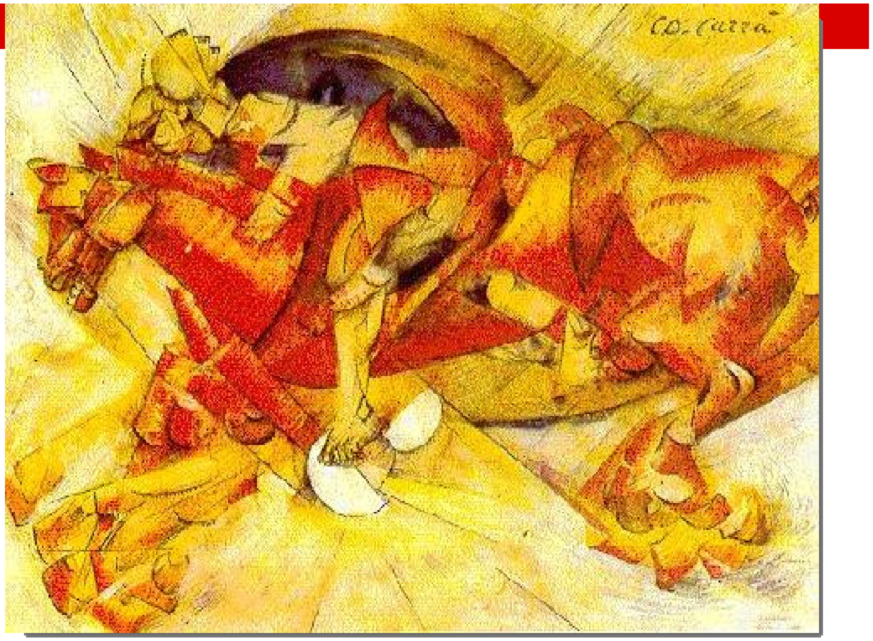
the information security provider



How Does Your Company's Identity Security Compare with that of the Federal Government?

Auston Holt

public

Auston Holt 2010-04-15 v1.3 ©atsec information security, 2010

Auston Holt

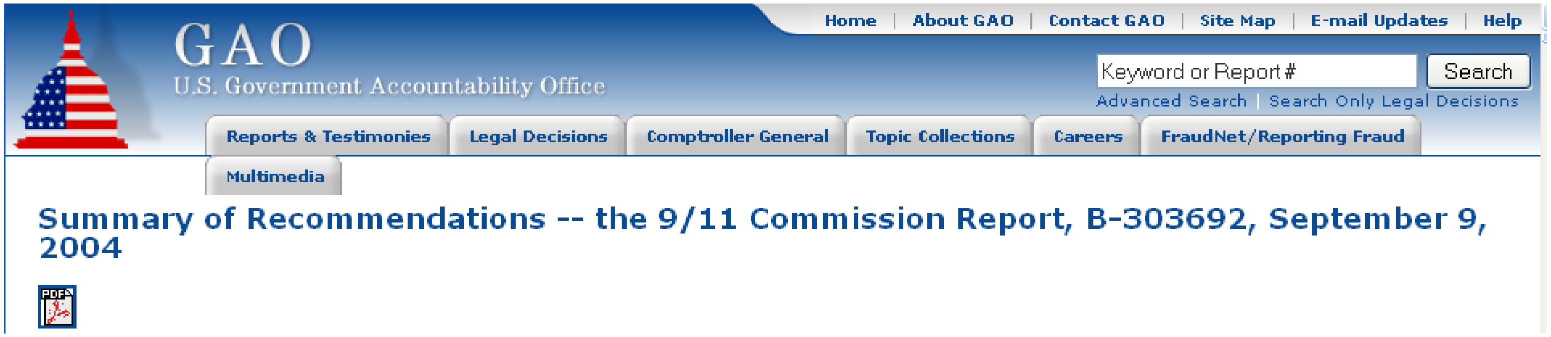
Security consultant, atsec information security corporation

- Deputy Chief Information Security Officer
- Laboratory accreditation lead
  - NPIVP Lab
  - GSA FIPS 201 Evaluation Program Lab
- Common Criteria
  - evaluator
  - consultant
- Bachelor of Arts in Computer Science, University of Texas at Austin
- Certifications acheived: CISSP, SSCP

September 11, 2001

September 11, 2001

- The 9/11 Commission Report
- “Recommendation: Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. [...]”(Page 390)

