Interagency Advisory Board (IAB) Meeting

March 15, 2006
Introductory Remarks

Mike Butler
IAB Chairman
# Federal HSPD-12 Technical Issues

<table>
<thead>
<tr>
<th>Issue #</th>
<th>Explanation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue #1</td>
<td>PIV Auth Key and CAC Signature Key both have OID 0x0101</td>
<td><img src="color.png" alt="Issue is resolved" /></td>
</tr>
<tr>
<td>Issue #2</td>
<td>The Security Object does not provide guidance for the following objects</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #3</td>
<td>Read Binary vs. Get Data</td>
<td><img src="color.png" alt="No action on this issue" /></td>
</tr>
<tr>
<td>Issue #4</td>
<td>CHUID Buffer Length</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #5</td>
<td>Expiration Date consistency-not clear in SP 800-73</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #6</td>
<td>PIV Auth Key Cert</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #7</td>
<td>More guidance is requested for the digital camera interface that is used at enrollment</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #8</td>
<td>Requirement to use PIN to access public key</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
<tr>
<td>Issue #9</td>
<td>Transitional vs End-State, 2-byte vs 3-byte tags in the data model</td>
<td><img src="color.png" alt="Issue resolution is in progress" /></td>
</tr>
</tbody>
</table>

## Color Coding Key

<table>
<thead>
<tr>
<th>Color</th>
<th>Issue Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Issue is resolved</td>
</tr>
<tr>
<td>Yellow</td>
<td>Issue resolution is in progress</td>
</tr>
<tr>
<td>Red</td>
<td>No action on this issue</td>
</tr>
</tbody>
</table>
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- Break
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- Interactive Session
- Press wrap-up
Winter Fox Interoperability Demonstration

23 February 2006

Coordinated by:
Department of Homeland Security
Office of National Capital Region Coordination
Thomas J. Lockwood, Director

Hosted by:
Department of Defense
Pentagon Force Protection Agency
Robert Taylor, Director
Goal: Multi-jurisdictional Identity Trust Model

To demonstrate multi-jurisdictional identity interoperability by electronically binding personalized First Responder Authentication Cards (FRACs), that were issued from different back-end infrastructures, to authorized responder in a communication-in or out environment.
Objectives and Targeted Population

**Objective**
To demonstrate multi-jurisdictional interoperability by validating DoD CACs or First Responder FRACs issued from different back-end infrastructures

**Targeted Participation**
Participation for this exercise was focused primarily on federal, state, regional, local, private sector, and public safety leadership to grasp a better understanding of a trusted and secure electronic identity trust model that provides multi-jurisdictional interoperability that can be leveraged for incident identity and emergency attribute(s) management.
Multi-Jurisdictional Recognition

INFORMATION FEED:
- FEDERAL
- STATE
- LOCAL
- PRIVATE

First Responder Validation Authority
(Produced and Synchronized Nightly)

PDA INFORMATION FORMAT:
- DATA
- TEXT
- IMAGE
Federal / State / Perimeter Access Controls

Scenario 2
Virginia State Property

1. Escort Required
2. Simulated Incident Scene Third perimeter Staging Area
3. Escorted Required
4. Authorized FRAC & ESF
5. Incident Scene Second Perimeter Staging Area
6. Escorted Required
7. Authorized FRAC
8. VDOT Smart Traffic Center

Scenario 1
Pentagon Federal Property

1. Staging Area (Incident Scene Outer Perimeter)
2. Mobile ID Unit
3. Authorized FRAC or DoD CAC
4. Authorized FRAC & ESF
5. Incident Scene Second Perimeter Staging Area
6. Escorted Required
7. Authorized FRAC
8. VDOT Smart Traffic Center
9. Federal Office Building II

Access Controls:
- Authorized FRAC or DoD CAC
- Escort Required
- Authorized FRAC & ESF
Multi-jurisdictional Identity Management

Scenario 3

Maryland State Property

- Dispatching Federal assistance team dispatched from a federal agency

1) The Federal assistance and COOP/COG teams will cross numerous state, county and federal jurisdictions in order to reach final destinations

3) Notification of arrivals will be transmitted by email (coms-in) and SATCOM message (coms-out) back to the sponsoring agency

