Key Establishment

Elaine Barker, NIST

Establish a Key
(Section 6.4.18)

- Establish keys and metadata for use by one or more entities.

- When secure interoperability is required, a Federal CKMS **shall** support establishing a key and associated metadata between entities (PR: 6.42).

Obtaining Assurances

- An FCKMS **shall**:
  - Validate domain parameters, when used (Section 6.4.2.1 and PR: 6.49),
  - Validate public keys using approved methods (Section 6.4.22 and PR:6.50), and
  - Validate the certification path prior to using a public key in the certificate (Section 6.4.23 and PR: 6.51).

Obtaining Assurances 2

- An FCKMS **shall**:
  - Validate a symmetric key before initial use (Section 6.4.24 and PR:6.52).
  - Validate a private key (or key pair) before first use (Section 6.4.25 and PR:6.53); required of the owner.
  - Validate the possession of a private key using approved methods (Section 6.4.26 and PR:6.54).

Manage the Trust Anchor Store (Section 6.4.28)

- An FCKMS **shall:**
  - Use only trust anchors that merit trust (PR: 6.56), and
  - Only make authorized additions, modifications, and deletions to trust anchors (PR: 6.57).
- An FCKMS **should:**
  - Use trust anchor formats as specified in [RFC 5914] (PA: 6.19), and
  - Perform source authentication, usage authorization, and integrity checks before trust anchors are initially used (PA: 6.20).

Key-Establishment Process

- PR: 2.1 requires the support of NIST-approved cryptographic algorithms, schemes and modes of operation. Doesn't require use; should it?
- Key-establishment scheme (e.g., as specified in SP 800-56A and B): A set of mathematical operations used to establish keys.
- Protocol (e.g., TLS, SSH, IPsec, etc.): The sequence of messages used to exchange information.

Key-Establishment Process 2

- Key Transport (Section 6.6.1) – i.e., sending a key from one party to another (see SP 800-56A and B)
  - An FCKMS **shall** verify the identity and authorization of the source, the integrity of the received data and that confidentiality has been provided (PR: 6.60).

Key-Establishment Process 3

- Key Agreement (Section 6.6.2) – i.e., two parties determine keys using contributions from each party (see SP 800-56A and B)
  - An FCKMS **shall** obtain assurance of the identity of each party involved in the transaction (PR: 6.61).

Key-Establishment Process 4

- Key Confirmation (Section 6.6.3) – i.e., make sure that the parties have the same key(s)
  - An FCKMS **should** support key confirmation for all key-establishment transactions (PA: 6.21).
- Key-establish Protocols (Section 6.6.4)
  - An FCKMS **shall** support one or more **approved** key-establishment protocols (PA: 6.22). Note: Change to a PR.