Physical Access Control and PIV

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Status Quo: FIPS 201 Revision 2

- Up to three factors for authentication (Have, Know, Are)
- Three area of facility access (restricted, limited, exclusion)

- Two factor and three factor authentication – is it used?

- One factor authentication
  - CHUID authentication mechanism deprecated in R2 with additional text indicating its removal in a future revision
  - CAK became a mandatory on-card authenticator
    - one of CHUID's replacement mechanism, but is sparingly in use

- Secure Messaging / Virtual Contact Interface introduced

Most PACS related PIV material/use cases are specified in SP 800-116, not the FIPS. Let's keep it that way.

FIPS 201 R3 Proposed Changes

Proposed changes will be coordinated with ISC to identify security and interoperability requirements in consideration of alternative long-term approaches

- Remove CHUID Authentication Mechanism in FIPS 201 due to security concerns
  - CHUID authentication mechanism to remain in SP 800-116 as “legacy mechanism” with associated risk based use
  - PKI-CAK to remain one of the alternative for one factor authentication

FIPS 201 R3 Proposed Changes

- Other options to add in SP800-116 R2 over time (e.g., server based biometric matching based on PIV card identifier provided by PIV Card)
- Enable use of mobile devices as one factor wireless authentication

CHUID Authentication Mechanism ALTERNATIVES - Desired PACS Properties

- First line of defense (entry from unrestricted to restricted area)
- High traffic -> fast authentication
- 'Touch and go' wireless transaction desired
- Based on mature, stable Standard

Alternative: PIV Card's PKI-CAK

- Public key challenge/response is slower. It could improve with optimization
  - Use ECDSA, instead of RSA based cryptographic algorithms
  - FIPS 140-2 POST optimization,
  - card/reader speed negotiation optimization
  - Improved hardware (card and reader)
  - Expectation Management
    - Reading a static number off the card (CHUID FASC-N) will always be faster. A reasonable slow down is to be expected.
    - Analog to PIN and Chip transaction slow down– we are more tolerant/ accepting and transaction time improved.

Continued Alternatives PIV Card Server-Based

Proposed Addition: Server-based authentication

- Read of UUID/FASC-N identifier from PIV card to look up biometric stored on server and to match server retrieved template with live scan.

- Specified in PIV and ePACS document
- Several options possible: fingerprint, face or iris matching

- Q: Are these mechanisms used? Does your organization see value to add mechanism?

Continued Alternatives Mobile Devices

Proposed Addition: Use of Mobile Device in PACS

- Mobile Devices with Near Field Communication (NFC) are a natural fit for PACS installed base - both communicate wirelessly via ISO/IEC 14443
- Should other communications protocols be considered? Are there pilots in Federal Government?

PACS FIPS Revision Goals/Considerations

- Keep current set of PIV card Authentication mechanisms in FIPS 201 but
- New Authentication schemes to be part of SP 800-116

PACS infrastructure refresh cycles are slow

- FIPS 201-3 should enable mechanisms that can interact with current PACS installed base
  - For wireless communication: Use of contactless protocols (ISO/IEC 14443) – enabling mobile devices and NFC
  - Not all smartphones devices support NFC in card emulation mode
  - For wired communication: ISO/IEC 7816

Questions?

Contact Information

PIV PoC:
Hildegard Ferraiolo
PIV Program Manager
hildegard.ferraiolo@nist.gov

Andrew Regenscheid
Andrew.Regenscheid@nist.gov