5) All electronic identity transactions at locations will be transmitted by email (coms-in) and SATCOM message (coms-out) back to the sponsoring agency

Scenario 4

Maryland County Municipal

- Dispatching emergency evacuation of COOP/COG personnel to a relocation site

2) Once the teams reach their final destinations each member will check-in using their FRACs for electronic identity and PIN verification

4) Upon conclusion of the demonstration all participants will electronically check-out

Port of Baltimore
Incident Area Access Control

Pentagon
Sponsoring Agency

Frederick County
Maryland check-point
PKI Interoperability

Credential Issuers
- DoD / CAC
- VA / NCR / FRAC
- MD / FRAC
- TSA / TWIC

ID Cards

Privileged Lists
- Trusted: ...
- Trusted: ...
- Trusted: ...
- Trusted: ...

Validation Authority

Compressed, Signed Validation Lists
(produced and synchronized every 24 hours at minimum)
- Valid
- Valid
- Valid
- Valid

Authorization Handhelds

First Responder Attribute Authority

*CRLs – certificate revocation lists
# Winter Fox Data Sample

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Cardholder Name</th>
<th>Card Issuer</th>
<th>ID Type</th>
<th>Summary</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/23/2006 10:28</td>
<td>BYS, JOHN, M, 2ND</td>
<td>CT</td>
<td>Driver's License</td>
<td>Success: Driver's license scan</td>
<td>Baltimore Operator</td>
</tr>
<tr>
<td>2/23/2006 10:24</td>
<td>COLOMBA, ANGELO</td>
<td>DHS Smart Card CA-2</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>Default Operator</td>
</tr>
<tr>
<td>2/23/2006 12:01</td>
<td>COLOMBA, ANGELO</td>
<td>DHS Smart Card CA-2</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>Default Operator</td>
</tr>
<tr>
<td>2/23/2006 11:05</td>
<td>DANIEL A. PICKENS</td>
<td>DHS Smart Card CA-2</td>
<td>Smart Card</td>
<td>Failure: PIN Verification</td>
<td>PPFA Operator</td>
</tr>
<tr>
<td>2/23/2006 11:06</td>
<td>DANIEL A. PICKENS</td>
<td>DHS Smart Card CA-2</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>PPFA Operator</td>
</tr>
<tr>
<td>2/23/2006 11:07</td>
<td>HAGY, JAMES, WILEY</td>
<td>MD</td>
<td>Driver's License</td>
<td>Success: Driver's license scan</td>
<td>Maryland Operator</td>
</tr>
<tr>
<td>2/23/2006 10:24</td>
<td>JOHN E MARKEY 1</td>
<td>PIVMobile CA</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>Maryland Operator</td>
</tr>
<tr>
<td>2/23/2006 11:04</td>
<td>JOHN E MARKEY 1</td>
<td>PIVMobile CA</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>Maryland Operator</td>
</tr>
<tr>
<td>2/23/2006 10:02</td>
<td>ROGER EWIN ROEHR</td>
<td>TWIC Program CA1</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>PPFA Operator</td>
</tr>
</tbody>
</table>
Winter Fox
(data sample a closer look)

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Cardholder Name</th>
<th>Card Issuer</th>
<th>ID Type</th>
<th>Summary</th>
<th>Operator</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Cardholder Name</th>
<th>Card Issuer</th>
<th>ID Type</th>
<th>Summary</th>
<th>Operator</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Cardholder Name</th>
<th>Card Issuer</th>
<th>ID Type</th>
<th>Summary</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/23/2006 10:02</td>
<td>ROGER EWIN ROEHR</td>
<td>TWIC Program CA1 MD</td>
<td>Smart Card</td>
<td>Success: Card Validation</td>
<td>PFPA Operator</td>
</tr>
</tbody>
</table>
Winter Fox Identity Transaction Metrics

**Locations:**
- 285 total scans recorded:
  - 138 scans into VDOT Smart Traffic Center
  - 87 scans into Pentagon Federal Property
  - 35 scans into Baltimore Incident Area
  - 25 scans Frederick County, MD

