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 government employees and contractors
- Visual and electronic identity verification
- Government-wide
  - Technical interoperability
  - Common basis for reciprocity

Satisfying HSPD-12 Requirements

- Enhance security
- Increase government efficiency
- Reduce identity fraud
- Protect personal privacy
- Eliminate variations in quality and security of forms of personal identification

Current PIV Program Challenges

- Tight schedule mandated by EOP
- Unfunded nature of mandate
- Transition issues (e.g., challenges faced by agencies with installed bases when making changes to those bases or to existing development plans)
- Interoperability consequences from reluctance to accept precisely defined card interface (aka hard card edge)
- Biometric interoperability dependence on common accuracy standard
- Weigand interface dependency on physical access control environment
- Imprecise nature of current contactless technical standards

Current PIV Program Challenges (Continued)

- Wide variety of logical access control application interfaces
- Varying levels of technical understanding and infrastructure among agencies
- Foreign ownership or controlling interest in smart card vendor (deemed export issues)
- Conformance test infrastructure support requirements (admin & technical)
- Need for multiple NPIVP-certified products in very near-term
- Privacy concerns (e.g., identity databases, contactless interfaces)
- Need for stable standards vs requirement to revisit FIPS 201 in FY 2006

Federal Information Processing Standards (FIPS)

- Mandatory
- FISMA removed the waiver option
- In recent history, only two waivers had ever officially been requested and approved
- Technology advancements have contributed to the removal of waivers as more product developers are implementing the standards, increasing availability of compliant products especially in the area of encryption

Special Publications (800 Series)

- Security and interoperability publications
- Used to support and complement FIPS
- Prior to 2005, officially viewed as guidance
- FISMA reporting instructions for FY2005 called for agency compliance with NIST standards **and** guidance

HSPD #12
Key PIV Documents

- **HSPD-12**, Policy for a Common Identification Standard for Federal Employees and Contractors
- **OMB M-05-24**, Implementation of HSPD 12 - Policy for a Common Identification Standard for Federal Employees and Contractors
- **FIPS 201**, Personal Identity Verification for Federal Employees and Contractors
- **SP 800-73**, Interfaces for Personal Identity Verification
- **SP 800-76**, Biometric Data Specification for Personal Identity Verification
- **SP 800-78**, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- **SP 800-79**, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
- **SP 800-85**, PIV Middleware and PIV Card Application Conformance Test Guidelines (Revision to permit transitional and end-point issuance system conformance certification)
- **NISTIR 7284**, Personal Identity Verification Card Management Report

Functional Components

- PIV Front-End Subsystem — PIV Card, card and biometric readers, and personal identification number (PIN) input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.
- PIV Card Issuance and Management Subsystem — the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.
- Access Control Subsystem — the physical and logical access control systems, the protected resources, and the authorization data.

Federal Information Processing Standard 201
Personal Identity Verification for Federal Employees and Contractors

- **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
  - Effective October 2005
- **Part II – Common Interoperability Requirements**
  - Specifications
  - Most provisions effective October 27, 2006
  - Implementation Timeframes IAW Agency Implementation Plans and OMB Memorandum M-05-24 of August 5, 2005

FIPS 201: Personal Identity Verification (PIV) Issued February 25, 2005

- Mandatory Prerequisites for Personal Identity Verification (PIV) Card Issuance
- Mandatory and Optional PIV Card Visual Data
- Mandatory and Optional PIV Card Electromagnetic Elements
- Mandatory and Optional PIV Electronically Stored Data
- Minimal Card Information Available for “Free Read”
- Large population – affects every Federal government employee and eligible contractors (~ 10M+)

PIV Card Visual Data

Mandatory

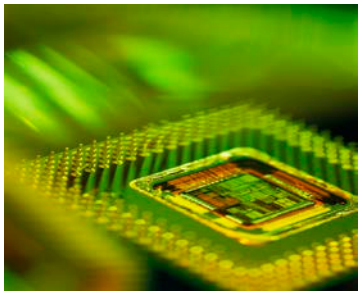
- Name
- Employee Affiliation
- Card Expiration Date
- Card Serial Number (Unique to Issuer)
- Issuer Identification

Optional

- Card Holder's Written Signature
- Pay Grade
- Rank
- Agency Name and/or Department
- Agency Seal
- Issue Date
- Information for Returning Lost Card
- Color codes
- Federal Emergency Official Designation

PIV Card Requirements

- Mandatory
  - Integrated Circuit to Store/Process Data
- Optional
  - Magnetic Stripe
  - PDF 417 Bar Code
  - Linear 3 of 9 Bar Code
- Interfaces:
  - Contact (ISO/IEC 7816)
  - Contactless (ISO/IEC 14443)



