FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

PIV CARD APPLICATION

PKI-CAK

- Issues Raised: CHUID is a weak 1-Factor authentication method for PACS:
  - Analysis from SP 800-116
  - *Over the contactless interface, the CHUID can be sniffed*, skimmed, then *copied (cloned) and replayed.*
  - *Recommendation-1:* access control points separating two areas at the same impact level, either Controlled or Limited;
  - Recommendation-2: combined with the VIS authentication mechanism at access points between Unrestricted and Controlled areas.
  - **Recommendation-3 that the asymmetric CAK authentication mechanism be used instead of the CHUID authentication mechanism to the greatest extent practical.**

PKI-CAK

Desired Functionality:

– A stronger 1-Factor Authentication Method for the PIV Card contactless interface

Proposed Change

- Make the asymmetric CAK mandatory for interagency use, while specify the symmetric CAK as an optional local PACS solution

PKI-CAK

- **PIV Card Capability Changes**
- none to minor change
- Most PIV cards have the asymmetric CAK stored on-card today (as an option)

- Some CAK systems exist: http://fips201ep.cio.gov/apl.php
- Demonstrated Use: The Federated Physical Access Control System (PACS) Demonstration Project (GSA)
- A bit more challenging: implementation of PKI-CAK in existing (legacy) PACS system

6 Year Card Life-Cycle

- Issues Raised: PIV PKI credentials are generally valid for 3 years, while PIV Card validity is set for 5 years,
  - Agencies need to re-key during the card life.
  - Requires in-person visit to get their cards updated.

6 Year Card Life-Cycle:

Desired Functionality:

Align PIV X.509 certificates validity period with the PIV cards validity period

Proposed Change

- 6 year PIV card validity period for the PIV card
- PIV card and PIV X.509 certificates expiration coincide at year 6 – eliminating repeated re-keying
- Additional: Synchronize life-cycle of card, with biometric data.
- Biometric data collected and stored on the PIV card is good for 12 years.

6 Year Card-Life Cycle:

- PIV Card Capability Changes
- **Minor**
- Topographic change (+1 year) expiration
- Logical Credential (CHUID +1 year expiration)

- +1 year change will need to be implemented by personlization system / CMS

Alternative Biometric for Chain-of-Trust

Desired Functionality:

- A re-connect to the cardholder's enrollment records requires biometric 1:1 match using fingerprints
- But….how can a cardholder reconnect BIOMETRICALLY to the enrollment record of a cardholder without fingerprint representation on PIV card or on the enrollment record?

Proposed Change

- Iris defined as the alternative biometric to fingerprint for 1:1 biometric match to the enrollment record's biometrics

Alternative Biometric for Chain-of-Trust

PIV Card Capability Changes

- **minor change**
- The 1:1 biometric iris match is done off-card.
- The card only stores the iris image (~7K)

- Requires card management/personalization systems to provide iris capture capability to store iris image on-card.
- Implementation task is also with Issuer's Chain-of-Trust system to perform 1:1 iris match

Additional Biometric Authentication: Iris (section 6)

- Issues Raised Is there an alternate biometric authentication method other than the current fingerprint off-card comparison (BIO, BIO-A) for authentication?

Additional Biometric Authentication: Iris (section 6)

Proposed Change

- Iris defined as the alternative optional biometric authentication method
- Actual match is done off-card
- If the feature is implemented by an agency, it requires iris recognition capability by the reader.

Additional Biometric Authentication: Iris (section 6)

- PIV Card Capability Changes
- minor change
- The 1:1 iris match is done off-card.
- The card holds the iris image (~7K)

- Implementation task is with the LACS and PACS systems and readers to perform 1:1 iris match

Post Issuance Update

- Issues Raised From the BRM Meeting:

"Requiring in-person registration would prevent Agencies from implementing the ability for users to update PIV Cards with new PKI certificates remotely"

"Post-issuance update is certainly a needed function but should not be required"

Post Issuance Update

Proposed Changes

- A PIV Card post issuance update may be done locally (performed with the issuer in physical custody of the PIV Card) or **remotely** (performed with the PIV Card at a remote location).
- Post issuance updates shall be performed with issuer **security controls** equivalent to those applied during PIV Card reissuance.

Post Issuance: Proposed Change

- For remote post issuance updates, the following shall apply:
- Communication between the PIV Card issuer and the PIV Card shall occur only over **mutually authenticated secure sessions** between tested and validated cryptographic modules (one being the PIV Card).
- Data transmitted between the PIV Card issuer and PIV Card shall be **encrypted** and contain data **integrity checks.**
- The PIV Card will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update.