**Transactions:**
- 206 Success: Card Validation
- 79 Failure: Pin Verification

**Technology:**
- 5 Drivers license bar code, no bind to card
- 263 FRACs (w/ digital photo) plus PIN verification
- 16 CACs (w/o photo) plus PIN verification
- 1 TWIC (w/o photo) plus PIN verification
Winter Fox Validated Proof of Concepts

Validated key capabilities:

- A multi-jurisdictional identity trust model at a Pentagon federal facility, Virginia State facility, Maryland State port, and Maryland County municipality

- Routine electronic physical access into federal and state facilities

- Incident area first, second and third perimeter control using electronic identity validation for incident management

- Secure access through a local municipality-controlled check point

- In-transit visibility of COOP/COG human resource assets in a communication-in and/or out environment

- Satellite communications (SATCOM) manifest tracking of sponsoring agency personnel to a relocation sites

- Federal, state, and local EOC notification and cross agency personnel visibility

- Time keeping/reimbursement; post-event notification
Strategic Objectives

1. **Establishment of a multi-jurisdictional identity trust model** in accordance with existing standards and technology that enables interoperability for dynamic identity and emergency attribute management.

2. **Categorize all emergency response or critical infrastructure support personnel** in accordance with the National Response Plan (NRP) or National Infrastructure Protection Plan (NIPP).

3. **Integrate identity and NRP/NIPP category information into existing authoritative human resources databases/directories** for use with current technology tool sets that support the electronic proliferation of trusted and secure information for access decisions.

4. **Standardize NRP/NIPP occupation sub-categories and qualifications** in accordance with national and international personnel qualification standards as appropriate.

5. **Conduct exercises to integrate use with response requirements and applications development** for trusted and secure electronic incident management with accountability.

6. **Proof of concept of key capabilities:** personnel accountability / physical access, incident muster list, EOC notification/cross agency personnel visibility, time keeping/reimbursement; post-event notification, enhanced COOP/COG processes.
Notional PDA ID Authentication & Attribute Validation Screen Shot

1. **Identity Authentication Confirmation**
   - Unconfirmed
   - Incorrect Pin
   - Confirmed
   - Revoked

2. **Identity Assurance Level**
   - Basic
   - Medium
   - High

3. **NIPP Sector Coordinating Council**
   (17 sectors of critical infrastructure both public and private)

4. **NIMS ESF Category**
   - #1 – Transportation
   - #2 – Communications
   - #3 – Public Works and Engineering
   - #4 – Firefighting
   - #5 – Emergency Management
   - #6 – Mass Care, Housing, and Human Services
   - #7 – Resource Support
   - #8 – Public Health and Medical Services
   - #9 – Urban Search and Rescue
   - #10 – Oil and Hazardous Materials Response
   - #11 – Agriculture and Natural Resources
   - #12 – Energy
   - #13 – Public Safety and Security
   - #14 – Long-Term Community Recovery and Mitigation
   - #15 – External Affairs

5. **Attribute Nomenclature**
   - **Qualification** – (e.g., COOP, COG, State Trooper, doctor, utility, water)
   - **Certification** – (e.g., Skill, EMT, Firefighter, SWAT)
   - **Authorization** – (e.g., Lawful Entitlement, Weapons, security investigation)
   - **Privilege** – (e.g., Official Benefits, VIP)

6. **Sponsoring Agency**
   (store on card)

7. **Jurisdiction Location**
   (store on card)

8. **State**
   (store on card)
End state: Preparedness Identity Management

**Incident Management:**

To get the right people with the right attributes to the right places at the right times thus reducing response/recovery times and promoting restoration to pre-incident quality of life conditions

**Intended benefit:**

Emergency response officials will possess public-key infrastructure (PKI) identity cards that align with federal standards and enable electronic validation of identity and emergency attribute information for determining access privileges

**Additional benefit:**

Emergency response officials will possess PKI identity cards issued by respective sponsoring agencies in a distributed environment that can be integrated into standards-based physical and logical access systems
Questions?
FRACSupport@dhs.gov