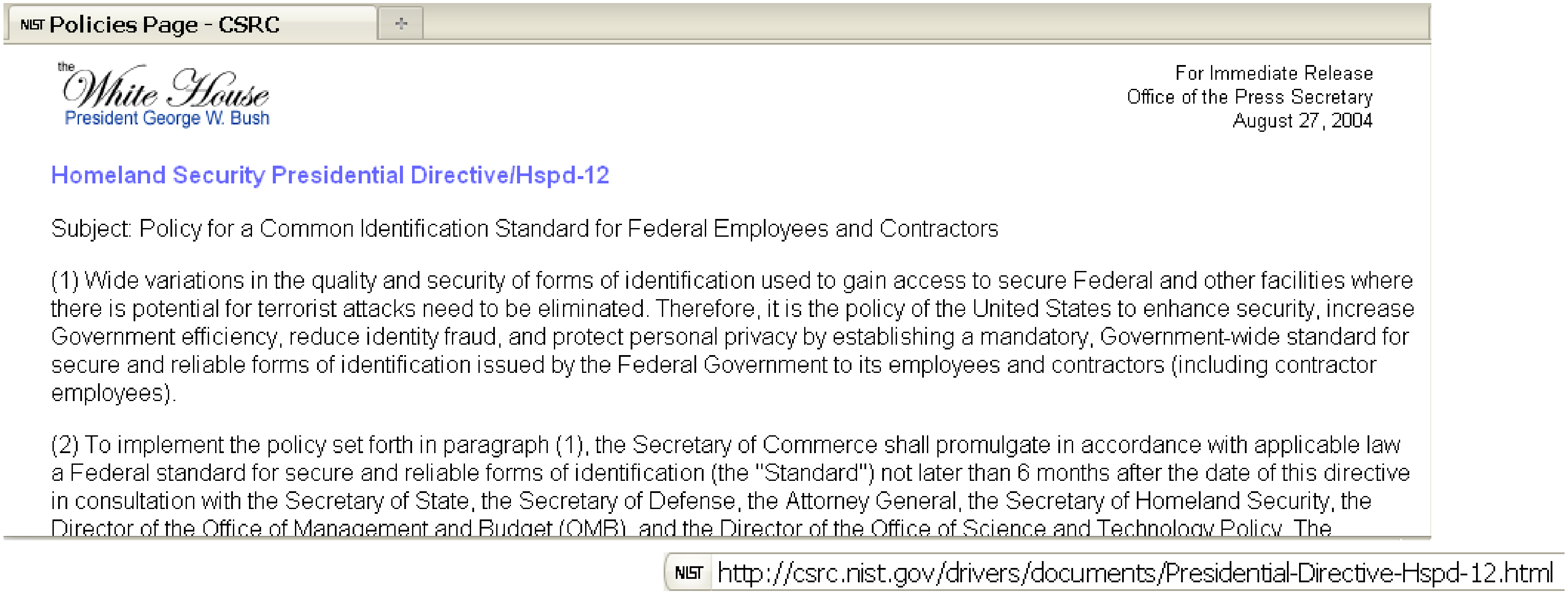

Home | About GAO | Contact GAO | Site Map | E-mail Updates | Help
GAO
U.S. Government Accountability Office
Keyword or Report #
Search
Advanced Search | Search Only Legal Decisions
Reports & Testimonies
Legal Decisions
Comptroller General
Topic Collections
Careers
FraudNet/Reporting Fraud
Multimedia
PDF

Summary of Recommendations -- the 9/11 Commission Report, B-303692, September 9, 2004

http://www.gao.gov/decisions/other/303692.htm

HSPD-12

Homeland Security Presidential Directive 12



the White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The

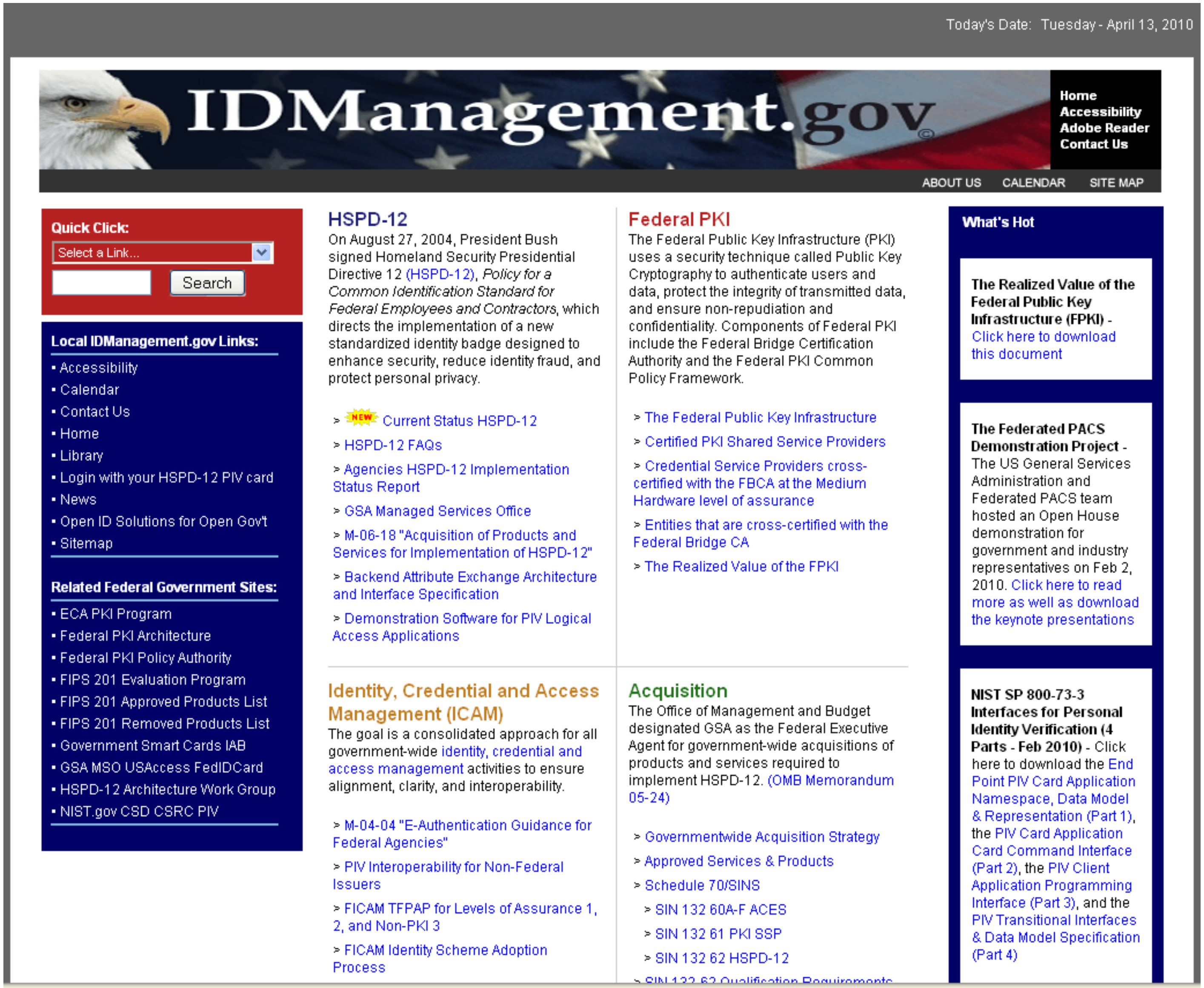
NIST http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html

HSPD-12

Homeland Security Presidential Directive 12

- August 27, 2004 (George Bush)
- "(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. […]"
- "(3)Secure and reliable forms of identification" for purposes of this directive means identification that
  - (a) is issued based on sound criteria for verifying an individual employee's identity;
  - (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
  - (c) can be rapidly authenticated electronically; and
  - (d) is issued only by providers whose reliability has been established by an official accreditation process. "

DoD, DOJ, NASA, DHS, OMB, GSA, SEC, DOT, EPA…



Today's Date: Tuesday - April 13, 2010

Quick Click:

Select a Link... [Search]

Local IDManagement.gov Links:

- Accessibility
- Calendar
- Contact Us
- Home
- Library
- Login with your HSPD-12 PIV card
- News
- Open ID Solutions for Open Gov't
- Sitemap

Related Federal Government Sites:

- ECA PKI Program
- Federal PKI Architecture
- Federal PKI Policy Authority
- FIPS 201 Evaluation Program
- FIPS 201 Approved Products List
- FIPS 201 Removed Products List
- Government Smart Cards IAB
- GSA MSO USAccess FedIDCard
- HSPD-12 Architecture Work Group
- NIST.gov CSD CSRC PIV

HSPD-12

On August 27, 2004, President Bush signed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, which directs the implementation of a new standardized identity badge designed to enhance security, reduce identity fraud, and protect personal privacy.

