Personal Identity Verification (PIV) for Federal Employees and Contractors

Tim Polk

tim.polk@nist.gov

Nov 18, 2004

HSPD-12

- *Policy for a Common Identification Standard for Federal Employees and Contractors*
- Identity credentials used to support physical and logical access control
- Include graduated criteria from least secure to most secure to ensure flexibility in selecting the appropriate level of security for applications
- Applicable to all Federal agencies
- Implement in a manner that protects citizens' privacy

NIST
National Institute of Standards and Technology

HSPD 12

- Directs the promulgation of a mandatory government-wide standard for secure and reliable forms of personal identification
  - Based on sound criteria for verifying an individual employee's identity
  - Is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation
  - Can be rapidly verified electronically
  - Is issued only by providers whose reliability has been established by an official accreditation process

NIST
National Institute of Standards and Technology

NIST Activities

- FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors
- Related Special Publications
- Proposed Validation Program
- Proposed Reference Implementation
- ….

NIST
National Institute of Standards and Technology

PIV –I

- Describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12
- Includes the personal identity proofing, registration, and issuance process
- Agencies shall meet the requirements no later than October 2005

NIST
National Institute of Standards and Technology

Identity Proofing and Registration

1	Two I-9 Identity Sources including one gov issued picture ID and fingerprints	Authentication of source documents by PIV card issuer Law enforcement check
2	Two I-9 Identity Sources including one gov issued picture ID and fingerprints	National Agency Check and Inquiries (NACI) using info from SF 85 or equiv
3	Two I-9 Identity Sources including one gov issued picture ID and fingerprints	National Agency Check and Inquiries and Credit Check (NACIC) using info from SF 85 P or equiv
4	Two I-9 Identity Sources including one gov issued picture ID and fingerprints	Limited Background Investigation (LBI) and Background Investigation (BI) using info from SF 85 P or equiv

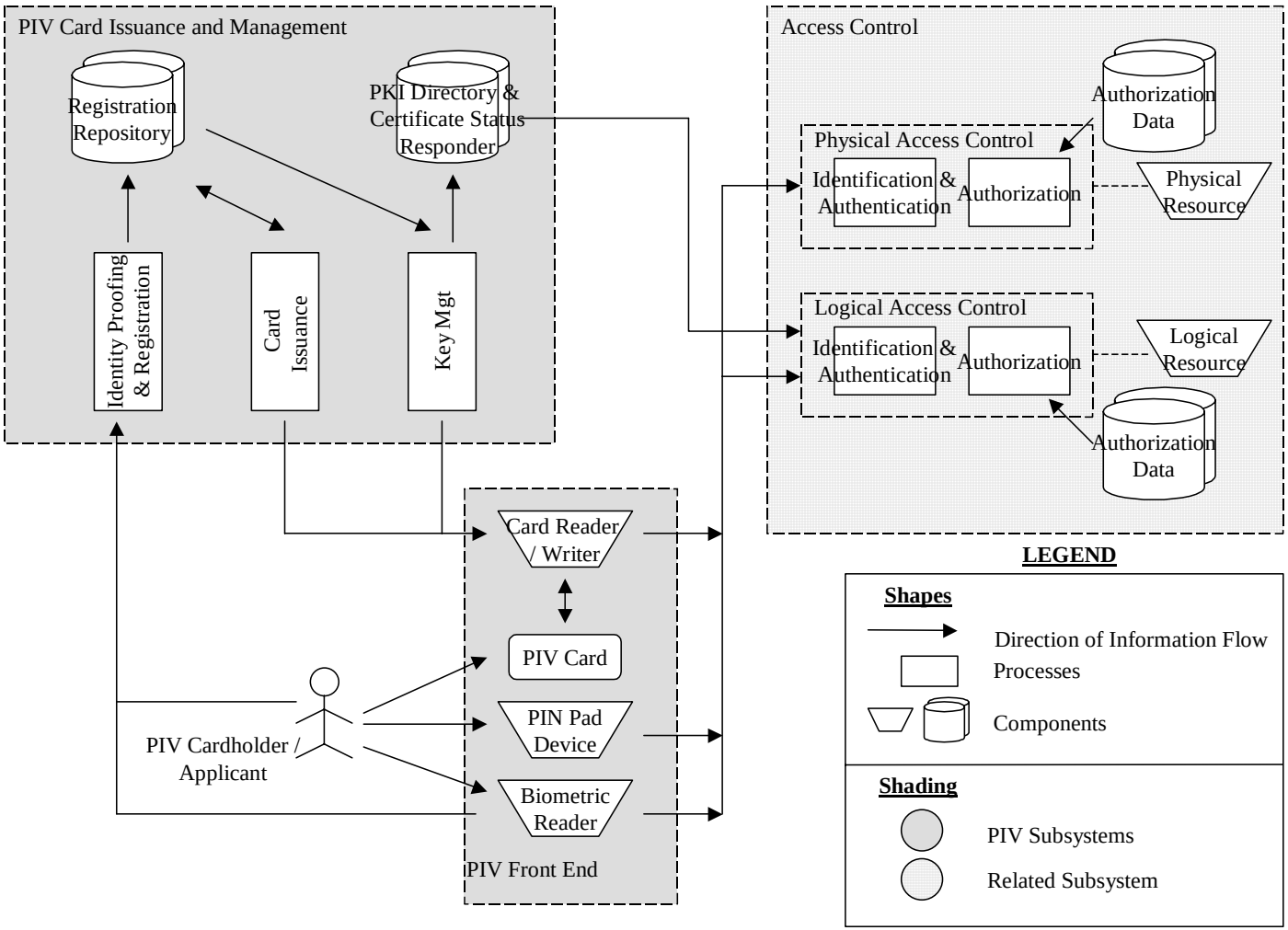
NIST
National Institute of Standards and Technology

