Derived PIV Credential – A Proof of Concept Implementation

Jeffrey Cichonski
NIST
National Cybersecurity Center of Excellence (NCCoE)

- Established in 2012.
- Part of NIST Information Technology Lab.
- Work with business sectors to define cybersecurity challenges.
- Identify applicable cybersecurity standards, guidelines, and recommended practices.
- Partners with industry to develop cybersecurity solutions using commercial technology.
NCCoE ‘Use Cases’ and ‘Building Blocks’

- A Use Case attempts to solve a business sector specific challenge.
  - e.g. Health Care, Energy, U.S. Government.

- A Building Block attempts to develop a very specific scoped solution applicable across multiple business sectors.
  - Investigate the Derived PIV Credential building block by identifying the requirements and necessary components to build a solution.
  - Identify partners and commercial IT products to support the proof of concept implementation.
Enable the use of a Personal Identity Verification (PIV) Credential on a device whose form factor does not support the use of smart cards for mobile devices.

Leverage existing PKI infrastructure and PIV cards.
Example Use Case Scenario

- Provide logical access to remote resources hosted within an on-premises data center or in a public cloud.

- Sign and encrypt email on the device.
Usage Scenario #1

- Organization provisions PIV cards internally using a card management system (CMS) and internal PKI.
  - Capable of supporting the issuance, maintenance, use, and termination of derived PIV X.509-based credentials
- Deploying modern client devices.
  - No - smart card reader
  - Yes – embeded hardware or software token
Organization wants to leverage shared provider-provisioned PIV credentials.
- Generate derived PIV Credential internally.
- Local CMS and PKI will support issuance, maintenance, use and termination of DPC

Deploying modern client devices.
- No - smart card reader
- Yes – embedded hardware or software token
General Characteristics

- Private cryptographic key stored in hardware or software cryptographic module.
- Easily inserted into mobile device e.g. Micro SD, USB token, and embedded cryptographic module existing on the mobile device.
- The ability to issue credentials of SP 800-63 Level of Assurance 3 and Level of Assurance 4.
- Leverages identity proofing and vetting results of PIV credential.
- Enrollee’s proof of possession of a valid PIV Card to receive a Derived PIV Credential.
- The derived credential certificate must be an x509 public key certificate meeting the requirements of the Federal PKI Common Policy Framework.
Workflow

Personal Identity Validation (PIV) Issuance Process

**Step 1:**
User and biometric information provided to registrar
Information is added to CMS

**Step 2:**
CMS imports the computer and user information from directory service

**Step 6:**
User self collects Derived PIV Credential

Relying Party Process

**Step 3:**
CMS maps the PIV credential to a user record

**Step 4:**
Enrollee validation – user visits kiosk or registrar presents physical card and performs:
- Biometric Match
- Real-time Card Validation

**Step 5:**
Registrar approves queues user1/Device1 Derived PIV Credential

Kiosk or Registrar

Registrar

Org\User1

Org\Device1

Org\User1

Org\Device1

Directory Service
Implementation Challenges

- Technical and procedural requirements for the assertion of e-authentication LOA of the derived PIV credential.
- Enrollment and issuance processes to varying crypto container technologies.
- Credential Lifecycle management
  - i.e. PIN unlock process
  - PIV card event triggering
- Need process to inform internal CMS about changes to enrollee PIV card
Next Steps

- Release the building block description for public comments
- Identify industry partners
- Develop and implement the proof of concept implementation
References

- NIST DRAFT SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials
- NIST SP 800-63-2 Electronic Authentication Guideline
Thank You!

- Questions?