Personal Identity Verification (PIV) Cards as Federated Identities – Challenges and Opportunities

Dr. Sarbari Gupta

sarbari@electrosoft-inc.com

703-437-9451 ext 12

8th Symposium on Identity and Trust on the Internet (IDtrust 2009)

April 14-16, 2009

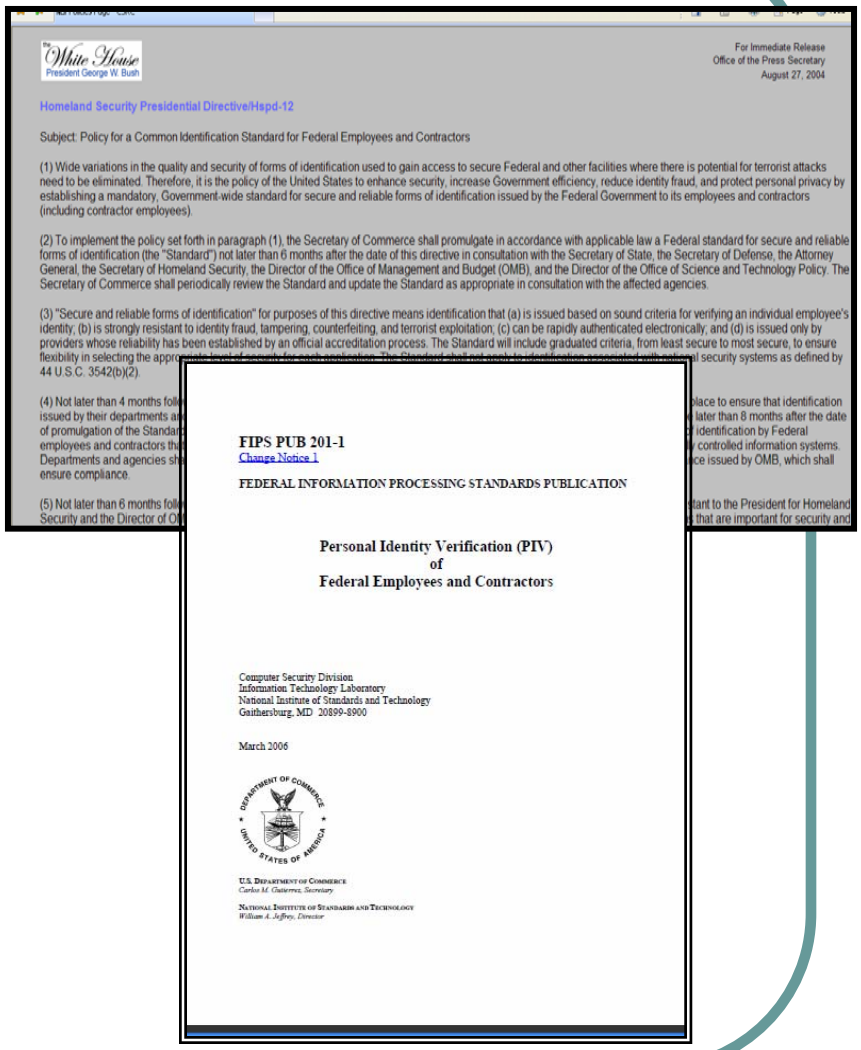
Electrosoft

Overview

- HSPD-12 requires Federal agencies to issue PIV Cards to all employees and contractors
- State/Local governments and commercial entities are issuing PIV-like Cards
- Immense opportunity to use PIV Cards (and PIV-like cards) as federated identities
  - Challenges
  - Strategies to promote federation

HSPD-12 Background

- **Homeland Security Presidential Directive 12**
  - Issued *August 2004*
  - Mandates Federal Agencies to issue common form of identification to Federal employees & contractors
- **FIPS 201 - Personal Identity Verification (PIV) of Federal Employees and Contractors**
  - PIV Card: Smart Card based digital identity container with a set of identity credentials
- **PIV Card Issuers are required to be accredited by Agency Official**
  - SP 800-79-1 – Accreditation Guide



The White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appr… …l security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months follo… …lace to ensure that identification issued by their departments a… later than 8 months after the date of promulgation of the Standar… identification by Federal employees and contractors th… controlled information systems. Departments and agencies sh… …ce issued by OMB, which shall ensure compliance.

(5) Not later than 6 months follo… …tant to the President for Homeland Security and the Director of O… that are important for security and

FIPS PUB 201-1
Change Notice 1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV)
of
Federal Employees and Contractors

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

March 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William A. Jeffrey, Director

PIV Card Credentials

- **Mandatory Credentials:**
  - **Cardholder Unique Identifier (CHUID)**
  - **PIV Authentication Private Key and X.509 Certificate (PKI)**
  - **Cardholder Fingerprints in Biometric Object (BIO)**

