

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

Problem to Solve

- 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.

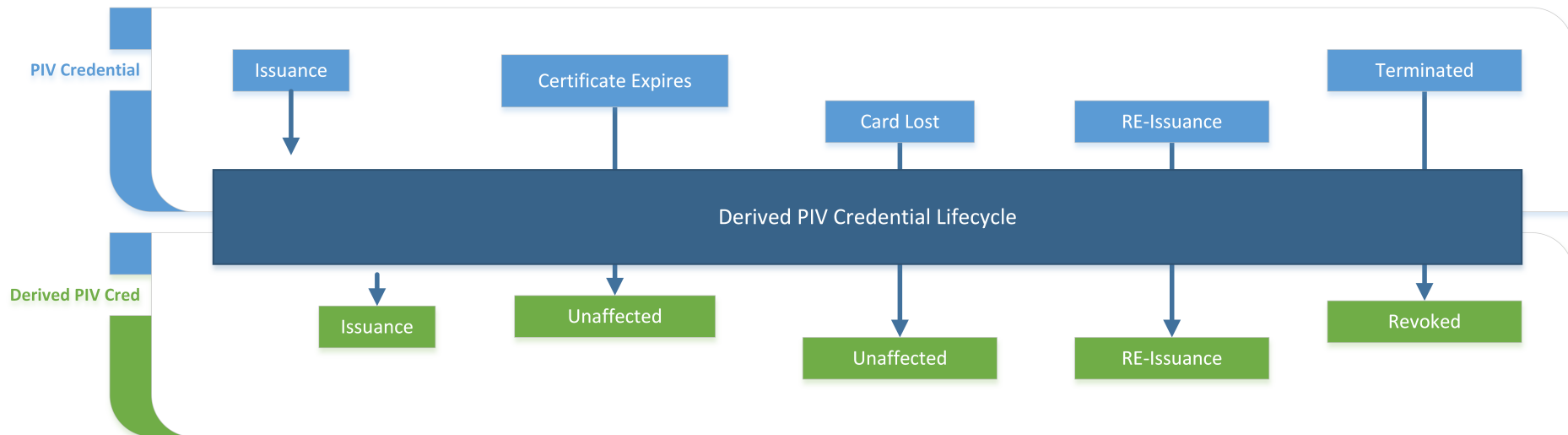
Example Use Case Scenario

1. Authenticate remotely to hosted resources using the Derived PIV Credential.
2. Sign and encrypt email on the device.

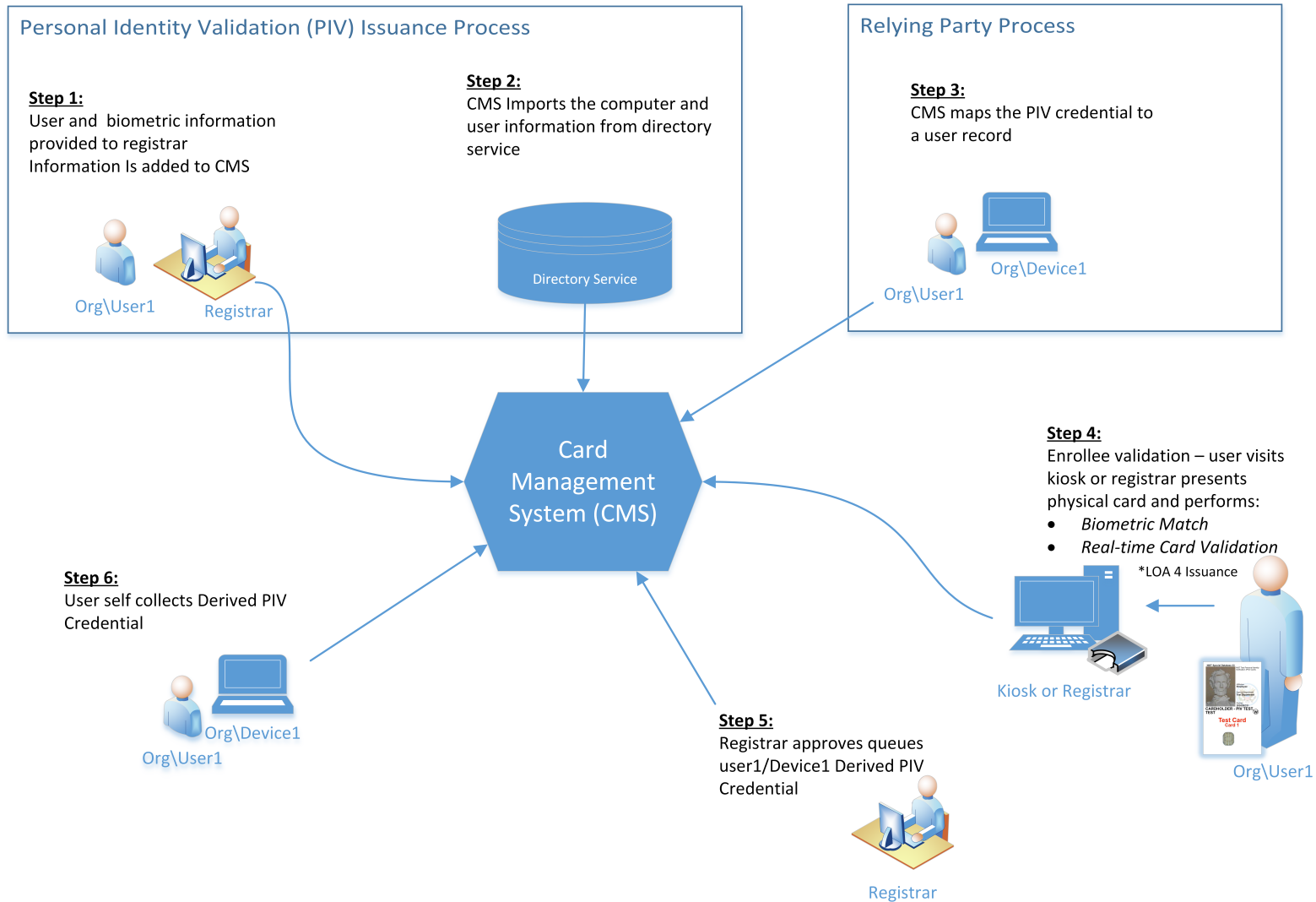
Requirements

- 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.

Derived PIV Lifecycle



Workflow



Next Steps

- Finalize the building block description
- Release 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?