PIV CREDENTIALS MAINTENANCE

Agenda

- Renewal
- Reissuance
- Post Issuance Updates
- Termination
- PIV Derived Credentials
- Verification Data Reset

Clarification: Renewal/Reissuance

Comment: The difference between reissuance and renewal of PIV Cards is unclear.

Revised Draft:

- *Renewal:*
  - *The PIV card is valid (uncompromised, not revoked, not expired)*
  - *The cardholder is in possession of the PIV card*
- *Reissuance:*
  - *The PIV card is lost, stolen, damaged*
  - *Logical credentials on-card are compromised*

Renewal

Comment: The renewal process shouldn't require the original PIV Card to be surrendered when requesting renewal.

Revised Draft:

- Original PIV Card shall be collected and destroyed when new card is issued.

Renewal

Comment: Renewal for the purposes of replacing an expiring PIV Card should not be limited to twelve weeks before expiration of old card.

Revised Draft:

Removed restrictions on when renewal may be performed.

Reissuance

Comment: Reissuance should not mandate revocation of certificates if there is no risk that the keys have been compromised.

Revised Draft:

Reissued now only applies to instances in which the old card is lost, stolen, or damaged, or when logical credentials on the card have become compromised. So, mandatory revocation is appropriate.

Post Issuance Updates

Comment: There shouldn't be a requirement to destroy the card if a post issuance update begins but fails.

- This requirement has been deleted.

Comment: Re-key is just a special case of post issuance update.

- The separate section on re-key has been deleted.

Termination

Comment: It is not clear why revocation of digital signature and key management certificates is optional.

Revised Draft:

Indicate that revocation of digital signature and key management certificates is only optional if card is collected and destroyed (per [COMMON]).

Termination

Comment: Unlike for reissuance, the 2011 Draft FIPS 201-2 does not specify a timeframe in which termination must be completed.

The revised draft copies the language from reissuance to require completion of normal termination procedures within 18 hours of notification.

PIV Derived Credentials

Comment: FIPS 201-2 needs to accommodate use of mobile devices that cannot work with contact card readers.

Revised Draft:

Introduce the concept of a PIV derived credential. Details will be specified in SP 800-157*.

* SP 800-157 is still under development.

Verification Data Reset

A procedure to reset the cardholder's on-card reference data for either:

1) PIN

2) fingerprint comparison data

PIN Reset

Comment: It is not clear if remote PIN reset is allowed in the 2011 Draft. Federal agencies should be able to perform PIN resets without requiring cardholders to appear in person before a card issuer.

Remote PIN Reset (continued)

Revised Draft:

Remote PIN reset using a General Computing Environment (desktops, laptops…etc)

1) cardholder initiates PIN reset with the issuer operator

2) operator authenticates PIV cardholder through an out-of-band authentication procedure (e.g., pre-registered knowledge tokens); and

3) Cardholder matches live scan with stored biometric through a 1:1 ***on-card comparison****.*

Remote PIN reset operation via secure mutually authenticated post issuance updates with CMS

.

New On-Card Fingerprint Verification Data Reset

Comment: The fingerprint verification reference data reset should be very similar to the PIN reset. Please combine the procedures.

Response: Remote reset is not applicable for fingerprint reference data reset. Fingerprints need to be re-enrolled – requiring an on-site visit.

Revised Draft:

- 1:1 biometric match to reconnect to the Chain-of-Trust using a different biometric modality (iris, face) than fingerprint image
- When an automated biometric match cannot be performed, an operator compares enrolled image with ID documents, one of which is the PIV card to be reset.
- New verification reference data is enrolled and stored on-card.

Questions (?)