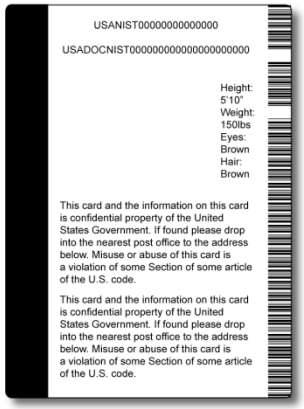


Personal Identity Verification Program

National Institute of Standards and Technology

Presidential Policy Driver

Homeland Security Presidential Directive 12

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (8/27/04)

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

General Objectives

- Common, secure, reliable identification for all government employees and contractors
- Identification to be used for access to federal resources (physical – fed. buildings, logical to federal IT resources).
- Interoperable Identification across Departments and Agencies.

FIPS 201 Specifications

Personal Identity Verification (PIV) for Government Employees and Contractors

- A smart card-based solution (PIV card)
  - Common on-card credential for logical and physical access

FIPS 201 REQUIREMENTS

PIV Electronically Stored Data

Mandatory:

- **PIN** (proves the identity of the cardholder to the card) (Something you know)
- Cardholder Unique Identifier (**CHUID**) – for contactless physical access
- **PIV Authentication Credential** (asymmetric key pair and corresponding PKI certificate) for logical access
- Two biometric fingerprints (something you are)

Optional:

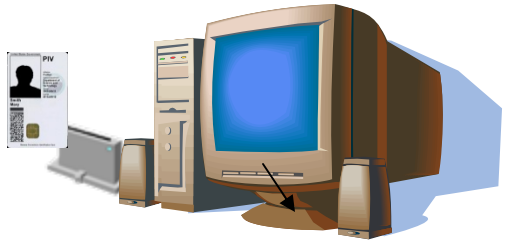
- An asymmetric key pair and corresponding certificate for **digital signatures**
- An asymmetric key pair and corresponding certificate for **key management**
- Asymmetric or symmetric **card authentication keys** for supporting additional physical access applications
- Symmetric key(s) associated with the card management system

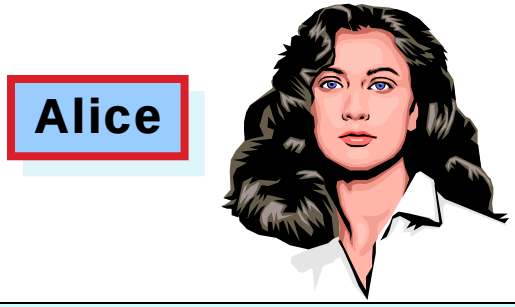
Personal Identity Verification (PIV)– Logical Access Demonstration

Demonstration Scenarios

Workstation Smart Card Logon

- Alice inserts her PIV Card into the Reader
- At the logon prompt, Alice enters her user ID and the PIN to her PIV Card***
- After successful PAM authentication, involving a challenge-response and certificate path validation, Alice is logged on the linux machine



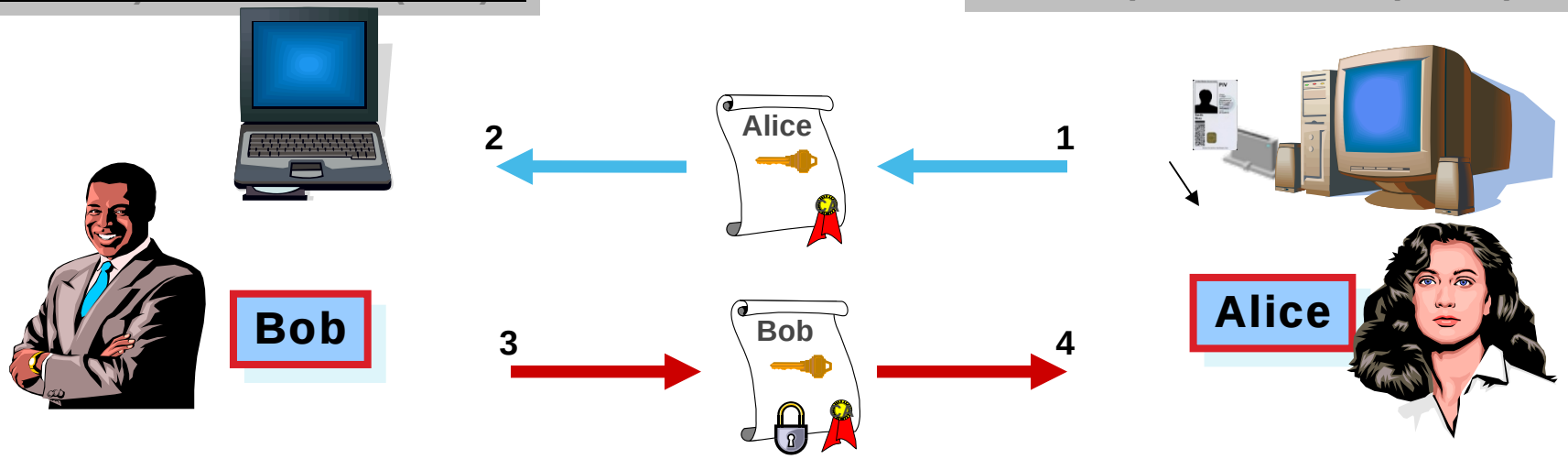


- OS - Linux (Fedora Core 5)
- Reader – SCM 331
- Software Components
  - a) PCSC-lite
  - b) CCID Reader Driver
  - c) PAM from M.U.S.C.L.E.
  - d) PIV Middleware
  - e) PKCS11 for PIV

Email Encryption and Signing

- OS – Windows XP
- Software Components
  a) Thunderbird (Win)

- OS - Linux (Fedora Core 5)
- Reader – SCM 331
- Additional Software Components
  a) Thunderbird (Linux)



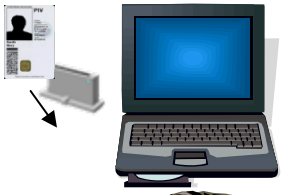
- Step 1 Alice signs an email with her on-card private digital signature key.
- Step 2 Alice sends the signature and the signature key's X.509 certificate to Bob.
- Step 3 Using the public key embedded in the received X.509 certificate, Bob verifies the signed email from Alice.
- Step 4 Bob encrypts an email for Alice using the her public key Management key (KMK) retrieved from her X.509 KMK certificate (stored locally)
- Step 5 – Alice decrypts Bob's message using her on-card private KMK.

Online Web Application Log-in

Clients Configuration
- OS - Linux (Fedora Core 5)
- Reader – SCM 331
- Additional Software Components
  - a) Firefox Browser

- OS – Windows XP
- Web Server – IIS v5.1

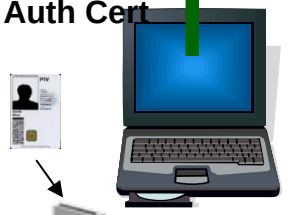
Alice's PIV Auth Cert



Alice

- Can access the application
- Has access control privileges to add new users

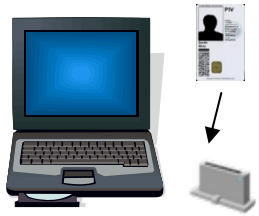
John's PIV Auth Cert



John

- Can access the application
- Cannot add new users

Mary's PIV Auth Cert



Mary

- Cannot access the application as her PIV Authentication certificate is revoked

Hildegard Ferraiolo
Computer Scientist
Hildegard.Ferraiolo@nist.gov

Elaine Newton
IDMS Program Manager
Elaine.Newton@nist.gov

http://csrc.nist.gov