> NEW Current Status HSPD-12
> HSPD-12 FAQs
> Agencies HSPD-12 Implementation Status Report
> GSA Managed Services Office
> M-06-18 "Acquisition of Products and Services for Implementation of HSPD-12"
> Backend Attribute Exchange Architecture and Interface Specification
> Demonstration Software for PIV Logical Access Applications

Federal PKI

The Federal Public Key Infrastructure (PKI) uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure non-repudiation and confidentiality. Components of Federal PKI include the Federal Bridge Certification Authority and the Federal PKI Common Policy Framework.

> The Federal Public Key Infrastructure
> Certified PKI Shared Service Providers
> Credential Service Providers cross-certified with the FBCA at the Medium Hardware level of assurance
> Entities that are cross-certified with the Federal Bridge CA
> The Realized Value of the FPKI

Identity, Credential and Access Management (ICAM)

The goal is a consolidated approach for all government-wide identity, credential and access management activities to ensure alignment, clarity, and interoperability.

> M-04-04 "E-Authentication Guidance for Federal Agencies"
> PIV Interoperability for Non-Federal Issuers
> FICAM TFPAP for Levels of Assurance 1, 2, and Non-PKI 3
> FICAM Identity Scheme Adoption Process

Acquisition

The Office of Management and Budget designated GSA as the Federal Executive Agent for government-wide acquisitions of products and services required to implement HSPD-12. (OMB Memorandum 05-24)

> Governmentwide Acquisition Strategy
> Approved Services & Products
> Schedule 70/SINS
> SIN 132 60A-F ACES
> SIN 132 61 PKI SSP
> SIN 132 62 HSPD-12
> SIN 132 62 Qualification Requirements

What's Hot

The Realized Value of the Federal Public Key Infrastructure (FPKI) - Click here to download this document

The Federated PACS Demonstration Project - The US General Services Administration and Federated PACS team hosted an Open House demonstration for government and industry representatives on Feb 2, 2010. Click here to read more as well as download the keynote presentations

NIST SP 800-73-3 Interfaces for Personal Identity Verification (4 Parts - Feb 2010) - Click here to download the End Point PIV Card Application Namespace, Data Model & Representation (Part 1), the PIV Card Application Card Command Interface (Part 2), the PIV Client Application Programming Interface (Part 3), and the PIV Transitional Interfaces & Data Model Specification (Part 4)

FIPS 201-1

- Personal Identity Verification (PIV) of Federal Employees and Contractors

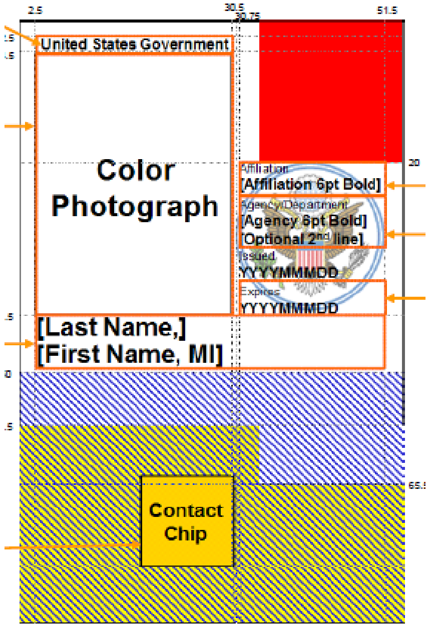


Figure 4-1. Card Front—Printable Areas
FIPS 201-1

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

- June 23, 2006 (FIPS 201, February 25, 2005)
- PIV-I & PIV-II

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

PIV-I

- Procedural requirements for
  - Issuance and revocation of credentials
  - PIV identity proofing and registration
  - PIV issuance and maintenance
  - PIV Privacy
- Not covered by PIV-I
  - Technical interoperability requirements for PIV credentials and systems
  - The use of a single universal credential

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

PIV-II

- Technical requirements
  - PIV Front-End
  - PIV Card Issuance and Management
  - Access Control

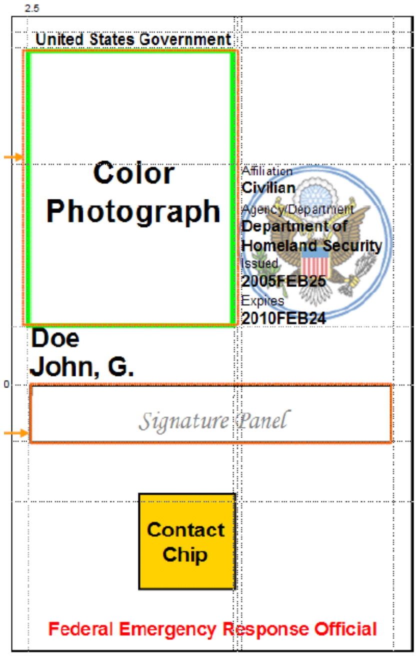


Figure 4-3. Card Front—Optional Data Placement—Example 2

FIPS 201-1

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

PIV-II (cont.)

- Front-End Subsystem
  - PIV Card
  - Card and biometric readers
  - Personal identification number (PIN) input device.
  - “The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.”

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

PIV-II

- 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."

FIPS 201-1

Personal Identity Verification (PIV) of Federal Employees and Contractors

PIV-II

- Access Control Subsystem

  "the physical and logical access control systems, the protected resources, and the authorization data."

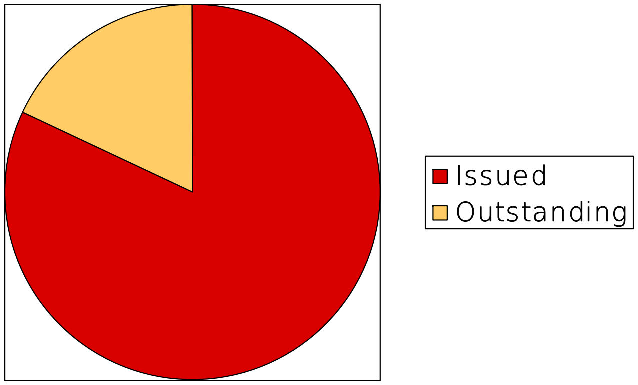
- Next: PIV Card Usage

PIV Cards

Current Usage

Credentials Issued as of December 1, 2009:

- Employees: 3,981,788 (86%)
- Contractors: 1,110,231 (72%)
- *(Total credentials issued: 5,092,019 (82%))*



Agency specific status:

- http://www.whitehouse.gov/omb/e-gov/hspd12_reports/
- Example: DoD Common Access Card (CAC)

Sources: http://www.idmanagement.gov, http://www.cac.mil

PIV Cards

Data Elements: SP 800-73-3 Part 1

Mandatory

- Card Capability Container (CCC)
- Card Holder Unique Identifier (CHUID)
- X.509 Certificate for PIV Authentication
- Cardholder Fingerprints
- Security Object