PIV Electronically Stored Data

Mandatory:

- PIN (used to prove the identity of the cardholder to the card)
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Two biometric fingerprints

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

FIPS 201 REQUIREMENTS

Authentication Mechanisms

Three Identity Authentication Assurance levels

- Authentication using PIV Visual Credentials
- Authentication using the PIV CHUID
- Authentication using PIV Biometric
- Authentication using PIV asymmetric Cryptography (PKI)

PIV Card Management

FIPS201 specifies:

- PIV Card Issuance
- PIV Card Maintenance
- PIV Card Renewal
- Card re-issuance
- Card PIN reset
- Card termination

Interfaces for Personal Identity Verification

SP 800-73 specifies:

- PIV Data Model (Mandatory and Optional Data Elements)
- Optional Transition Card Interfaces (APIs, Object Naming Structure and Mapping Mechanism, Data Formats and Structures, Card Commands)
- Mandatory End-Point Card Interfaces Card Re-issuance
  - Data Objects
  - Data Types
  - Client Application Programming Interfaces
  - PIV Card Application Card Command Interface

Biometric Data Specification for Personal Identity Verification

SP 800-76 specifies:

- Template specification is the INCITS 378:2004 standard.
- 800-76 template specification is an application profile of INCITS 378
- 800-76 template specification restricts the options of INCITS 378 :
  - No extended data
  - No proprietary data
  - Up to three views for each finger.
  - Restriction of minutia type (bifurcation, ridge ending)
- Face specification is INCITS 385 for image acquisition and storage
- CBEFF PIV Format is specified with definitive data types for its elements and the FASC-N included per 800-73

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

SP 800-78 specifies:

- Mandatory PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Optional Keys
  - Asymmetric key pair and corresponding certificate for digital signatures
  - Asymmetric key pair and corresponding certificate for key management
  - Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Cryptographic Algorithms and Key Sizes
- Authentication Information Stored on the PIV Card

Special Publication 800-79

Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

SP 800-79 specifies:

- Certification & Accreditation Fundamentals
  - C&A Phases (Initiation, Certification, Accreditation, Monitoring)
  - Accreditation Decisions (Authorization, Interim Authorization, Denial)
  - Accreditation Package and Supporting Documentation
- Attributes of PIV Card Issuers (PCI) and Assessment Methods
- PCI Functions and Operations (Plan, Document, Implement, Operate)
- PIV Services and Operations
  - Applicant ID Proofing and Registration
  - PIV Card Issuance
  - PIV Card Life Cycle Management

