

# IAB Agenda

- **Smart Card Alliance Introduction** (*Randy Vanderhoof, SCA*)
- **Keynote: Credentialing and Security** (*COL Hensley, JTF-GNO*)
- **Transportation Worker Identification Card (TWIC) Update** (*John Schwartz, DHS*)
- **Winter Storm Exercise: Results and Next Steps** (*Lemar Jones, PFPA & Craig Wilson, DHS*)
- **GSA Approved Products List Status** (*Dave Temoshok, GSA*)
- **NIST Update on Standards** (*Hildy Ferraiolo, NIST*)
- **Single Enrollment Process for Shared Service Provider Program** (*Michel Kareis, GSA*)
- **IAB Chairman Remarks** (*Mike Butler, IAB*)



# HSPD-12 Implementation: FIPS-201 Evaluation Program

---

***David Temoshok***  
***Director, Identity Policy and Management***  
***GSA Office of Governmentwide Policy***

**Industry Advisory Board**  
**April 11, 2007**

## Key Architecture Design Considerations



- Different authentication assurance levels are needed for different types of transactions.
- Architecture must support multiple authentication technologies – PIN, biometric template, CHUID, authentication keys.
- Architecture must support multiple protocols.
- Federal Government will not mandate a single proprietary solution, therefore, Architecture must support multiple COTS products.
- All architecture components must interoperate with ALL other components (see [www.idmanagement.gov](http://www.idmanagement.gov)) – requires product testing.
- Interface specifications are necessary for inter-system data exchange.
- Controls must protect privacy of personal information.

# NIST and GSA Roles – HSPD-12 Testing



- **NIST** -- Establish security and interoperability requirements in FIPS 201 and related interface specifications and test suites.
- **NIST** – Accredit laboratories to perform lab testing for:
  - FIPS 140-2 Cryptographic Modules
  - Smart Card PIV applets
  - PIV middleware
  - Validated products at <http://csrc.nist.gov/npivp/>
- **NIST** – Test fingerprint biometric generation and matching equipment per NIST SP 800-76-1 “PIV Biometric Data Specification
- **GSA** – Establish FIPS-201 Evaluation Program to determine conformance to FIPS-201 normative requirements.
  - 22 categories of products and services identified that require evaluation
  - Approved Product List at <http://fips201ep.cio.gov/>
- **GSA** -- Establish and maintain Approved Products Lists for product and services determined to be compliant with FIPS 201 normative requirements
- **GSA** – Provide government-wide schedule contracts on IT Schedule 70 and SIN 132-61 and 62 for FIPS 201 compliant products/services
- **GSA** – Test agency-specific configuration for ICC encoding (Electronic Personalization) of PIV data model per OMB-07-06

# Status of GSA FIPS 201 Evaluation Program



- GSA/NIST identified 22 categories of products/services directly impacted by FIPS 201 requirements
  - ✓ All 22 categories of products/services are needed for full HSPD-12 implementation
- Current product and services approvals:
  - ✓ 220+ products on FIPS 201 Approved Product List
  - ✓ Approved products in all categories except: Card Reader Biometric, Card Reader Authentication Key, PIV Delivery Service
  - ✓ 6 approved PKI Shared Service Providers
  - ✓ 20+ approved integrators, 8 provide end-to-end HSPD-12 solutions
- GSA is proceeding from contracted lab services to certified 3<sup>rd</sup>-party labs for FIPS-201 conformance evaluations
  - ✓ GSA contracted for lab services for all EP evaluations 5/06 – 4/07
  - ✓ 2/2/07 Federal Register Notice that GSA is changing FIPS-2-1 EP fee structure and moving to 3<sup>rd</sup>-party lab certification
  - ✓ Effective 4/3/07 GSA discontinued contracted evaluations

# Accessing the FIPS 201 Approved Products List



FIPS 201 Evaluation Program - Microsoft Internet Explorer provided by General Services Administration