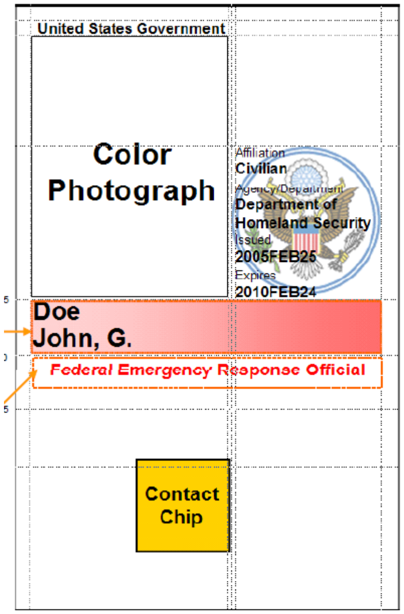


Figure 4-4. Card Front—Optional Data Placement—Example 3

FIPS 201-1

PIV Card Data Elements

SP 800-73-3 Part 1

Optional

- Cardholder Facial Image
- Printed Information
- X.509 Certificate for Digital Signature
- X.509 Certificate for Key Management
- X.509 Certificate for Card Authentication
- Discovery Object
- Key History Object
- Retired X.509 Certificates for Key Management
- Cardholder Iris Images

Next: Authentication uses?

Authentication

FIPS 201-1

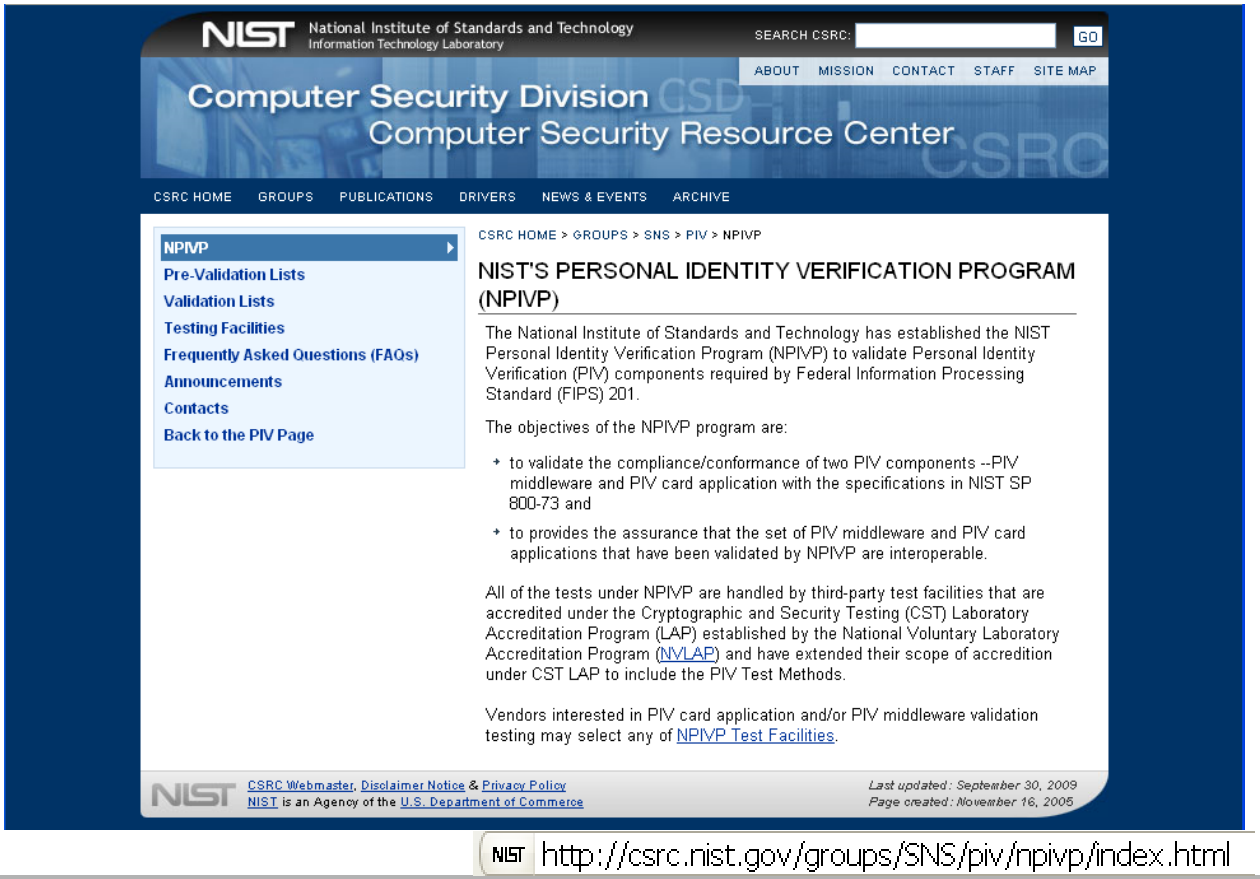
Options

- Visual
- Card Holder Unique ID (CHUID)
- Biometric
- .X509

Next: Why should the technology be trusted?

NPIVP (NIST)

NIST Personal Identity Verification Program



NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
Computer Security Division CSD
Computer Security Resource Center CSRC
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
NEWS & EVENTS
ARCHIVE
NPIVP
Pre-Validation Lists
Validation Lists
Testing Facilities
Frequently Asked Questions (FAQs)
Announcements
Contacts
Back to the PIV Page
CSRC HOME > GROUPS > SNS > PIV > NPIVP

NIST'S PERSONAL IDENTITY VERIFICATION PROGRAM (NPIVP)

The National Institute of Standards and Technology has established the NIST Personal Identity Verification Program (NPIVP) to validate Personal Identity Verification (PIV) components required by Federal Information Processing Standard (FIPS) 201.

The objectives of the NPIVP program are:

- to validate the compliance/conformance of two PIV components --PIV middleware and PIV card application with the specifications in NIST SP 800-73 and
- to provides the assurance that the set of PIV middleware and PIV card applications that have been validated by NPIVP are interoperable.

All of the tests under NPIVP are handled by third-party test facilities that are accredited under the Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP) established by the National Voluntary Laboratory Accreditation Program (NVLAP) and have extended their scope of accreditation under CST LAP to include the PIV Test Methods.

Vendors interested in PIV card application and/or PIV middleware validation testing may select any of NPIVP Test Facilities.