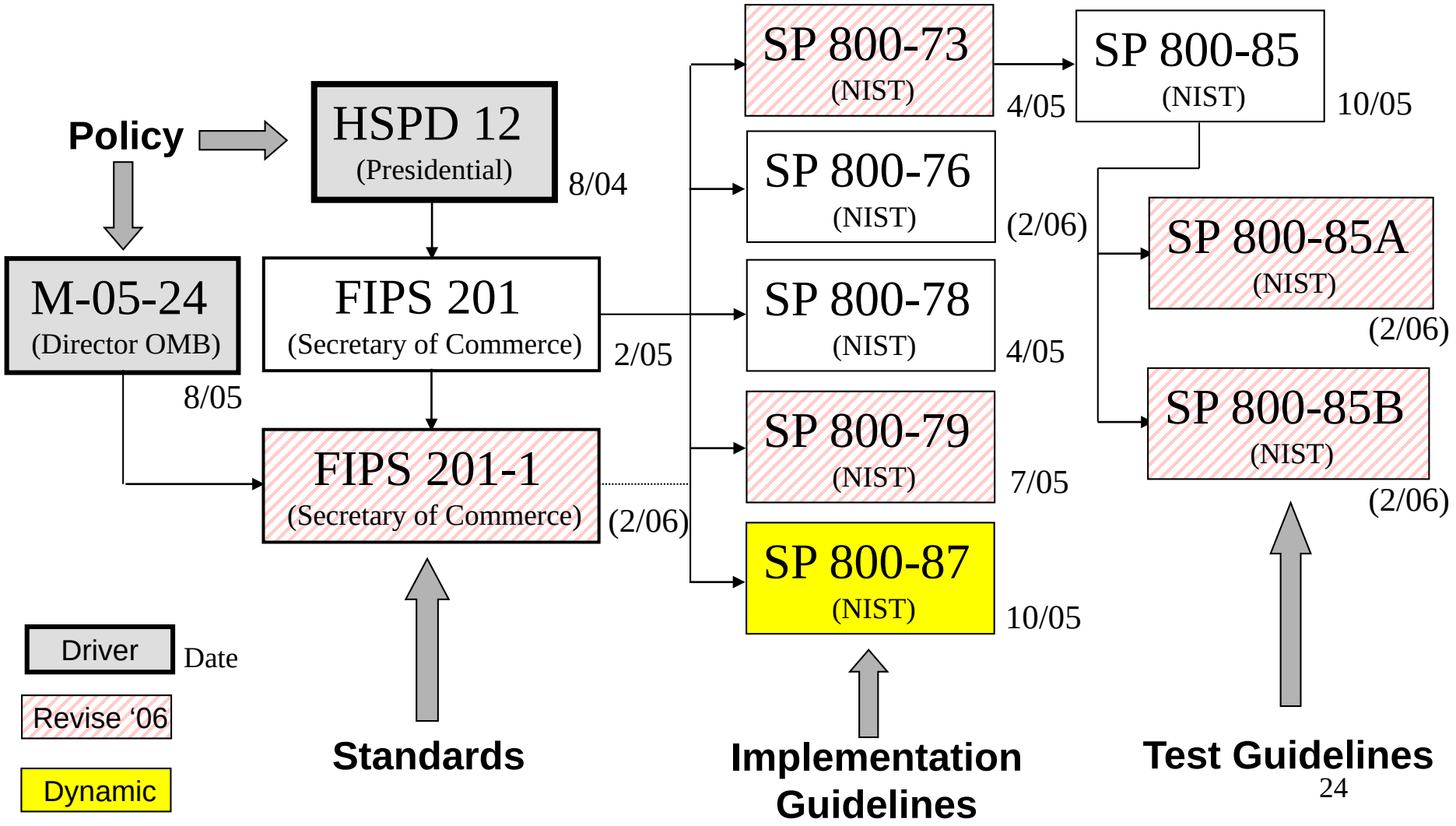
Additional PIV Tools and Guidelines

- SP 800-73 Reference Implementation (Mandatory SP 800-73 elements)
- SP 800-87 Codes for the Identification of Federal and Federally-Assisted Organizations (Replaces Withdrawn FIPS 95-2)
- NPIVP Laboratory Designation for PIV Conformance Testing
- PIV Website http://csrc.nist.gov

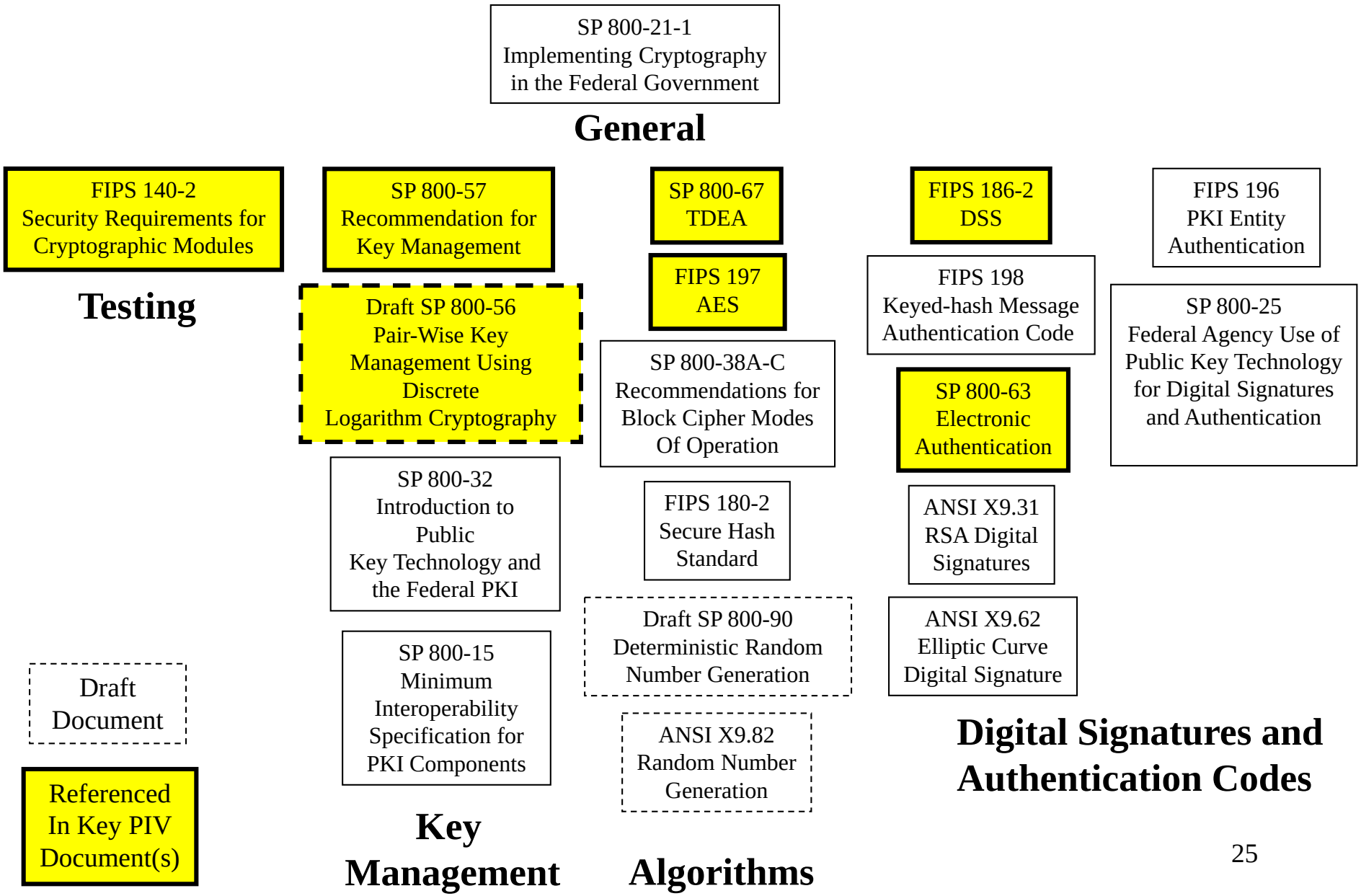
SP 800-85 PIV Middleware and PIV Card Application Conformance Test Guidelines

