FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

SECURE CHANNEL PROTOCOLS

Authentication Using On-card Biometric Comparison

- Section 6.2.5 of March 2011 Draft FIPS 201-2
- Contact or contactless interface
- Card to reader authentication required
- Live-scan biometric is supplied to card (encrypted)
- Card sends success or failure indicator (integrity protected)
- See NIST Interagency Report 7452 for one possible implementation

Card Management

- Support for remote post-issuance update on data on cards by Card Management System (CMS).
- Mutual Authentication between card and card management system (CMS).
- Data must be encrypted and integrity protected.

Other Use Cases?

- Allow more (all?) card operations to be performed over the contactless interface?
- Enable secure channel to be used with other applications on PIV Card?

Secure Channel Properties

- Inter-agency interoperability: **required**
- One protocol or multiple protocols?
  - Should secure channel protocol(s) be standardized for all use cases or should card management operations be excluded?

Secure Channel Properties (cont.)

- Card-to-reader authentication only?
- Mutual authentication?
- Cardholder identity only revealed to authenticated reader?
- What are the infrastructure requirements?
- Who will operate the infrastructure?

Example: OPACITY

- Supports both card-to-reader authentication and mutual authentication
- Each card requires a Card Verifiable Certificate (CVC)
- Each reader that supports mutual authentication requires a CVC
- Root public keys are needed to verify CVCs
- Who issues the CVCs? How many root public keys are there? How are lists of root public keys on cards and readers managed?