CSRC Webmaster, Disclaimer Notice & Privacy Policy
NIST is an Agency of the U.S. Department of Commerce

Last updated: September 30, 2009
Page created: November 16, 2005

NIST http://csrc.nist.gov/groups/SNS/piv/npivp/index.html

NPIVP (NIST)

NIST Personal Identity Verification Program

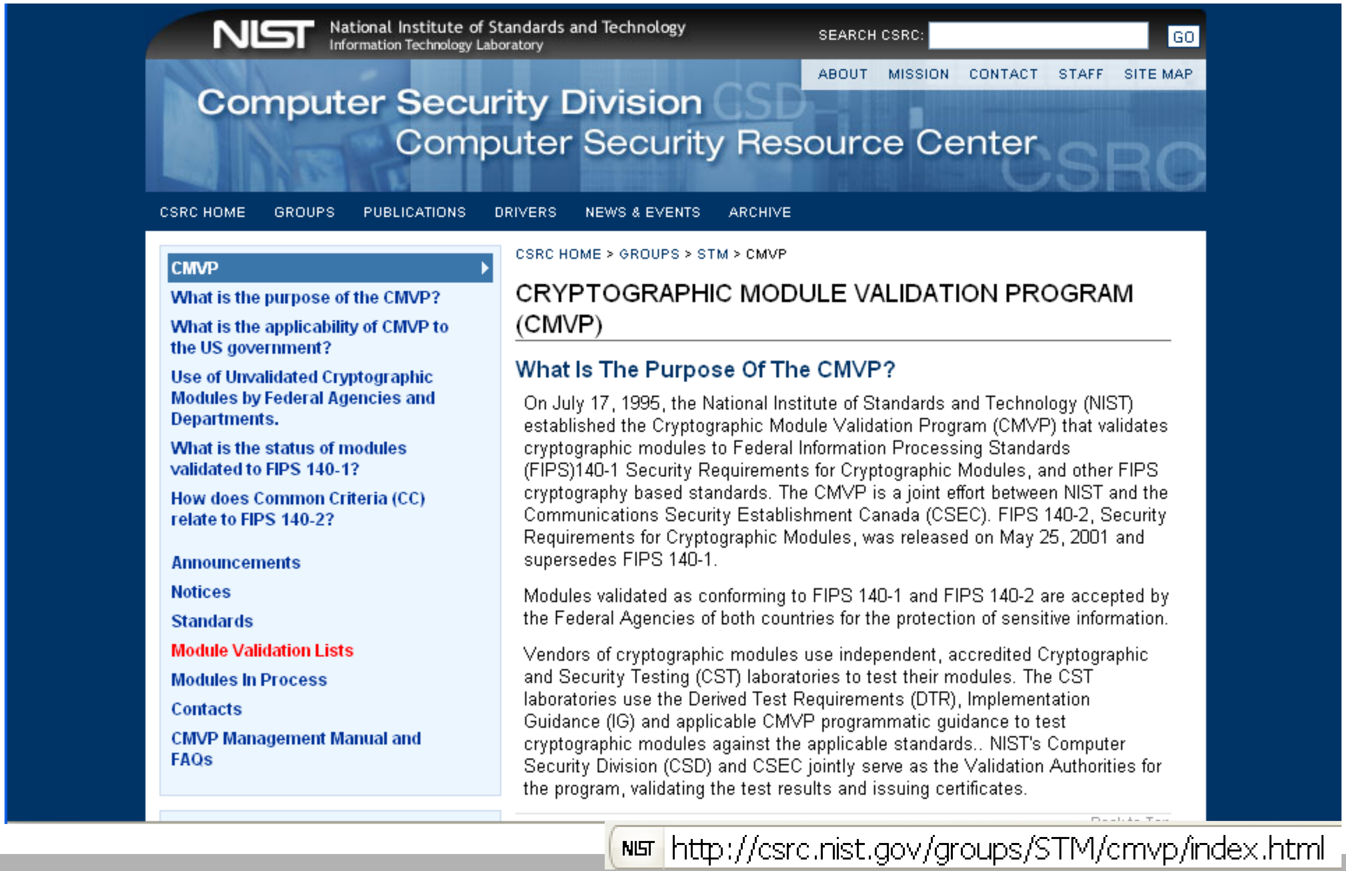
PIV-II

- Front-End Subsystem
  - Card Application
  - Middleware

- Next: what about cryptography?

CMVP (NIST & CSE)

Cryptographic Module Validation Program



NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
Computer Security Division CSD
Computer Security Resource Center CSRC
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
NEWS & EVENTS
ARCHIVE
CMVP
What is the purpose of the CMVP?
What is the applicability of CMVP to the US government?
Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments.
What is the status of modules validated to FIPS 140-1?
How does Common Criteria (CC) relate to FIPS 140-2?
Announcements
Notices
Standards
Module Validation Lists
Modules In Process
Contacts
CMVP Management Manual and FAQs
CSRC HOME > GROUPS > STM > CMVP

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

What Is The Purpose Of The CMVP?

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 and supersedes FIPS 140-1.

Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules. The CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards.. NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

NIST http://csrc.nist.gov/groups/STM/cmvp/index.html

CMVP (NIST & CSE)