- Test Plan, Test Set-up, and Test System Configuration
- Test Suite Elements (Middleware Tests, Card Command Interface Tests and Data Object Representation Tests)
- Derived Test Requirements
- Test Assertions
- Test and Compliance Documentation
- Acceptance Criteria
- Test and Compliance Process
- Being Revised to Separate Card/Middleware Interface and Data Object Representation Volumes (Phase II)

HSPD #12
PIV Document Relationships



Cryptographic Standards and Guidelines



C&A Standards and Guidelines

SP 800-37
Guide for the Security Certification and Accreditation of Federal Information Systems

FIPS 199
Standards for Security Categorization of Federal Information and Federal Information Systems

FIPS 200
Minimum Security Requirements for Federal Information and Information Systems

SP 800-18 Rev. 1
Guide for Developing Security Plans for Federal Information Systems

Security Planning

SP 800-26
Security Self- Assessment Guide for Information Technology Systems

SP 800-59
Guideline for Identifying an Information System as a National Security System

SP 800-53
Recommended Security Controls for Federal Information Systems

SP 800-26 Rev.1
Guide for Information System Security Assessments and System Reporting Form

SP 800-60
Guide for Mapping Types of Information and Information Systems to Security Categories

SP 800-53A
Guide for Assessing the Security Controls in Federal Information Systems

Security Assessment, Certification & Accreditation

SP 800-30
Risk Management Guide for Information Technology Systems

Security Categorization

Security Controls

Draft Document

Referenced In Key PIV Document(s)

Referenced and Being Revised

Conformance Testing
NIST PIV Program (NPIVP)

- Atlan Laboratories, McLean, VA
- atsec information security corporation, Austin, TX
- BKP Security Labs, Santa Clara, CA USA
- BT Cryptographic Module Testing, Fleet, Hampshire,
- CEAL: a CygnaCom Solutions, McLean, VA
- COACT Inc. CAFÉ Laboratory, Columbia, MD
- DOMUS IT Security Laboratory, Ontario, Canada
- EWA – Canada IT Security Evaluation & Test, Ottawa, Ontario, Canada
- ICSA Labs, a division of Cybertrust, Inc., Mechanicsburg, PA
- InfoGard Laboratories, Inc., San Luis Obispo, CA
- LogicaCMG FIPS Laboratory, Leatherhead, Surrey UK

CRADA: PIV Demonstration

Card Issuance & Management	Front-End Components	Access Control Components	System Integrators
Datacard	Bamboo Technologies	ADT	BearingPoint
Entrust	BQT Technologies	BridgePoint Systems	Centech Group
Fargo Electronics	G&D	Cogent Systems	Lockheed Martin
Precise Biometrics	Gemplus	Electrosoft	Northrop Grumman
Probaris Technologies	Lowry Computer	HID	Oracle
RSA Security	Middleware Associates	Hirsch Electronics	SAIC
Ultra Electronics	Oberthur Card Systems	Lenel Systems	SETECS
	Omnikey	Novell	Viisage Technologies
	SCM Microsystems	Quintron Systems	XTec
	Ultra Electronics	Secure Network Systems	
	Veridt	Sensormatic	

Thank you!

William C. Barker
National Institute of Standards and Technology
301-975-8443
wbarker@nist.gov
http://csrc@nist.gov