FPKIPA

Federal Public Key Infrastructure Policy Authority

FPKI
Common Derived PIV Certificate Policies

FIPS 201-2 Associated Special Publication Workshop

Matt King & Wendy Brown

FPKIPA

4 March 2015

Agenda

- FPKI Overview
- Common Derived PIV Certificate Policies
- Q&A

Background

- FPKI Policy Authority (FPKIPA) responsible for defining Certificate Policy for Federal Public Key credentials
    - Federal Common Policy CP defines policies for HSDP-12 Personal Identify Verification (PIV) Cards
    - PIV Cards only for Federal Employees and Contract support
    - PIV Cards require a PIV-Authentication certificate
    - The smartcard form-factor is not always compatible with current mobile devices

Solution

- FIPS 201-2 defines additional PIV authentication certificates available for logical access from mobile devices
- SP 800-157 *Guidelines for Derived Personal Identity Verification (PIV) Credentials*
  - References Certificate Policies defined in Federal Common Policy CP
- Federal Common Policy CP defines requirements for issuance of acceptable PIV certificates

Common Derived PIV

- Only available for current PIV holders
- Leverages PIV for ID-Proofing
- Considered a PIV authentication certificate when use of PIV Card is not possible
  - Logical access only[1]
  - Meets PIV according to FISMA

[1] The limits on use (for logical access only) are stipulated in NIST SP 800-157

Common Derived PIV - Scope

- It's about *Authentication* of Humans
  - The scope of Common Derived PIV is limited to an *Authentication* certificate[1]
- *Not* Signature or Encryption

[1] The limits on use (for logical access only) are stipulated in NIST SP 800-157

Use Cases

- Common Derived PIV Use Case: In Scope
  - Authentication
    - Network/web apps
      - PIV or
      - Common Derived PIV now allowed
- Use Case: Out of Scope for Common Derived PIV
  - Authentication
    - PACs
      - Only allowed with PIV Card
      - *Prohibited* for Common Derived PIV by NIST 800-157
  - Email & Documents
    - Signature and encryption
      - Signature and encryption certificates asserting Common and Common Hardware certificate policies are already allowed on multiple devices

Q&A