms well-defined?