



Identity, Credential, and Access Management

Understanding the differences in PIV, PIV-I, PIV-C August 23, 2010

Tim Baldrige
AWG Co-Chair
Office of the CIO
NASA
tim.baldrige@nasa.gov



Non-Federal Issuer (NFI) Trust Governance

- The Federal Bridge Certification Authority (FBCA) Certifies NFIs For Use By Federal Relying Parties
- The FBCA Certificate Policy (CP) Contains The Detailed Requirements That Those NFIs Must Meet
- There Is No Intent Or Expectation For Trust By Federal Departments And Agencies Of Cards Or Tokens Where Certificates Are Issued Outside The Federal PKI Policy Authority



Normative PIV-I and PIV-C Reference Documents

- http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
- http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf
- http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf
- http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf
- http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf



PIV Cards

➤ Personal Identification Verification Cards

- Cornerstone Credential For All Security Controls For Both Information Resources And Facilities Protection
- In HSPD-12 Federal Departments And Agencies Are Required To Issue PIV Cards to Permanent Government Personal And Contractors
- Issued ONLY By Federal Entities
- May Be Relied On By Federal And Non-Federal Entities
- Background Investigation – Minimum NACI
- Assert Federal Common Policy Framework (FCPF) Certificate Policy OIDs for PIV



PIV-I ... PIV Interoperable Cards

- Personal Identification Verification – Interoperable (by Non-Federal Issuers – NFI) Cards
 - Cornerstone Credential For All Security Controls For Both Information Resources And Facilities Protection
 - Intended Primarily For Issuance By Non-Federal Entities
 - May Be Relied On By Federal And Non-federal Entities
 - Identity and Affiliation Certainty Equivalent to PIV
 - No Issuer Background Investigation of Cardholders
 - Asserts Federal Bridge Certificate Authority (FBCA) Certificate Policy OIDs for PIV-I



PIV-C ... PIV Compatible Cards

- A PIV-C (Personal Identity Verification – Compatible) Card meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government Relying Parties (RPs).
 - Sole Allowance To Trust Existing Legacy Issuance By Non-Federal Entities Who Otherwise Meet FBCA CP Requirements Except PIV-I
 - May Be Relied On By Federal And Non-federal Entities Up To The Extent Permitted By FBCA CP For Hardware Tokens
 - No Issuer Background Investigation Of Cardholders
 - By Definition PIV-C Must Not Assert or Map to FCPF PIV or FBCA PIV-I Certificate Policy OIDs



PIV Interoperable for Non-Federal Issuers

- Is not a replacement for PIV
- Requires the same enrollment process as PIV
- Does not assert any level of individual trustworthiness
 - No Background Investigation
 - Only I-9 Document Verification
- In a three factor (have, know, are) authentication PIV-I is a very high confidence identity assertion (Level 4)
- No need to revoke cards when individuals leave an Agency, thus relieving the relying Agencies of temporary credential costs and the need to recover credentials at contract completion or other separating events



PIV-I Hardware Subject DN

- PIV-I Hardware certificates shall indicate whether or not the Subscriber has an Organizational Affiliation by taking one of the following forms:
 - **For certificates with an Organizational Affiliation:**
 - *cn=Subscriber's full name, ou=Affiliated Organization Name,{Base DN}*
 - **For certificates with no Organizational Affiliation:**
 - *cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}*



PIV-I Card Authentication Subject DN

➤ PIV-I Card Authentication certificates shall indicate whether or not the Subscriber has an Organizational Affiliation by taking one of the following forms:

- **For certificates with an Organizational Affiliation:**
 - `serialNumber=UUID, ou=Affiliated Organization Name,{Base DN}`
- **For certificates with no Organizational Affiliation:**
 - `serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}`



One Note...

- NIST 800 76-2
 - Biometric Data Specification for Personal Identity Verification
 - Revision is in work at NIST – Public Draft expected.
 - Normative Specification for inclusion of UUID in CBEFF header



The Realized Value of Federal PKI Infrastructure

➤ <https://www.idmanagement.gov/documents/RealizedValueFederalPKI.pdf>

➤ Hitchhiker's Guide to PKI...

- Evaluate forward Trust Path
 - Certificate Policies
 - Policy Mapping
- Check for Revocation of each Certificate in Chain
- Evaluate Root Certificate
 - Assurance Level (Certificate Issuance Policy)
 - Purpose (Certificate Application Policy – EKU)
- Cache Results