Cryptographic Module Validation Program

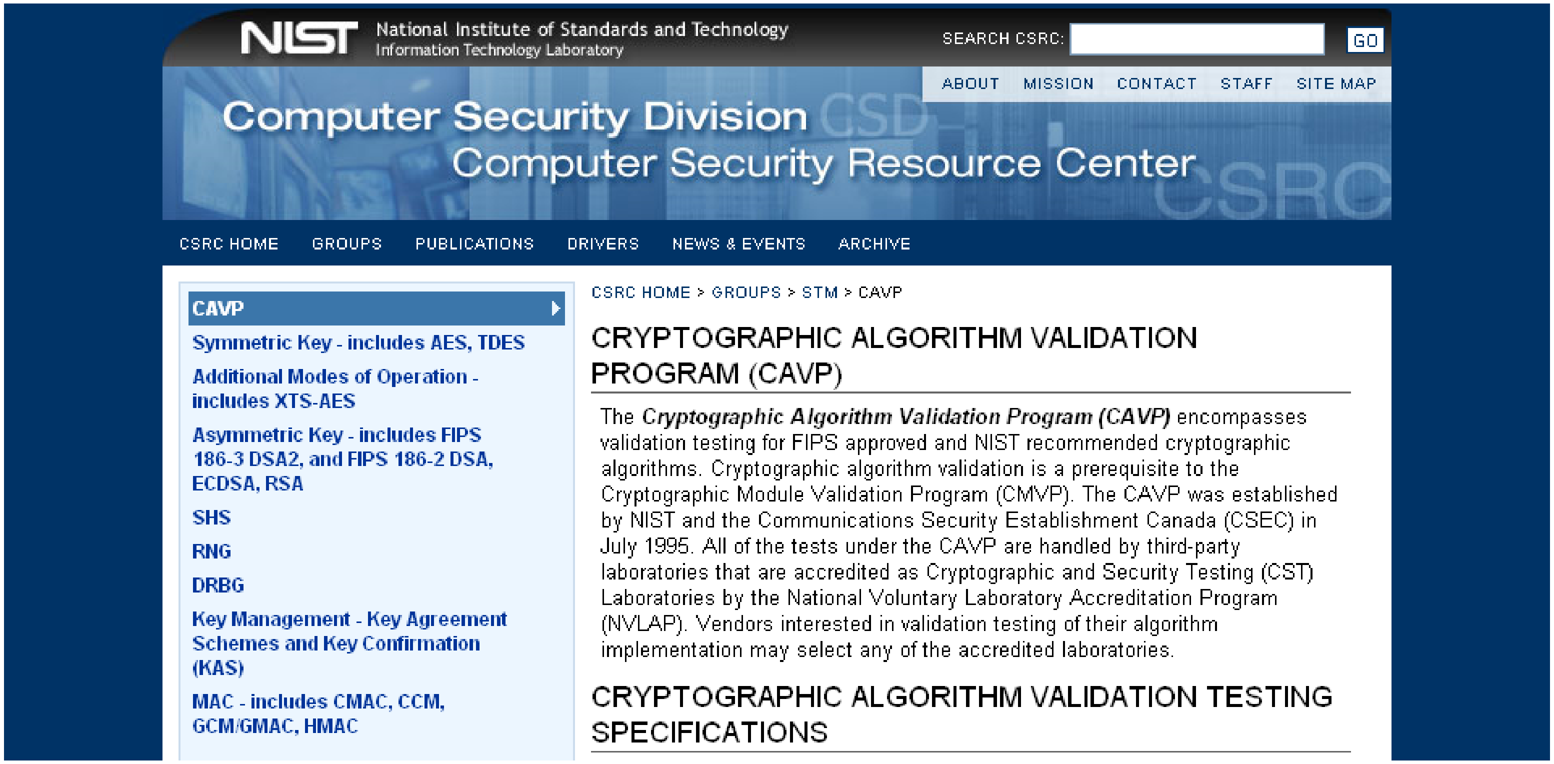
PIV-II

- Front-End Subsystem
  - PIV card (cryptographic module)
  - "All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage."- FIPS 201-1

- Next: algorithms?

CAVP (NIST & CSE)

Cryptographic Algorithm Validation Program


NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
Computer Security Division CSD
Computer Security Resource Center CSRC
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
NEWS & EVENTS
ARCHIVE
CAVP
Symmetric Key - includes AES, TDES
Additional Modes of Operation - includes XTS-AES
Asymmetric Key - includes FIPS 186-3 DSA2, and FIPS 186-2 DSA, ECDSA, RSA
SHS
RNG
DRBG
Key Management - Key Agreement Schemes and Key Confirmation (KAS)
MAC - includes CMAC, CCM, GCM/GMAC, HMAC
CSRC HOME > GROUPS > STM > CAVP

CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM (CAVP)

The *Cryptographic Algorithm Validation Program (CAVP)* encompasses validation testing for FIPS approved and NIST recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). The CAVP was established by NIST and the Communications Security Establishment Canada (CSEC) in July 1995. All of the tests under the CAVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing of their algorithm implementation may select any of the accredited laboratories.

CRYPTOGRAPHIC ALGORITHM VALIDATION TESTING SPECIFICATIONS

NIST http://csrc.nist.gov/groups/STM/cavp/index.html

CAVP (NIST & CSE)

Cryptographic Algorithm Validation Program

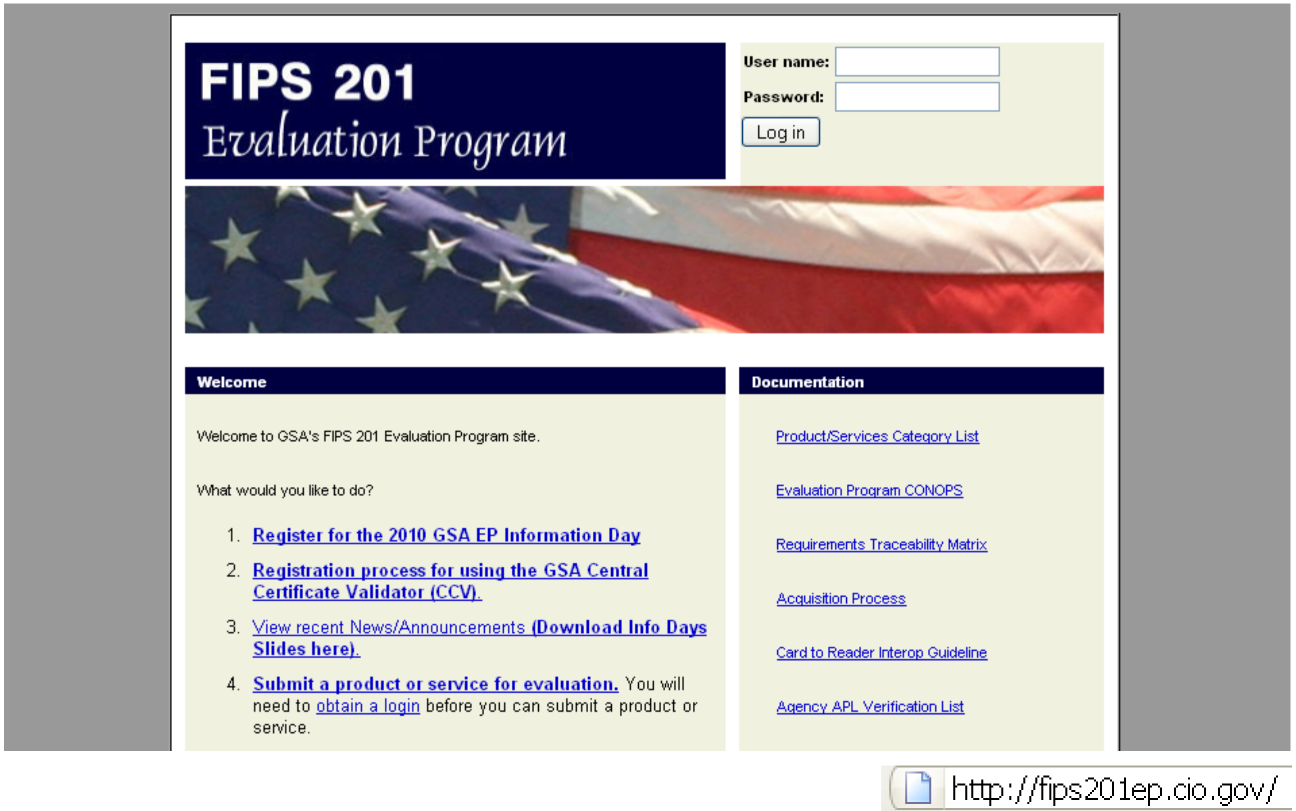
PIV-II

- Front-End Subsystem
  - Cryptographic algorithms used by PIV card

- Next: final approval

GSA FIPS 201 EP

- US Government General Services Administration FIPS 201 Evaluation Program



Welcome

Welcome to GSA's FIPS 201 Evaluation Program site.

