NIST's FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors

Masaryk University in Brno
Faculty of Informatics

Jan Krhovják

Outline

- Introduction and basics of PIV
- Minimum requirements (PIV-I)
  - Personal identity proofing & Registration
  - Issuance & Maintenance
  - Security & Privacy protecting
- Detailed technical specifications (PIV-II)
  - System Overview
  - Front-End Subsystem
  - Issuance & Management Subsystem
  - Access Control Subsystem
- Conclusion

Introduction to PIV

- Physical and logical access control process
  - Access to the security-sensitive buildings, computer systems or data
  - Authentication of individual's identity => need of PIV
- 25. February 2005 – NIST released FIPS 201
- Purpose of the standard
  - Defining reliable government PIV system
  - Developing standard within the constraints of law
- Standard composed of two parts: PIV-I, PIV-II
  - PIV-II => technical interoperability

Basics of PIV (I,II)

- Four primary parties of PIV-I processes
  - Applicant – individual who needs PIV credentials
  - Sponsor – authority that consider applicants request
  - Registrar – entity responsible for identity proofing
  - Issuer – authorized identity card creator

- PIV-II adds other two parties
  - Digital signatory – signs PIV biometrics and CHUID
  - Authentication certification authority

PIV-I: Control Objectives

- Each agency's PIV implementation shall meet four control objectives for secure and reliable forms of identification
  - Based on sound criteria for verifying identity
  - Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
  - Can be rapidly authenticated electronically
  - Can be issued only by providers established by official accreditation process
- List of 10 more detailed items specifies objectives

PIV-I: Identity Proofing & Registration

- Involves applicant, sponsor, and registrar
- Sponsor
  - Signs and submits the original PIV request
- Applicant
  - In-person appearance at a registrar enrollment station
  - Presenting two forms of approved identification
    - The documents are scanned and must go trough document proofing process that authenticates them (time consuming)
  - Biometric information is also captured (PIV-II)
    - Multiple fingerprints & facial photograph
- Registrar
  - Cross-checking applicants against federal databases

PIV-I: Issuance & Maintenance

- Involves applicant and issuer
- Issuer
  - Confirm validity of PIV request received from sponsor
  - Controls creation and personalization of new PIV credential
  - Shall notify sponsor & registrar that process is done
  - Maintains requests, notices, expiration dates etc.
- Applicant (or authorized delegate)
  - In-person appearance at issuer to collect credentials
  - His identity must be verified
  - Must sign acceptance of PIV credential and the related responsibilities