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

## FIPS 201 Evaluation Program

### FIPS 201 Evaluation Program Approved Product List

Click on the column headings in order to sort the list

Supplier	Category	UUE Name	UUE #	H/W ver	S/W ver	F/W ver	Contact Name	Contact #	Valid Date	Restrictions / Tested With
Verisign, Inc.	Shared Service Provider	Verisign SSP PKI	n/a	n/a	1.1	n/a	Nicholas F. Piazzola	410-691-2100	06/14/06	none
ORC, Inc.	Shared Service Provider	ORC ACES/SSP	n/a	n/a	3.3.1	n/a	Daniel Turissini	703-401-1706	06/15/06	none
Cybertrust, Inc.	Shared Service Provider	Cybertrust Federal SSP	n/a	n/a	n/a	n/a	Thomas Greco	443-367-7052	06/20/06	none
Cogent Systems, Inc.	Template Generator	BioSDK 4.1/COGENT BSP	00170A47	n/a	4.1	n/a	Bruno Lassus	703-476-9381	06/28/06	none
Cogent Systems, Inc.	Template Matcher	BioSDK 4.1/COGENT BSP	00170A45	n/a	4.1	n/a	Bruno Lassus	703-476-9381	06/28/06	none
Cross Match Technologies Inc.	Fingerprint Capture Station	ID 500	ID 500	n/a	n/a	n/a	Paul Frasca	703-841-6285	06/28/06	none
Cross Match Technologies Inc.	Fingerprint Capture Station	ID 500M	ID 500M	n/a	n/a	n/a	Paul Frasca	703-841-6285	06/28/06	none
Cross Match Technologies Inc.	Fingerprint Capture Station	ID 700	ID 700	n/a	n/a	n/a	Paul Frasca	703-841-6285	06/28/06	none
Cross Match Technologies Inc.	Fingerprint Capture Station	LScan Guardian	LScan Guardian	n/a	n/a	n/a	Paul Frasca	703-841-6285	06/29/06	none
Oberthur Card Systems	PIV Card	PIV End Point Dual Interface Smart Card	n/a	1.08	1.08	n/a	Christophe Goyet	703-322-8951	06/30/06	The magnetic stripe feature has

24 of 24 - Clipboard  
Item collected.

Start | 5:07 PM

## *PIV Card Encoding Test – 800-85B Tool*



- FIPS 201 APL category “Electronic Personalization” tests for conformant encoding of the PIV data model on the cards ICC.
- Full test specifications are contained in NIST SP 800-85B.
- NIST developed 800-85B tool to implement test specifications of SP 800-85B.
  - 800-85B test tool and Installation and Configuration Guide are available at: [http://csrc.nist.gov/piv-program/dm\\_tester/index.html](http://csrc.nist.gov/piv-program/dm_tester/index.html)
- 4 basic set of conformance tests:
  - BER-TLV (Basic Encoding Rules – Tag, Length, Value) – 11 tests verify that all data objects conform to specified encoding formats
  - Biometric Data – 57 tests verify biometric data conformance to SP 800-76-1 specifications
  - Certificate Profile – 35 tests verify certificate conformance to PKI Common Policy and SP 800-78-1.
  - Digital Signature – 66 tests verify digital signature for all signed data objects and verify security object hashes.

## *Status of Agency Card Testing*



- OMB M-07-06 required all agencies to provide PIV card with agency-specific configuration to GSA for testing.
- GSA is applying 800-85B test tool for all Agency Card Testing to validate encoding of PIV data model.
- GSA will test all optional objects encoded on card.
- Card encoding and Test Tool are complex.
- A dozen agency-specific card configurations have been approved.
- This testing is absolutely necessary to even begin to talk about interoperability.



## *For More Information*

- Visit our Websites:  
<http://www.idmanagement.gov>  
<http://www.cio.gov/ficc>  
<http://www.cio.gov/fpkipa>  
<http://www.csrc.nist.gov/piv-project>

- Or contact:

David Temoshok

Director, Identity Policy and Management

202-208-7655

[david.temoshok@gsa.gov](mailto:david.temoshok@gsa.gov)