What would you like to do?

1. Register for the 2010 GSA EP Information Day
2. Registration process for using the GSA Central Certificate Validator (CCV).
3. View recent News/Announcements (Download Info Days Slides here).
4. Submit a product or service for evaluation. You will need to obtain a login before you can submit a product or service.

Documentation

Product/Services Category List

Evaluation Program CONOPS

Requirements Traceability Matrix

Acquisition Process

Card to Reader Interop Guideline

Agency APL Verification List

http://fips201ep.cio.gov/

GSA FIPS 201 EP

US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Front-End Subsystem
- Card Issuance and Management Subsystem
- Access Control Subsystem

GSA FIPS 201 EP

US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Front-End Subsystem

1. PIV Card
2. Cryptographic Module
3. Electromagnetically Opaque Sleeve …

GSA FIPS 201 EP

- US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Front-End Subsystem

4. PIV Card Reader - Authentication Key
5. PIV Card Reader - Biometric
6. PIV Card Reader - Biometric Authentication
7. PIV Card Reader - CHUID Authentication (Contact)
8. PIV Card Reader - CHUID Authentication (Contactless)
9. PIV Card Reader - CHUID (Contact)
10. PIV Card Reader - CHUID (Contactless)
11. PIV Card Reader – Transparent

GSA FIPS 201 EP

US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Card Issuance and Management Subsystem

12. Caching Status Proxy
13. Card Printer Station
14. Certificate Validator
15. Certificate Validator (without authentication)
    Note: no authentication with client
16. Electronic Personalization
17. Electronic Personalization (service)
18. Facial Image Capturing Camera
19. Facial Image Capturing (Middleware)

GSA FIPS 201 EP

US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Card Issuance and Management Subsystem

20. Fingerprint Capture Station
21. Graphical Personalization (*service*)
22. Online Certificate Status Protocol (OCSP) Responder
23. PIV Card Delivery (*service*)
24. Single Fingerprint Capture Device
25. Sever-based Certificate Validation Protocol (SCVP) Client
26. SCVP Client (without authentication)
    Note: client does not authenticate to Certificate Validator.
27. Template Generator

GSA FIPS 201 EP

US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Access Control Subsystem

28. PIV Middleware (integrated as part of logical access control system)
29. Template Matcher

GSA FIPS 201 EP

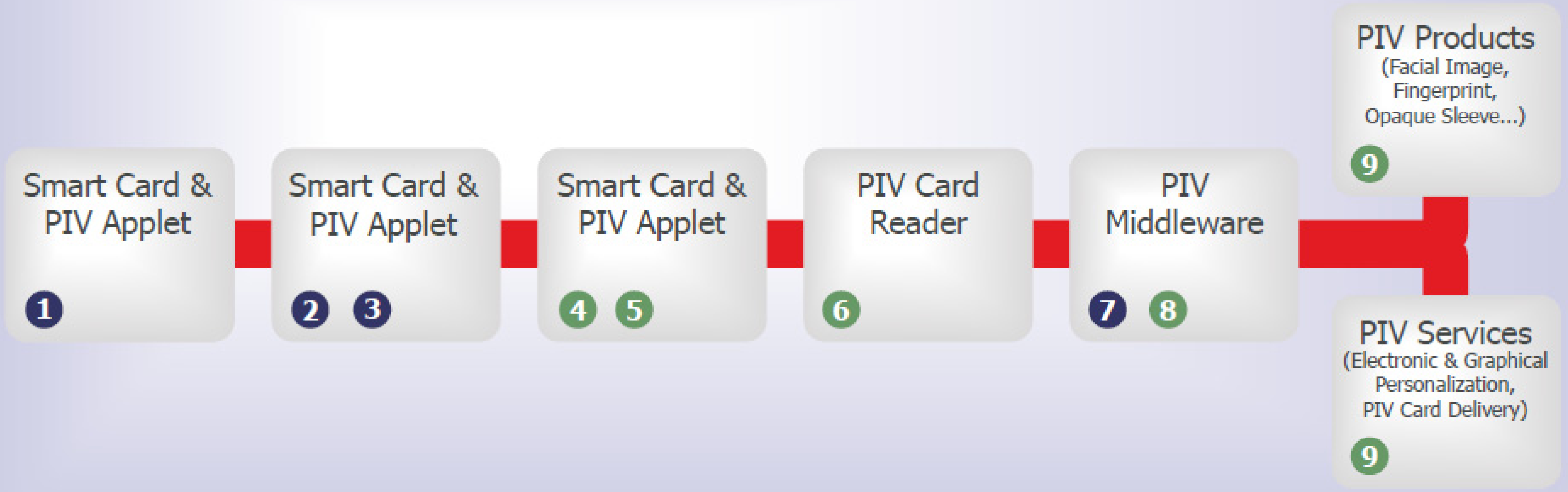
US Government General Services Administration FIPS 201 Evaluation Program

PIV-II

- Multiple Categories

30. Biometric Authentication System
31. CAK Authentication System
32. CHUID Authentication System
33. PIV Authentication System

FIPS 201 Compliant Identity and Access Solution



Smart Card & PIV Applet 1

Smart Card & PIV Applet 2 3

Smart Card & PIV Applet 4 5

PIV Card Reader 6

PIV Middleware 7 8

PIV Products (Facial Image, Fingerprint, Opaque Sleeve...) 9

PIV Services (Electronic & Graphical Personalization, PIV Card Delivery) 9

● NIST PIV Program Governed Testing

1. NPIVP PIV card applet certification
2. CAVP CAVS certification
3. CMVP FIPS 140-2 certification
7. NPIVP middleware certification

● GSA FIPS 201 Evaluation Program

4. GSA VTDR and GSA lab testing
5. GSA PIV card approval
6. GSA card reader approval
8. GSA middleware approval
9. GSA EP approval of additional FIPS 201 products and services

