* Cryptographic Key Management Workshop

Session 4: Spectrum of Applications

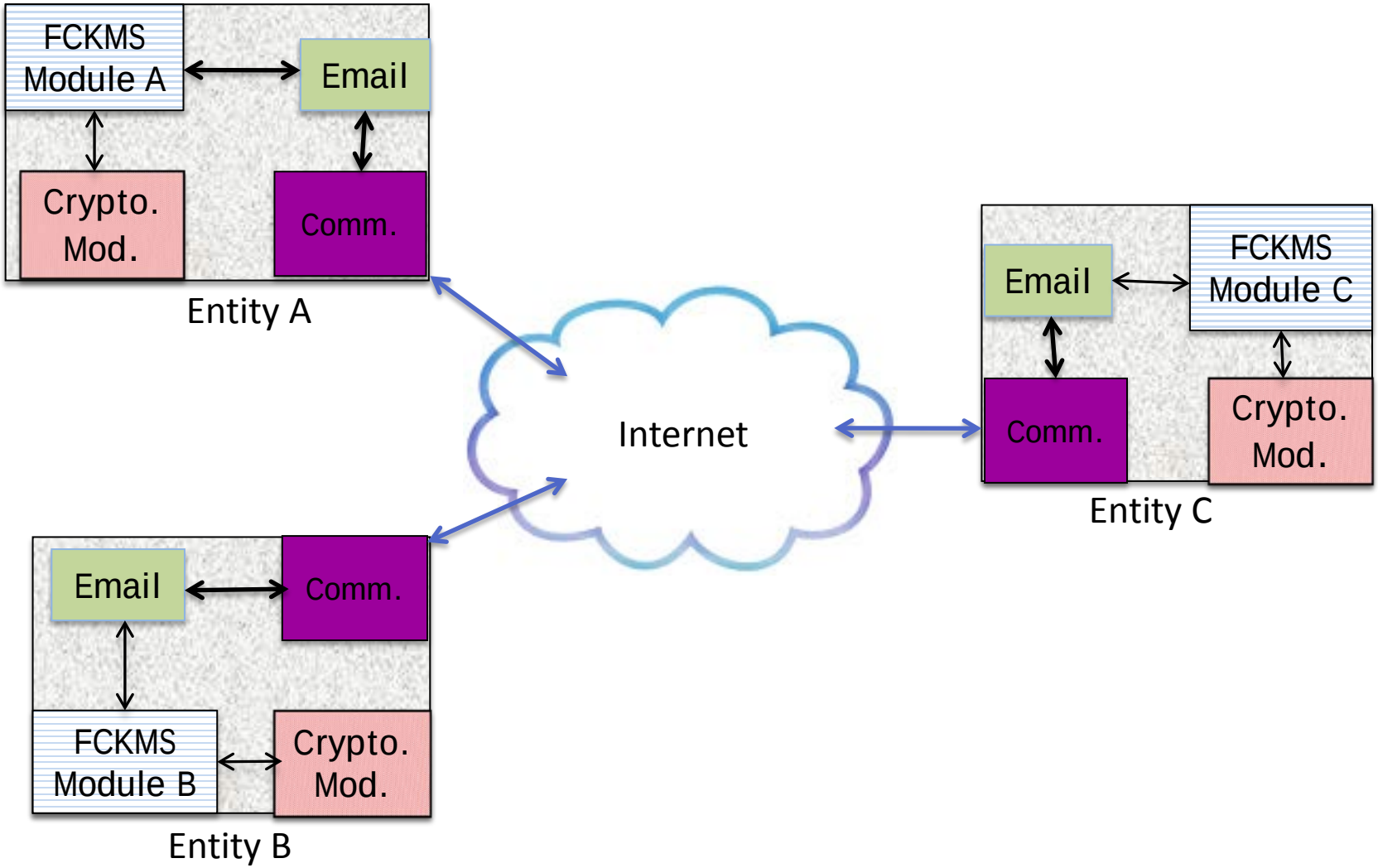
Elaine Barker. et al.

*Application Scope

Goal: To provide a basis for all current and future applications and environments requiring key management for the Federal government.

- Browsers
- Email
- Mobile applications, e.g., laptops, tablets, smart phones, etc.
- Cloud
- Key and metadata storage
- Key establishment

*Email Application



*Email Application

- Entities will need to be in the same FCKMS or Security Domain to establish keys.

*Mobile Applications

Lily Chen, NIST

*Key management in mobile devices

- The keys in a mobile device belong to different stack holders
  - Device specific keys – usually installed by mobile manufactures
  - Communication service authentication keys – in the smartcard – service providers
  - Wireless link protection keys – established with the network (3G, LTE, etc.) – service providers
  - Application specific keys – for different applications such as TLS, DRM, etc. – applications
  - User specific keys – to protect user data – user can lock and unlock using password
  - Enterprise/government keys – in BYOD environment

*Multiple CKMSs in mobile devices

- The mobile devices and service are COTS products
- FCKMS depends on other CKMSs
  - FR:3.4 The CKMS design shall specify the COTS products used in the CKMS
  - FR:3.5 The CKMS design shall specify which security functions are performed by COTS products.
  - FR:3.6 The CKMS design shall specify how COTS products are configured and augmented to meet the CKMS goal.
- The areas and standards to look into
  - Trusted platform (hardware root of trust, Draft NIST SP 800-164)
  - Telecommunication standards (3GPP, LTS, IEEE 802.11, etc.)
  - Application standards (TLS, IKE, DRM, OASIS, etc.)
  - Configurations

*Mobile challenges

- Different CKMSs may have different policies and different goals
- Manufactures may not release the key management details for device keys
- Service authentication keys are provider specific
- New applications are introduced frequently and so are key management issues

*Cloud Security

Michaela Iorga, NIST

*Key and Metadata Storage

Elaine Barker, NIST

*Key and Metadata Storage

- Local, backup or archive storage outside a cryptographic module.
- Could be accessed by multiple entities.
- Section 6.1.2 (Key Protections):
  - **Shall** physically or cryptographically protect all symmetric and private keys from unauthorized disclosure, use, and modification (PR: 6.2).
  - **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 (PR: 6.3).
  - **Should** cryptographically protect all keys against unauthorized disclosure and modification when outside a cryptographic module (PA: 6.1).

