Authenticating PIV for PACS

David Engberg, CTO

PIV Electronic Interfaces

ISO 7816-4 contact interface

- Mandatory X.509 authentication certificate
- On-card 6-8 digit PIN with retry limits
- Two fingerprint biometric templates
- Static Cardholder Unique Identifier (CHUID)
- Optional facial image

ISO 14443 contactless interface

- Static Cardholder Unique Identifier (CHUID)
- Optional X.509 card authentication cert
- No biometrics, no PIN

PIV Authentication: Contact Interface

Step 1: Read certificate

Step 2: Validate certificate

Step 3: Challenge PIN

Step 4: Confirm PIN

Step 5: Challenge Private Key

Step 6: Verify Private Key Operation

Step 7: Read biometric(s)

Step 8: Match biometric(s)

CoreStreet

Revocation Checking: OCSP

Step 1: Read certificate

Step 2: Validate certificate

Step 3: Challenge PIN

Step 4: Confirm PIN

Step 5: Challenge Private Key

Step 6: Verify Private Key Operation

Step 7: Read biometric(s)

Step 8: Match biometric(s)

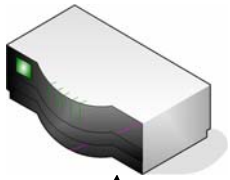
(OCSP)

CoreStreet

PIV Authentication: Contactless Interface (Mandatory)

Step 1: Read CHUID (FASC-N + Signature)

Lower Assurance Authentication



Access Control System

FASC-N

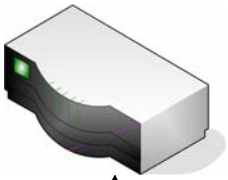
Readers

CHUID

Contactless PIV

- Free read data only
- Low anti-counterfeiting
- Fast (card only)

Higher Assurance: Off-Card



Access Control System

FASC-N with biometric and/or PIN

Readers

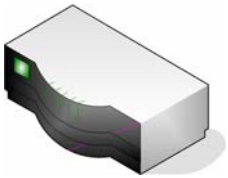
CHUID

Contactless PIV

- **Low assurance card plus second (third …) factors**
- **PIN or biometric enrolled and stored in PACS**
- **Slower user interaction**

CoreStreet

Enrollment: Use the Card!



Access Control System

CHUID
PIV Auth Cert
ANSI 378 biometrics
Facial Image

Contactless Badge

- **Enroll existing cards, issued by ANY agency**
- **Strongly authenticate cardholder before enrolling**
- **Check revocation during enrollment and periodically after**
- **PIN or biometric enrolled and stored in PACS**
- **Slower user interaction**

PIV Authentication: Contactless Interface (Optional)

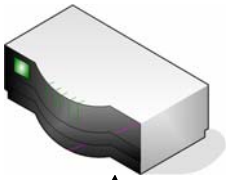
Step 1: Read certificate

Step 2: Validate certificate

Step 3: Challenge Private Key

Step 4: Verify Private Key Operation

Higher Assurance: Certificate-Based (Optional)



Access Control System

Certificate + Key Challenge

Readers

Certificate + Key Challenge

Contactless PIV

- **Cryptographic challenge-response protocol**
- **Strong anti-cloning**
- **Fast**

Questions

Questions?

David Engberg

dave@corestreet.com