Security Professional Jobs

FIPS 201-1

Companies supplying FIPS 201 Approved Products

- Austin
  - 3M Company
  - Dell, Inc.
  - Gemalto, Inc.
  - Key Ovation
- …

Security Professional Jobs

FIPS 201-1

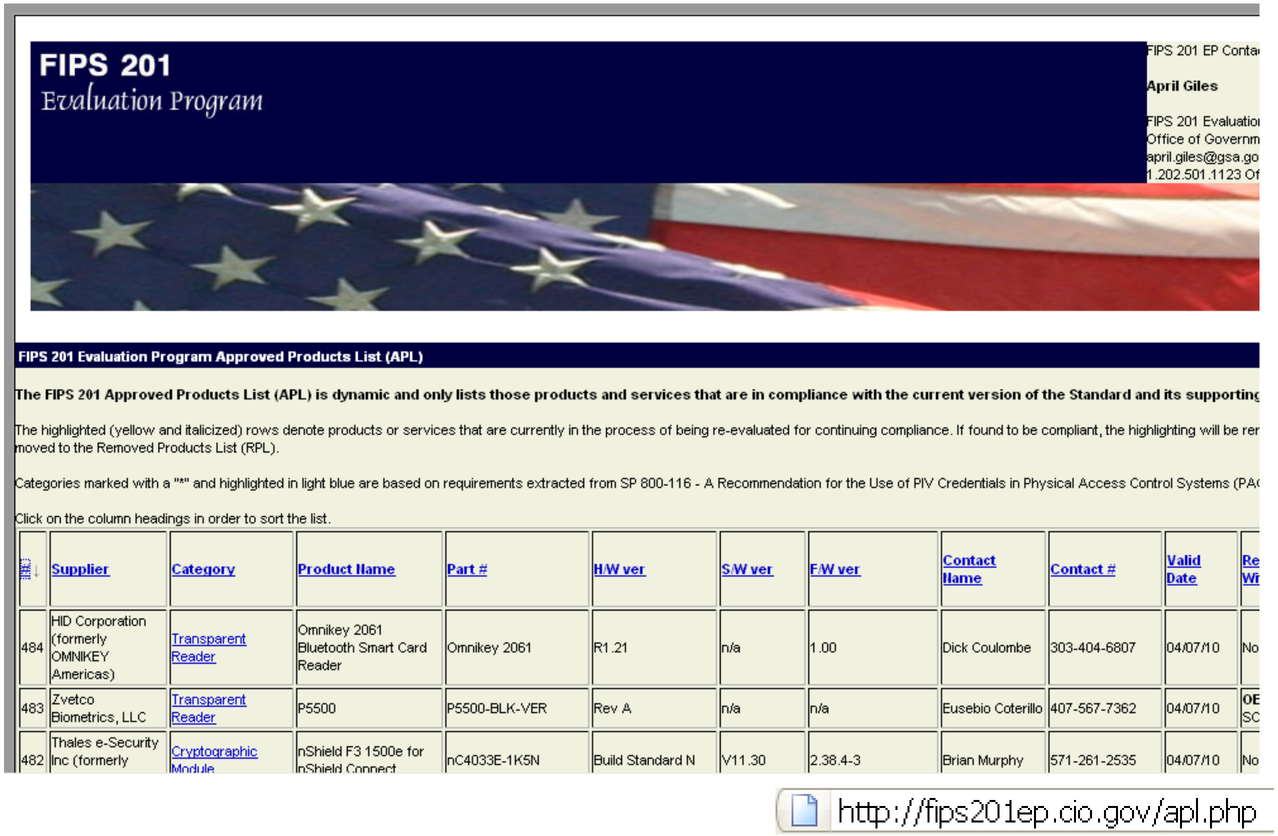
Companies supplying FIPS 201 Approved Products

- Additional
  - Charismathics Inc.
  - Codebench, Inc.
  - HID Global Corporation
  - Brady People ID / JAM
  - Thales e-Security Inc.
  - MaxID Corp.
  - Several more suppliers listed on http://fips201ep.cio.gov/apl.php

Security Professional Jobs

FIPS 201-1

- Product Development
- System Architect
- Operational Support
- Database specification
- Fraud investigation
- Forensics



FIPS 201
Evaluation Program

FIPS 201 EP Conta

April Giles

FIPS 201 Evaluatio
Office of Governm
april.giles@gsa.go
1.202.501.1123 Of

FIPS 201 Evaluation Program Approved Products List (APL)

The FIPS 201 Approved Products List (APL) is dynamic and only lists those products and services that are in compliance with the current version of the Standard and its supporting

The highlighted (yellow and italicized) rows denote products or services that are currently in the process of being re-evaluated for continuing compliance. If found to be compliant, the highlighting will be removed to the Removed Products List (RPL).

Categories marked with a "*" and highlighted in light blue are based on requirements extracted from SP 800-116 - A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PA

Click on the column headings in order to sort the list.

# ↓	Supplier	Category	Product Name	Part #	H/W ver	S/W ver	F/W ver	Contact Name	Contact #	Valid Date	Re Wi
484	HID Corporation (formerly OMNIKEY Americas)	Transparent Reader	Omnikey 2061 Bluetooth Smart Card Reader	Omnikey 2061	R1.21	n/a	1.00	Dick Coulombe	303-404-6807	04/07/10	No
483	Zvetco Biometrics, LLC	Transparent Reader	P5500	P5500-BLK-VER	Rev A	n/a	n/a	Eusebio Coterillo	407-567-7362	04/07/10	**OE** SC
482	Thales e-Security Inc (formerly	Cryptographic Module	nShield F3 1500e for nShield Connect	nC4033E-1K5N	Build Standard N	V11.30	2.38.4-3	Brian Murphy	571-261-2535	04/07/10	No

http://fips201ep.cio.gov/apl.php

Security Professional Jobs

FIPS 201-1

- Testing & Evaluation
  - NPIVP Laboratories
  - Cryptographic and Security Testing (CST) Laboratories
  - GSA Evaluation Program Approved Labs
- Consulting
  - Product design, system design…
  - Vendor Test Data Reports (GSA FIPS 201 EP)

Personal Identity Verification of Federal Employees and Contractors, Security Testing and Evaluation

References

- 9/11 Commission
  http://www.9-11commission.gov/
- HSPD-12
  http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html
- FIPS 140-2, FIPS 201-1
  http://csrc.nist.gov/publications/PubsFL.html
- IDMangagement.gov
  http://www.idmanagement.gov,
- CAC DoD Common Access Card
  http://www.cac.mil
- NPIVP
  http://csrc.nist.gov/groups/SNS/piv/npivp/index.html
- CMVP
  http://csrc.nist.gov/groups/STM/cmvp/index.html
- CAVP
  http://csrc.nist.gov/groups/STM/cavp/index.html
- GSA FIPS 201 EP
  http://fips201ep.cio.gov/

Questions?