PIV-II

- Details the technical specifications for components and processes to support interoperability of PIV cards with personal authentication, access control, and PIV card management systems across Federal Government
- OMB will issue guidance regarding agency development of transition plans to PIV-II

NIST
National Institute of Standards and Technology

PIV –II Functional Components



National Institute of Standards and Technology

PIV-II Front-End Subsystem

- PIV Card Specifications
  - Physical Credentials
    - Card Durability
    - Electronic Interfaces
    - Topology (look and feel)
  - Logical Credentials
    - Cardholder Unique Identifier (CHUID)
    - Cryptographic Specifications
    - Biometrics
- Card Reader Specifications

NIST
National Institute of Standards and Technology

Electronic Interfaces

- Requires contact and contactless interfaces
- In concert with ANSI and ISO standards activities
- API specified in SP 800-73

NIST
National Institute of Standards and Technology

Topology

- Front of Card (Mandatory)

  Photograph, Name, Employee Affiliation Employment Identifier, Text – United States Government,Expiration Date

- Back Of Card (Mandatory)

  Agency Card Serial Number, Issuer Identification Number

- Back of Military Card

  Specified in accordance with Geneva Convention format

Logical Credentials

- Mandatory Data Elements

  Personal Identification Number, Cardholder Unique Identification Object (CHUID), One asymmetric key pair and certificate, two biometric fingerprints, biometric facial image

- Optional Data Elements

  Asymmetric key pair and certificate for digital signatures, Asymmetric key pair and certificate for key management, Asymmetric or symmetric keys for additional physical access application, Symmetric keys for card management system

CHUID

- Cardholder Unique Identifier object
  - Includes the FASC-N, which is unique to each PIV card
  - Require digital signature (PACS medium)
- Mandatory file on the card accessible through either interface
- Open read

Cryptographic Specifications

- Algorithms
  - RSA
  - Elliptic Curve
- Key Management
  - Support for Common Policy
  - CRLs
  - OCSP Status Responders

NIST
National Institute of Standards and Technology

Biometrics

- Requires two fingerprint images
- Requires one facial image
- Accessible only through contact interface

NIST
National Institute of Standards and Technology

PIV-II Issuance and Management

- Card Issuance and Management Subsystem
  - New requirements for biometric enrollment and PKI certificate management
- Card Issuance and Management Process
  - New requirement to expose card status information

PIV-II Card Authentication

- PIV Card Authentication Mechanisms
- Authentication for Physical Access Control
- Authentication for Logical Access Control

NIST
National Institute of Standards and Technology

PIV-II Card Authentication (cont.)

- Visual Authentication
- CHUID Authentication
- Biometric Authentication
- Symmetric Key Cryptography
- Asymmetric Key Cryptography

PIV Validation, Certification and Accreditation

- PIV-I ID Proofing, Registration and Issuance
  - Agency Accreditation (short term)
  - Government-wide Accreditation program (long term)
- PIV-II Validation
  - Plan to develop validation program

NIST
National Institute of Standards and Technology

Summary of Agency Responsibilities

- Identity proofing for applicants
- Specific record keeping requirements
- Procurement of PIV cards & readers
- PIV Card Issuance & Management
- Accreditation of Agency PIV system
- Integration of PIV system into fabric of Agency access control capabilities

NIST
National Institute of Standards and Technology

Where are we now?

- Public comment period through Dec 25, 2004
- Completed Standard by February 25, 2005

NIST
National Institute of Standards and Technology

For more information

www.csrc.nist.gov/PIV-project

NIST
National Institute of Standards and Technology