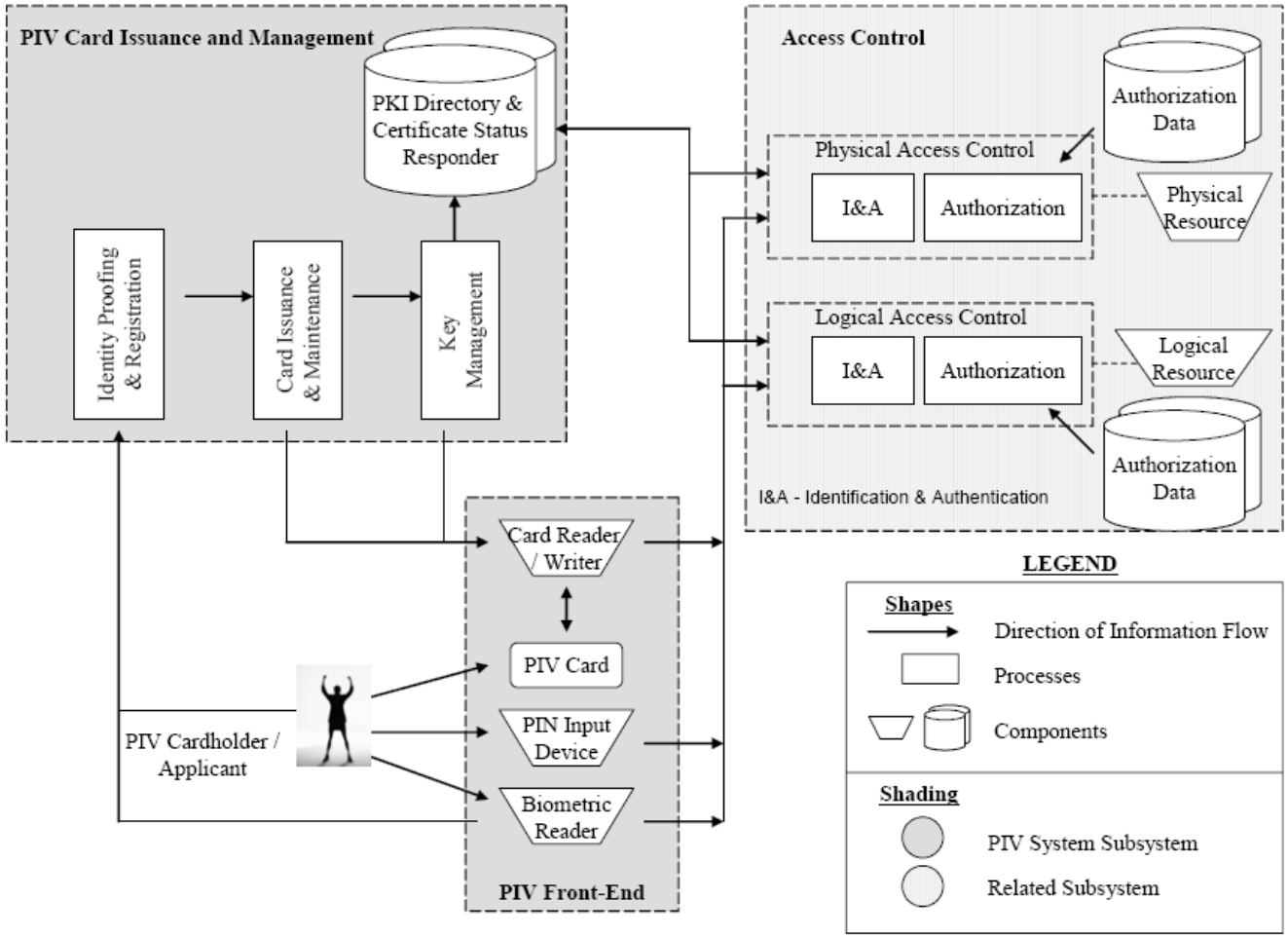
PIV-I: Security and Privacy

- PIV identity proofing, registration and issuance process adhere to the principle of separation
  - No single individual can issue PIV credential
- PIV system must protecting privacy
  - Special role of official for privacy
    - Overseas the privacy-related matters
    - Responsible for implementing privacy requirements
  - Entire document should be published and maintained
    - Types of collected information & purpose of collection
      - Focused on personal information in identifiable form
    - How information will be protected
    - What information may be disclosed to whom
    - Complete set of uses of credentials and related information

