FIPS 201
Personal Identity Verification For Federal Employees and Contractors

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

General Objectives

Common reliable identification verification for Government employees and contractors

- Reliable Identification Verification
- Government-wide
    - Interoperability
    - Basis for reciprocity

Personal Identity Verification Requirements

HSPD: Policy for a Common Identification Standard

- Departments and agencies shall have a program in place to ensure conformance within 4 months after issuance of FIPS
- Departments and agencies to identify applications important to security that would benefit from conformance to the standard within 6 months after issuance
- Compliance with the Standard is required in applicable Federal applications within 8 months following issuance

Community Concerns

- Agency investment in legacy systems
- Resource and time required to implement changes to existing systems
- Differences among Agencies regarding confidentiality and privacy requirements for identity information
- Differences among Agencies regarding which mechanisms are most effective with respect to:
    - Physical and logical security
    - Performance
    - Business issues

Phased-Implementation Approach

Two Parts to PIV Standard

- **Part I – Common Identification and Security Requirements**
  - HSPD #12 Control Objectives
    Examples: Identification shall be issued based on strong Government-wide criteria for verifying an individual employee's identity
    The identification shall be capable of being rapidly authenticated electronically Government-wide
  - Identity Proofing Requirements (revised from October draft)
  - Effective October 2005

- **Part II – Common Interoperability Requirements**
  - Specifications
  - Most Elements (revised) of October Preliminary Draft
  - No set deadline for implementation in PIV standard

- **Migration Timeframe (i.e., Phase I to II)**
  - IAW HSPD #12, Implementation Plans for OMB before July 2005
  - OMB approves agency plans and/or develops schedule directive

Part I

Personal Identity Verification Standard for Federal Government Employees and Contractors

- Promulgate Federal Information Processing Standard within 6 months

- Establish requirements for:

  - Identity Token (ID Card) Application by Person
  - Identity Source Document Request by Organization
  - Identity Registration and ID Card Issuance by Issuer
  - Access Control (Determined by resource owner)

FIPS 201 Part II

- Integrated circuit card-based identity token (i.e., ID Card).
- Standard at framework level with minimum mandatory implementation for interoperability specified.
- Basis for specification of issuer accreditation and host system validation requirements .
- Basis for specification of ID card, data base infrastructure, protocols, and interfaces to card.
- Card/token issuance based on I-9 Identity Source Documents, request by government organization, and approval by authorized Federal official.
- Biometric and cryptographic mechanisms.
- Supporting ICC Specifications in Special Publication 800-73

FIPS 201 Schedule

Delivery of Detailed Strawman Outline Components -	**August 31, 2004**
Finalize Technical Interagency Working Group Membership (TIWG) -	**September 2, 2004**
Announce First TIWG Meeting -	**September 2, 2004**
Announce Government Workshop -	**September 3, 2004**
Submit Public Workshop *Federal Register* Announcement -	**September 3, 2004**
Integration Meeting for Concept Draft Components -	**September 3, 2004**
Complete Strawman Content Proposal -	**September 7, 2004**
Distribute Concept to FICC IAB/TIWG Members -	**September 8, 2004**
Concept Comments to NIST for Review at First TIWG Meeting* -	**September 14, 2004**
First Meeting of TIWG -	**September 15, 2004**
Collect Initial Draft Component Submissions -	**September 21, 2004**
Completion of Working Group Comment Period -	**September 22, 2004**
Government-only Workshop Day -	**October 6, 2004**
Public Workshop Day -	**October 7, 2004**
Completion of Government Workshop Comment Period -	**October 12, 2004**
Assemble Preliminary Draft -	**October 19, 2004**
Completion of Public Workshop Comment Period -	**October 21, 2004**
Decision on Changes to Draft and Writing Assignments -	**October 22, 2004**
Completion of Public Draft of Standard -	**November 8, 2004**
Completion of Comment Period for Public Draft -	**December 23, 2004**
Completion of Revision of Standard -	**January 13, 2005**
Completion of Responses to Comments on Public Draft -	**January 14, 2005**
Delivery of FIPS Submission Package by NIST to DoC -	**February 4, 2005**
DoC Approval -	**February 25, 2005**

Items on critical path are in boldface.

*** External actions**

AGENDA FOR NIST INDUSTRY WORKSHOP

Time	Topic/Event	Speaker
8:45 -- 9:00 am	Welcome and Workshop Objectives	Tim Grance, NIST
9:00 -- 9:30 am	Presentation on Special Publication 800-73 (SP 800-73), Integrated Circuit Card for Personal Identity Verification	Jim Dray, NIST
9:30 -- 10:15 am	Discussion and Comments on SP 800-73	Jim Dray, NIST
10:15 -- 10:30 am	Break	
10:30 -- 11:15 am	Open Discussion and Comments on Registration and Issuance	Donna Dodson, NIST
11:15 -- 12:00	Open Discussion of Biometrics	Ramaswami Chandramouli, NIST
12:00 -- 12:45 pm	Lunch	
12:45 -- 1:30 pm	Open Discussion Cryptography	Tim Polk, NIST
1:30 -- 2:00 pm	Other Comments and Closing Remarks	W. Curtis Barker, NIST

Contact Information

William C. Barker
Program Manager
301-975-8443
800-437-4385 X8443
wbarker@nist.gov

Web Site:

http://csrc.nist.gov/piv-project/

Back-Up

Basis for Requirements

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors

Personal Identity Verification Threats

General Threat: Unauthorized access to physical facilities or logical assets under the protection umbrella of the PIV System and in which a PIV card is employed in access control processes.