Post Issuance Update

- PIV Card Capability Changes
- Card Management Capability, which is currently out of scope of FIPS 201-2
  - Each CMS implements its own flavor of remote post issuance update procedure in accordance to FIPS 201-2 security control.
- If Card Management is specified for PIV,
  - Define end-to-end secure channel in SP 800-73-4
  - Data encryption (algorithm, key size) and integrity mechanism to be specified in SP 800-78-4

PIN reset

Definitions:

PIN reset:

- Used in cases where a card's PIN based authentication methods is locked because the wrong PIN has been entered repeatedly -- exceeding number of allowed tries.
- Note: The card is NOT completely locked. PIV card use / authentications that do not require PIN still work.

PIN reset

- To reset PIN, issuer/CMS is not necessary involved, if the cardholders knows the PUK (PIN resetting code) – PUK should be stored securely by cardholder.

PIN change:

- CMS involvement not necessary. To change current PIN, cardholder enters his/her current PIN, followed by the new PIN.
- Can be done with an “PIN change application” on a secure desktop.

PIN Reset (section 2.5.5)

- Issues Raised:
- FIPS 201-2 should define to what extent alternate forms of authentication for PIN reset.

- Can local PIN Reset be accommodated?

PIN Reset

- Security Controls to Maintain (unchanged):
  - A PIN reset requires a Biometric 1:1 match of the cardholder with the biometric stored on the card to **prevent a stolen card to be reset by someone other than the cardholder**

- The card is NOT completely locked. PIV card use / authentications that do not require PIN still work.

- OCC does not require PIN!

PIN Reset

Proposed Change (to be added FIPS 201-2):

– Use OCC card activation to reset the PIN.

….but what about:

– Cardholders with temporary unavailability of live scan due to finger injury at the time of reset or

– PIV card does not have on-card biometrics due to unacceptable quality score / injure

  - cardholder may instead provide a primary identity source document (see Section 2.3) to issuer in order to reset PIN.

PIN Reset

- PIN Reset can be done locally, using on a secure and/or dedicated desktop with PIN reset application.

- Does not need to involve post issuance update procedure (secure end-to-end session between CMS and PIV card)

PIN Reset

- PIV Card Capability Changes
- Implementation of on-card biometric comparison
- storage of OCC fingerprint template

Other Type of Verification Data Reset (OCC Card Activation Reset)

- Issues Raised: Draft FIPS 201-2 includes an option for On-Card Biometric Comparison (OCC) to activate the PIV card for privileged operations. **How can OCC verification data be reset on-card?**

Other Verification Data Reset

- Observation: Biometric verification data reset is different than PIN Reset. A cardholder can forget the PIN, but not his/her biometric.
- Most common reason for biometric verification data reset:
- Due to poor fingerprint quality
  - a. Accidently stored a poor quality biometric on the card
  - b. Poor live scan at time of authentication attempt
- Time lapse – The cardholder's fingerprints 'aged' over time and do not compare/authenticate easily with on-card 'younger' fingerprints, eventually locking the card activation via OCC.

Other Verification Data Reset

- Verification data ‘reset’ of biometric verification data done through re-enrollment of biometric.
- Security Measures Maintained (unchanged):
  - A ‘reset’ requires a Biometric 1:1 match of the cardholder live scan with the biometric stored on the card or with the enrollment record’s biometric. This prevents a stolen card to be reset by someone other than the cardholder.

Other Verification Data Reset

Proposed Change:

– Use different type of biometric (iris) to ‘reset’(re-enroll) verification data (OCC data).
  - In case iris live scan is unavailable due to temporary injury (eye patch) or
  - in case there is no alternative biometric,
  - provide a primary identity source document (see Section 2.3) to issuer in order to reset verification data (OCC data).

Other Verification Data Reset

- PIV Card Capability Changes
- Storage of iris on-card (7K)

- Re-enrollment done with Issuer/CMS
  - Iris matcher
  - OCC re-enrollment

On-Card Biometric Comparison for Authentication

- Desired Feature
- In collaboration with federal agencies and industry, NIST researched and published "Secure Biometric Match-on-Card Feasibility Report " in 2007
- The Business Requirement Meeting re-confirmed need for Match-on-Card capability for
  - 1) optional PIV card activation (instead of PIN)
  - **2) an optional authentication method (contact and contactless interface)**

On Card Biometric Comparison for Authentication

- PIV Card Capability Changes
- Biometric template storage on-card
- An additional on-card application for biometric match implementation
- If OCC is used over contactless interface:
  - Addition of secure channel, data encryption and integrity check is needed

Questions?

The business requirement meeting showed conflicting interest in contactless OCC needs. Some agency did not want/need OCC on the contactless interface. We would like to hear if contactless OCC is desired and its specific use case.

Thank you

Hildegard Ferraiolo

hferraio@nist.gov