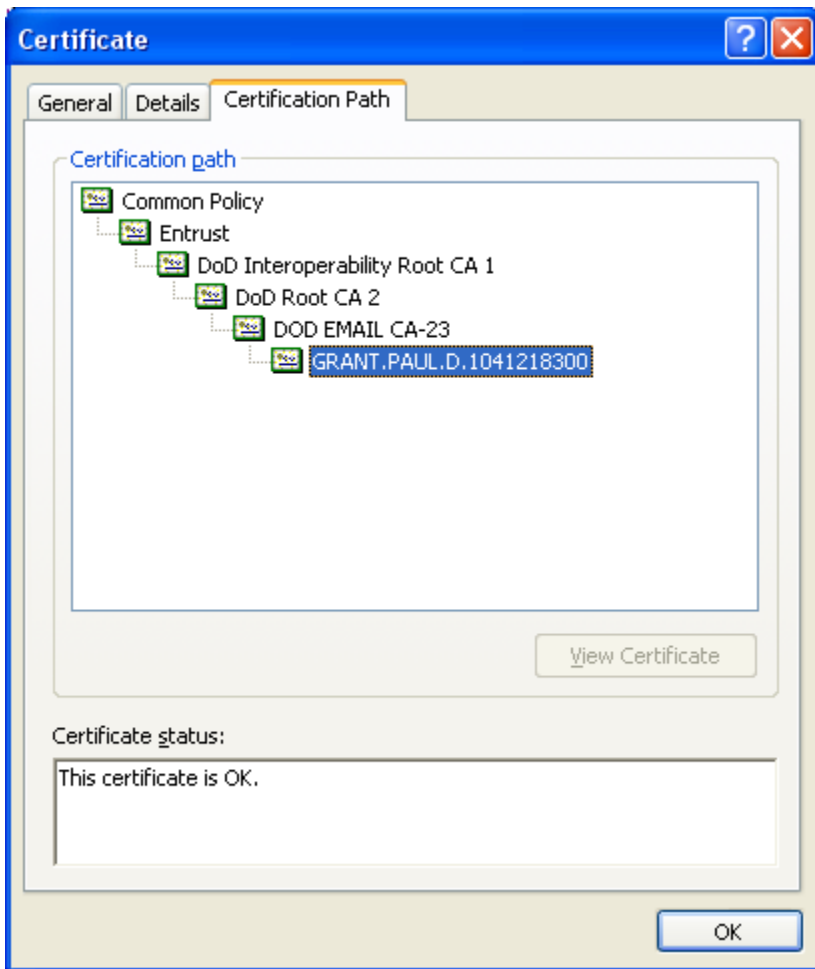
Identity, Credential, and Access Management

http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/pki_registration.html

- 2.16.840.1.101.3.2.1.3.1 id-fpki-certpcy-rudimentaryAssurance
- 2.16.840.1.101.3.2.1.3.2 id-fpki-certpcy-basicAssurance
- 2.16.840.1.101.3.2.1.3.3 id-fpki-certpcy-mediumAssurance
- 2.16.840.1.101.3.2.1.3.4 id-fpki-certpcy-highAssurance
- 2.16.840.1.101.3.2.1.3.5 id-fpki-certpcy-testAssurance
- 2.16.840.1.101.3.2.1.3.12 id-fpki-certpcy-mediumHardware
- 2.16.840.1.101.3.2.1.3.14 id-fpki-certpcy-medium-CBP
- 2.16.840.1.101.3.2.1.3.15 id-fpki-certpcy-mediumHW-CBP
- 2.16.840.1.101.3.2.1.3.18 id-fpki-certpcy-pivi-hardware
- 2.16.840.1.101.3.2.1.3.19 id-fpki-certpcy-pivi-cardAuth
- 2.16.840.1.101.3.2.1.3.20 id-fpki-certpcy-pivi-contentSigning
- 2.16.840.1.101.3.2.1.3.6 id-fpki-common-policy
- 2.16.840.1.101.3.2.1.3.7 id-fpki-common-hardware
- 2.16.840.1.101.3.2.1.3.8 id-fpki-common-devices
- 2.16.840.1.101.3.2.1.3.13 id-fpki-common-authentication
- 2.16.840.1.101.3.2.1.3.16 id-fpki-common-high
- 2.16.840.1.101.3.2.1.3.17 id-fpki-common-cardAuth



Example Forward Trust Path



- Policy Identifier- Leaf
 - 2.16.840.1.101.2.1.11.9
 - id-US-dod-mediumhardware
- Policy Mapping
 - Issuer Domain
 - 2.16.840.1.101.3.2.1.3.12
 - id-fpki-certpcy-mediumHardware
 - Subject Domain
 - 2.16.840.1.101.2.1.11.9
 - id-US-dod-mediumhardware
- Policy Identifier – Root
 - 2.16.840.1.101.3.2.1.3.7
 - id-fpki-common-hardware



Identity, Credential, and Access Management

- Federal Departments and Agencies as RPs are solely responsible for discriminating between PIV, PIV-I and Medium Hardware PKI certificates issued under FCPF and FBCA in determining access to information resources and facilities.
- PIV, PIV-I and Medium Hardware PKI certificates issued under FCPF and FBCA are intended to provide the highest practical remote network authentication assurance (Level 4 NIST SP 800-63-1 draft)



Mapping Certificate Policy to Access Control

- [http://technet.microsoft.com/en-us/library/dd378897\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd378897(WS.10).aspx)
- **Authentication Mechanism Assurance**
 - **Feature of Windows Server 2008 R2 Directory Services**
 - When a certificate-based logon method (for example, smart-card logon) is used, and authentication mechanism assurance is enabled, an additional group membership is added to the user's access token during logon
- HSPD-12 Logical Access Authentication and Active Directory Domains.doc
- <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=b86d8fe2-a76a-4692-9983-5ee65f0f4e88>



Take Home

- PIV and PIV-I Assurance More Than Some Confidence IF You...
 - Validate Digitally Signed Objects
 - Validate Certificates to a Qualified Trust Anchor
 - Validate All Certificates In Trust Path Are Not Revoked
 - Satisfactory Dept. & Agency Initial or Reciprocal BI Check for PIV-I



Take Home (continued)

➤ Important PIV-I Internal Efficiency Gains

- Reliable, Effective And Convenient Enrollment And Card Issuance For Transient Personnel To Establish Identity Certainty For Both Federal And Non-federal Relying Parties
- The Rigor Followed For Single Card Issuance Permits Card Use For A Multitude Of Federal And Non-federal Applications And Facilities Access
- Departments And Agencies Use Of OPM For Background Investigations And Reporting Adjudication Results To The Opm Central Verification System (CVS) Offers A Central Repository For Reciprocity Reduces Bi Cost And Time As Individuals Move Among Departments And Agencies



QUESTIONS