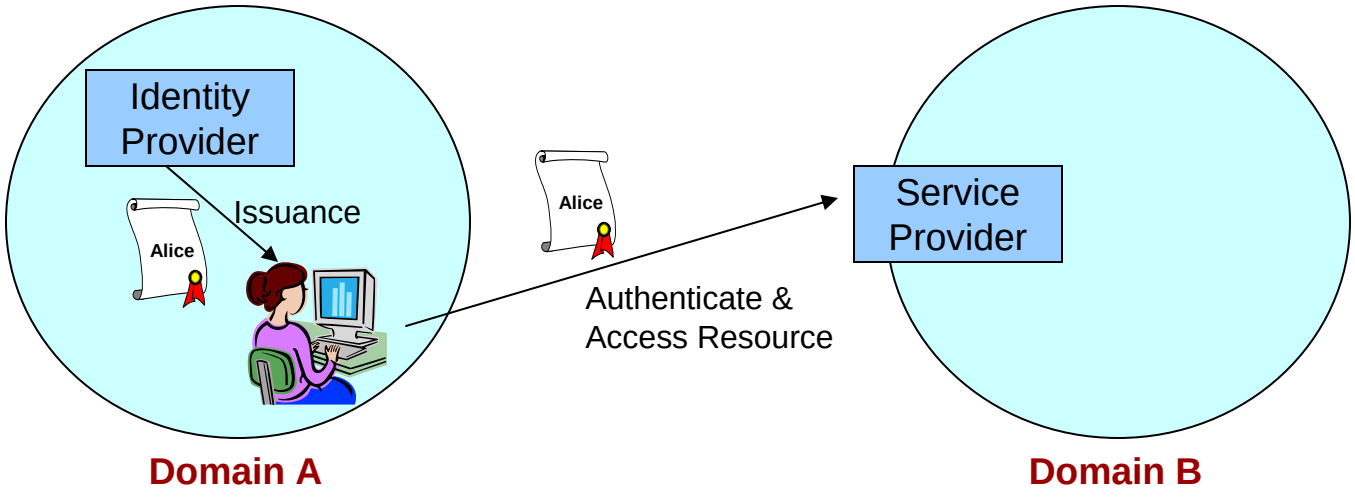
- **Optional Credentials:**
  - **PIV Card Authentication Key (CAK)**
  - **PIV Digital Signature Private Key & X.509 Certificate**
  - **PIV Key Management Private Key & X.509 Certificate**
  - **Cardholder Facial Image**

Pictures courtesy www.fedidcard.gov

Digital Identity Federation

- ***Identity federation can be defined as 'the agreements, standards and technologies that make identity and entitlements portable' across otherwise autonomous security domains [Burton Group]***

- ***Goal: Enable users of one domain to securely access data or services of another domain***



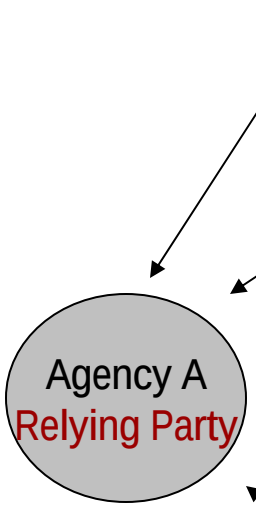
PIV-Interoperable & PIV-Compatible Cards

- **Defined to promote *identity federation* between Federal and non-Federal Organizations**
- **Issued to personnel not eligible for PIV Cards**
  - **State and Local Government**
  - **Commercial Organizations**
- **PIV Compatible:**
  - **Meets technical specifications for PIV Card**
  - **Issuance process does not assure trust by federal relying parties**
- **PIV Interoperable:**
  - **Meets technical specifications for PIV Card**
  - **Issuance process assures trust in PKI Certificate**
    - **E-Authentication Level 4 Registration Requirements**
    - **PKI certificate issued under policy mapped to FBCA *Medium-HW* policy**

FIPS 201 & FBCA Medium-HW Policy

FIPS 201-1	FBCA *Medium-HW* policy
NACI has to be completed for full scope PIV card.	NACI not required for regular applicants.
FBI fingerprint check required.	Fingerprint check not required.
Facial image collected at registration.	Facial image not collected.
The applicant must appear in person at Registrar at least once prior to issuance.	Remote registration of applicant possible; applicant may avoid in-person encounter prior to issuance.
Two forms of original identity source documents. At least one must be a government issued picture ID.	One Federal government issued picture ID or two non-Federal IDs one of which is a picture ID.
Only designated sponsors can submit request for PIV card for an applicant.	No requirement for a sponsor for an applicant.
Identity proofing and registration process approved by head of agency.	Third party audit required for authorization to operate CA.

PIV Federation - Risks and Mitigations



	RISK	MITIGATION
PIV Card Agency B (SSP PKI)	**PKI – SSP** **BIO – SSP** **CHUID – SSP** **Accreditation Quality - ?**	**PKI – OK** **BIO – OK** **CHUID – OK** **Review Accreditation Package**
PIV Card Agency C (Legacy PKI)	**PKI – FBCA Medium-HW** **BIO – ?** **CHUID – ?** **Accreditation Quality - ?**	**PKI – OK** **BIO – Explicitly trust Signer Cert** **CHUID – Explicitly trust Signer Cert** **Review Accreditation Package**
PIV-Interoperable Card Organization D (Non-Fed SSP)	**PKI – FBCA Medium-HW** **BIO – ?** **CHUID – ?** **Accreditation not Reqd**	**PKI – OK** **BIO – Explicitly trust Signer Cert** **CHUID – Explicitly trust Signer Cert** **Require Independent Assessment**
PIV Compatible Card Organization E (Org PKI)	**PKI – ?** **BIO – ?** **CHUID – ?** **Accreditation not Reqd**	**PKI – Explicitly trust Issuer** **BIO – Explicitly trust Signer Cert** **CHUID – Explicitly trust Signer Cert** **Require Independent Assessment**

Fostering ID Federation with PIV-like Cards

- **Suggestions:**
  - **OMB Memo: Federal Relying Party can accept PIV-Interoperable Cards only from Issuers that are accredited/assessed using SP 800-79-1**
  - **Update Certificate Profiles for FBCA Medium-HW policy to indicate authority of PIV Object Signers**
    - **E.g., Common Policy supports *id-PIV-content-signing* certificate extension**
  - **Align the requirements of FIPS 201, Common Policy and FBCA Medium-HW Policy**
  - **Establish 3rd party audit regime for compliance with FIPS 201 requirements**

Summary

- **Immense opportunity to use PIV Cards (and PIV-like cards) as federated identities**

- **QUESTIONS??**