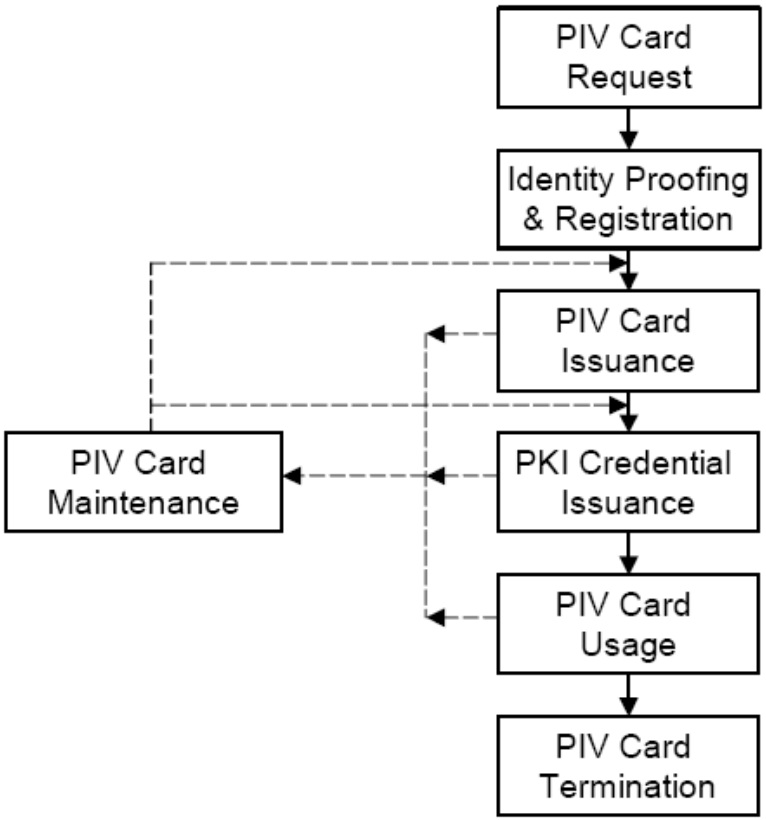
PIV-II: System Overview

- Basic functional components
  - Front-end subsystem
    - PIV card, cards and biometric readers, PIN input device
    - Cardholder interacts with these components
  - Card issuance and management subsystem
    - Components responsible for identity proofing and registration, card and key issuance, management, various repositories and services (e.g. PKI, certificate status server)
  - Access control subsystem
    - Access control to physical and logical resources
    - Technical specification is not part of this standard
      - Various mechanisms are discussed
- Notional model + data flows => next slide

PIV-II:
System Overview – picture



PIV-II:
PIV Card Life Cycle



– initiation request

– verifying claimed identity

– physical (visual surface) and logical (contents) personalization

– generating and loading logical credentials onto the card

– performing cardholder authentication for access

– destroying the card and all data and keys

PIV-II:
Front-End Subsystem 1

- Physical PIV card topology
  - Printed material
    - Shall not rub off or interfere with chip area
  - Tamper proofing and resistance (at least one feature)
    - Optical varying structures and inks
    - Laser etching and engraving
    - Watermarking, holographic images
  - Physical characteristics and durability
  - Visual topology (visual and printed information)
    - Mandatory/optional items on the front/back of the card
  - Logical identity credentials (details of composition)
  - PIV card activation (PIN based)
    - By cardholder or card management system

PIV-II:
Front-End Subsystem 2

- Cardholder unique identifier (CHUID)
  - Federal Agency Smart Credential Number
  - Expiration date
- Biometric data specifications
  - Full set of fingerprints – two compactly stored on card
    - Accessible only over the contact interface after entry of PIN
  - Facial image – not required to be stored on the card
  - Other characteristics (e.g. pixel depth and density)
- Card reader specifications
  - Contains also requirements for PIN input devices
    - For physical access – integration within the reader
    - For logical access – may be used keyboard

PIV-II:
Front-End Subsystem 3

- Cryptographic specifications
  - PIV card must store minimally one key pair
    - And support correspondent cryptosystem
  - PIV card shall implement
    - RSA and ECC key pair generation
    - RSA and ECC cryptographic operations
    - Importation and storage of X.509 certificates
  - Support of digital signature keys => cryptographic hash algorithm is not required (performed off-card)
  - Operations using PIV keys shall be performed on-card
  - PIV keys shall be generated within FIPS 140-2 validated HSM (overall validation at Level 2 or above)
    - PIV card shall provide Level 3 physical security!

PIV-II: Issuance & Management Subsystem

- Extends (and describes in detail) most of PIV-I processes
  - Control objectives
    - Interoperability requirements
  - Identity proofing and registration
    - Biometrics (fingerprints and facial image)
  - Issuance and maintenance requirements
    - PIV card: issuance, maintenance, renewal, reissuance, PIN reset, termination
  - Key management requirements
    - Architecture, PKI certificate (X.509 certificate/CRL contents), migration from legacy PKIs, PKI repository
  - Privacy requirements (equal to PIV-I)

PIV-II:
Access Control Subsystem

- Three identity authentications assurance levels
  - Some, high, or very high confidence
  - Depending on used type of PIV credentials
- Technical specification is not part of this standard
- Basic types of authentication mechanisms
  - PIV visual credentials (photograph, name, date …)
  - PIV CHUID (contains numerous elements)
  - PIV biometric (using attended or unattended)
  - PIV asymmetric cryptography
- Selection of mechanism(s) is dependent also on presence/lack of (contact/contactless) card reader

Conclusion

- Access control process needs authentication of individual's identity => need of PIV
  - NIST released FIPS 201
- PIV system described in two parts
  - PIV-I: Minimum requirements
    - Describes basic processes
  - PIV-II: Detailed technical specifications
    - Supports technical interoperability
- Primary component of system is PIV card
  - Used for authentication to various resources