- Improper issuance of valid card to malicious holder

- Counterfeiting of cards
  - Intercept or probing to access stored information
  - Successful cryptanalytic attacks against stored protected information

- Use of stolen or borrowed card to gain access
  - Intercept/technical surveillance to capture PIN(s)

- Use of card issued for access to lower sensitivity/criticality assets to achieve access to more sensitive/critical assets

Personal Identity Verification Requirements

HSPD-12: Policy for a Common Identification Standard

Secure and reliable forms of personal identification:

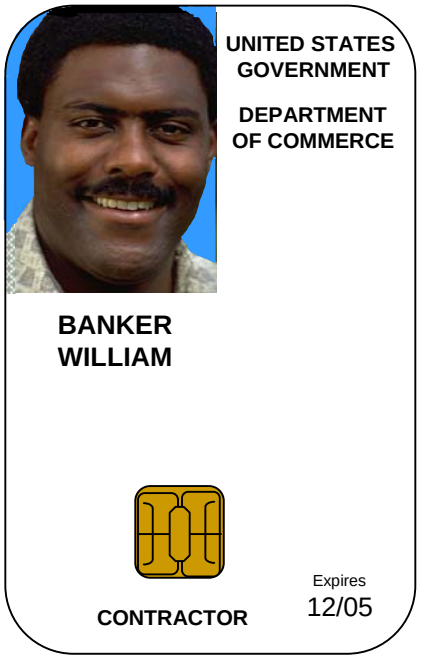
- Based on sound criteria to verify an individual employee's identity
- Is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
- Personal identity can be rapidly verified electronically
- Identity tokens issued only by providers whose reliability has been established by an official accreditation process

Personal Identity Verification Requirements

- Applicable to all government organizations and contractors
- To be used to grant access to Federally-controlled facilities and logical access to Federally-controlled information systems
- Graduated criteria from least secure to most secure to ensure flexibility in selecting the appropriate security level for each application
- Not applicable to identification associated with national security systems
- To be implemented in a manner that protects citizens' privacy

FIPS Development Process

- Public Announcement on Intent/Scope
  - HSPD-12: Policy for Common Identification Standard for Federal Employees/Contractors
  - Federal Register Notice #1: Scope/Workshop
- Draft Standard: Applicability, Foundation, Scope, Specifications, Implementations
- Government and Public Comments Solicited
  - TIWG Review and Federal Register Notice #2
- Revision of Standard: From Comments
- Publication/Promulgation of Standard
  - Federal Register Notice #3 announcing Standard



Phase I (Continued)

Mandatory Card Characteristics

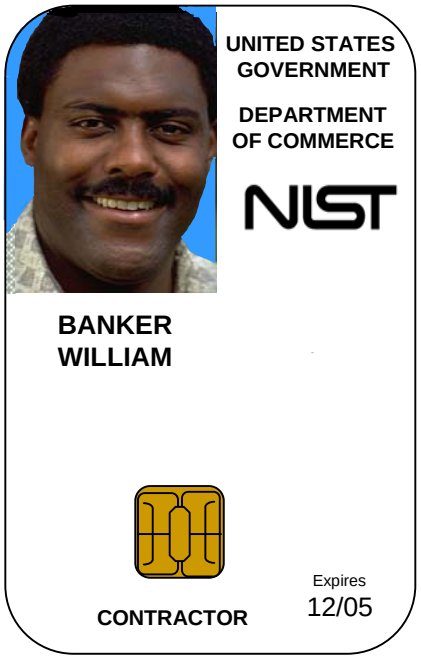
Basic:

- ISO/IEC 7810 Physical Characteristics
- ISO/IEC 7816 Contact Chip
- ISO/IEC 14443 (Parts 1-4 Draft) Proximity Card
- ISO/IEC 24727 (Future) Interoperability Specification [NIST IR 6887]

Mandatory Features Specification*:

- Cryptographic (2048 Bit RSA, 256 Bit AES, SHA 256)
- Fingerprint Image Specification
- Photographic Image Specification

* Illustrative examples only



Phase I (Continued)

Mandatory Card Content

Electronic Content Digitally Signed By Issuer:

- Digital Photograph (1 or 2)
- Digital Fingerprint Images (Left and right index)
- PKI Certificates (One per access level)
- User Identity (Card number?)
- Issuer Identity

Logic Elements:

- Cryptographic Digital Signature
- Cryptographic Challenge/Response?
- Encryption/Decryption
- Key Variable Processing (PIN-based notarization?)
- Biometric Data Processing

Phase I (Continued)

Optional Card Content

Electronic Content Digitally Signed By Issuer:

- Employee/Contractor Status
- Second Digital Photograph
- Ten Finger Digital Fingerprint Image
- Card Holder's Signature (Ties card to holder)
- Emergency Responder Designation
- Date of Issue
- Height
- Hair Color
- Eye Color