Key and Metadata Storage

Elaine Barker, NIST

Storage and Access

- **Where:** Local, backup or archive storage outside a cryptographic module.

- **Access:** Could be accessed by multiple entities.

Key Protections

(Section 6.1.2)

- An FCKMS **shall:**
  - Physically or cryptographically protect all symmetric and private keys from unauthorized disclosure, use, and modification (PR: 6.2),
  - Support the protection of keys at a level that is commensurate with the impact level of the data to be protected by the keys (PR: 6.3), and
  - Cryptographically protect all keys against unauthorized disclosure and modification when outside a cryptographic module (PA: 6.1).

Store Operational Key and Metadata

(Section 6.4.19)

- An FCKMS **shall** cryptographically or physically protect the integrity of all stored keys and metadata, and the confidentiality of stored private keys, secret keys, and their sensitive metadata. (PR: 6.35). Similar to PR: 6.2.
- An FCKMS **should** cryptographically protect stored keys and metadata. (PA: 6.12). Similar to PA: 6.1.

Cryptographic Module Entry and Output

(Sections 6.4.19 and 6.4.20)

- An FCKMS **shall:**
  - Enter/output keys used to protect information at the Moderate or High impact levels into a cryptographic module as split components or in encrypted form (PR: 6.43 & PR: 6.47). I.e., store the keys in encrypted form or as split components for Moderate and High systems.
  - Enter the sensitive metadata associated with keys used to protect information at the Moderate or High impact levels into a cryptographic module in encrypted form (PR: 6.44). I.e., store the metadata in encrypted form for Moderate and High systems.

Cryptographic Module Entry and Output 2

(Sections 6.4.19 and 6.4.20)

- An FCKMS **should** enter/output keys used to protect information at the Low impact level into a cryptographic module as split components or in encrypted form (PA: 6.16 & PA: 6.18). I.e., should store the keys in encrypted form or as split components for Low systems.
  - Note that the low level does not require the encryption of keys during storage.

Cryptographic Module Entry and Output 3

(Sections 6.4.19 and 6.4.20)

- An FCKMS **should** enter the sensitive metadata associated with keys used to protect information at the Low impact level into a cryptographic module in encrypted form (PA: 6.17). I.e., should store the metadata in encrypted form for Low systems.

Cryptographic Module Entry and Output 4
(Sections 6.4.19 and 6.4.20)

- However,

  An FCKMS **shall** assure that keys and their metadata are protected against replacement, modification, and unauthorized disclosure during entry/output into/from a cryptographic module (PR: 6.46 & PR: 6.48).

  Note: If not protected cryptographically, then the protection must be physical.

Backup a Key and its Metadata

(Section 6.4.15)

- An FCKMS **shall** backup keys and metadata with the same integrity and confidentiality protections as the operational copies of the keys and metadata and at the same or a higher security strength. (PR: 6.36).
- An FCKMS **should** backup long-term keys and metadata on a medium that is separate from that used for the operational storage of the keys and metadata PA: 6.13).

Archive a Key and/or Metadata
(Section 6.4.16)

- An FCKMS **shall:**
  - Archive with the same integrity and confidentiality protections as the operational copies of the keys and metadata and at the same or a higher security strength. (PR: 6.37),
  - Archive in accordance with applicable laws, regulations, and policies (PR: 6.38),
  - Destroy copies of keys and metadata on the old storage medium when archived keys and metadata are moved to a new medium (PR: 6.39).

Archive a Key and/or Metadata 2

(Section 6.4.16)

- An FCKMS **should:**
  - Archive long-term keys and metadata in accordance with SP 800-57, Part 1 (PA: 6.14), and
  - Move archived keys and metadata to an alternate readable storage medium before the old medium is replaced or becomes unreadable (PA: 6.15).

List Key Metadata
(Section 6.4.13)

- An FCKMS **shall** list only specific requested and authorized metadata elements for authorized entities (PR: 6.34).

Recover Key and/or Metadata
(Section 6.4.17)

- An FCKMS **shall:**
  - Support recovering keys and/or metadata that have been backed up or archived, following the FCKMS rules for recovery (PR: 6.40). Make sure the FCKMS Security Policy addresses recovery.
  - Protect the integrity and (if appropriate) the confidentiality of keys and metadata during recovery (PR: 6.41).

Cryptographic Key and/or Metadata Security: In Storage

(Section 6.5)

- An FCKMS **shall**:
  - Authenticate the identity and verify the authorization of the entity submitting keys and/or metadata for storage, and verify their integrity before they are stored (PR: 6.58), and
  - Allow only authorized entities to access stored keys and metadata (PR: 6.59).