*Key and Metadata Storage

- Section 6.4.14 Store Operational Key and Metadata):
  - **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.
  - **Should** cryptographically protect stored keys and metadata. (PA: 6.12). Similar to PA: 6.1.

*Key and Metadata Storage

- Sections 6.4.19 and 6.4.20 (Cryptomodule entry and output):
  - **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.
  - **Shall** 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.

*Key and Metadata Storage

- Sections 6.4.19 and 6.4.20 (contd.):
  - **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).
  - **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.

*Key and Metadata Storage

- Sections 6.4.19 and 6.4.20 (contd.):
  - **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.

*Key and Metadata Storage

- Section 6.4.15 (Backup a Key and its Metadata):
  - **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).
  - **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).

*Key and Metadata Storage

- Section 6.4.16 (Archive a Key and/or Metadata):
  - **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).
  - **Shall** archive in accordance with applicable laws, regulations, and policies (PR: 6.38).
  - When archived keys and metadata are moved to a new medium, copies of keys and metadata on the old storage medium **shall** be destroyed (PR: 6.39).
  - **Should** archive long-term keys and metadata in accordance with SP 800-57, Part 1 (PA: 6.14).
  - **Should** move archived keys and metadata to an alternate readable storage medium before the old medium is replaced or becomes unreadable (PA: 6.15).

*Key and Metadata Storage

- Section 6.4.13 (List Key Metadata):
  - **Shall** list only specific requested and authorized metadata elements for authorized entities (PR: 6.34).

*Key and Metadata Storage

- Section 6.4.17 (Recover Key and/or Metadata):
  - **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.
  - **Shall** protect the integrity and (if appropriate) the confidentiality of keys and metadata during recovery (PR: 6.41).

*Key and Metadata Storage

- Section 6.5:
  - Before keys and metadata are stored, a Federal CKMS **shall** authenticate the identity and verify the authorization of the entity submitting keys and/or metadata for storage, and verify the integrity of the keys and metadata (PR: 6.58).
  - Only authorized entities **shall** be allowed access to stored keys and metadata in a Federal CKMS (PR: 6.59).

*Key Establishment

Elaine Barker, NIST

*Key Establishment

- Establish keys and metadata for use by one or more entities.
- Section 6.4.18 (Establish a Key):
  - When secure interoperability is required, a Federal CKMS **shall** support establishing a key and associated metadata between entities (PR: 6.42).

*Key Establishment

- Obtaining Assurances:
  - Section 6.4.21 (Validate Domain Parameters)
    - ✓ **Shall** validate domain parameters (PR: 6.49).
  - Section 6.4.22 (Validate Public Key)
    - ✓ **Shall** validate using approved methods (PR: 6.50).
  - **Section 6.4.23 (Validate Public Key Certification Path)**
    - ✓ **Shall** validate the certification path prior to using the public key in the certificate (PR: 6.51).

*Key Establishment

- Obtaining Assurances (contd.):
  - Section 6.4.24 (Validate Symmetric Key)
    - ✓ **Shall** validate before initial use (PR: 6.52).
  - Section 6.4.25 (Validate Private Key (or Key Pair)
    - ✓ **Shall** validate before its first use. (PR: 6.53).
  - Section 6.4.26 (Validate the Possession of a Private Key)
    - ✓ **Shall** possession using approved methods (PR: 6.54).

*Key Establishment

- Section 6.4.28 (Manage the trust anchor Store)
  - **Shall** use only trust anchors that merit trust (PR: 6.56).
  - Only authorized additions, modifications, and deletions **shall** be made to trust anchors (PR: 6.57).
  - **Should** use trust anchor formats as specified in [RFC 5914] (PA: 6.19).
  - **Should** perform source authentication, usage authorization, and integrity checks before trust anchors are initially used (PA: 6.20).

*Key Establishment

- Key-establishment process:
  - PR: 2.1 requires support of NIST-approved cryptographic algorithms, schemes and modes of operation. Doesn't require use; should it?
  - Section 6.6.1 (Key Transport)
    - ✓ **Shall** verify the identity and authorization of the source, the integrity of the received data and that confidentiality has been provided (PR: 6.60).

      Section 6.6.2 (Key Agreement)
    - ✓ **Shall** obtain assurance of the identity of each party involved in the transaction. (PR: 6.61).

*Key Establishment

- Key-establishment process (contd.:
  - Section 6.6.3 (Key Confirmation)
    - ✓ **Should** support key confirmation for all key-establishment transactions (PA: 6.21).
  - Section 6.6.4 (Key-establish Protocols)
    - ✓ **Shall** support one or more **approved** key-establishment protocols (PA: 6.22). Note: Change to a PR.

*Questions and Comments?