Office of National Capital Region Coordination
202-254-2301

Craig A. Wilson
Partnership Coordinator
202-254-2305 (office)
703-597-4113  (cell)
craig.a.wilson@associates.dhs.gov
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance (Ramaswamy Chandramouli)
- NIST update on HSPD-12 Document Revision Progress (Curt Barker)
- GSA update on FIPS 201 Evaluation Program (April Giles)
- Break
- Smart Card Alliance (SCA) Conference (Randy Vanderhoof)
- Physical Access Synergy of PAIWG/SCA/SIA (Tony Cieri & Team Leads)
- Backend Authentication Scheme Working Group (BASWG) Update (Tim Baldridge)
- Interagency Partnership Working Group (IPWG) Update (Ron Martin)
- Common Handheld Device RFI Vendor Presentation (Frank Jones)
- Interactive Session
- Press wrap-up
Biometric Data Test Support for PIV

Ramaswamy Chandramouli (Mouli) (mouli@nist.gov) & Elaine Newton (elaine.newton@nist.gov)

IAB Meeting, March 15, 2006
<table>
<thead>
<tr>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Background</strong> - Tests for Biometric Data for PIV</td>
</tr>
<tr>
<td>• <strong>MINEX Test Report</strong></td>
</tr>
</tbody>
</table>
Background - Tests for Biometric Data for PIV

• **Biometric Data – Online Tests**
  - Format and Content of Biometric Record for conformance to SP 800-76
    - CBEFF Wrapper Format
    - INCITS 378 Profile Format
    - Signature Block Format & Content

• **Biometric Data – Offline Tests**
  - MINEX Tests
    - Tests for Template (Minutiae) Interoperability
Minutiae Interoperability
Exchange Test

(MINEX 04)

Elaine Newton
NIST
Exchange of Fingerprint Data

Factors To Consider:
- Accuracy
- Processing time
- Size on card

Images or Templates
Minutiae Example

Figure 1: Examples of Minutiae Placement Variation
A NIST Special Database 29 image annotated with the $(x, y, \theta, \text{type})$ minutiae points of the MINA template generators. Red indicates type “other”, green indicates “ridge ending”, and blue labels “bifurcation”.
Types of Templates

- Proprietary templates
  - Individual vendor’s representation of images
- Standard templates: INCITS 378 format
  - MIN:A templates
    - codes minutiae coordinates \((x, y)\), angle \((\theta)\), type, & quality
  - MIN:B templates
    - MIN:A data plus ridge count, core, and delta information
Largest Biometric Test to Date…

• 4 datasets:
  – POEBVA, DHS2, POE, and DOS
• Number of Samples
  – 60,000 matched fingerprint pairs
  – 120,000 non-match fingerprints
• 14 vendors
  – Six participants in MIN:B testing
• 4.4 billion comparisons resulting > 45 GB of data
Vendors

A. Cogent Systems Incorporated
B. Dermalog Identification Systems GMBH
C. Bioscrypt Incorporated
D. Sagem Morpho Incorporated
E. Neurotechnologija
F. Innovatrics
G. NEC Corporation
H. Technoimagia Corporation
I. Identix Incorporated
J. Biologica Sistemas
K. SPEX Forensics
L. Secugen Corporation
M. NITGen Corporation
N. Cross Match Technologies
Questions

• Does the template give accuracy comparable with proprietary (image-based) implementations?

• Can template data be generated and matched by different vendors without attendant increase in error rates?
Detection Error Tradeoff Curves
Types of Tests

- Single- v. Two- Finger
- Proprietary v. Native
- Native v. Interoperable
- Scenarios 1, 2, 3, & 4
- Four dataset of different quality
Results 1

- Proprietary templates are superior to MIN:A templates in accuracy.

- The enhanced MIN:B template performed only marginally better than the basic MIN:A template.
Proprietary and Native Performance for Single-Finger Test at FMR=0.01 for POEBVA data
Proprietary and Native Performance for Two-Finger Test at FMR=0.01 for POEBVA data
Results 2

• As with most recent tests (by NIST and others), the error rates between matching algorithms vary by an order of magnitude.

• Two-finger authentication with standard templates can achieve the accuracy of single-finger authentication with proprietary templates.
Results 3

• The leading vendors in template generation are not always the leaders in matching and vice-versa.
  – Some template generators produce standard templates that are matched more accurately than others. Some combination of templates fail completely.
  – Some matchers compare templates more accurately than others.
### Finding Interoperable Groups

#### Table

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>Mean</th>
<th>Rank</th>
<th>Med.</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0171</td>
<td>0.0162</td>
<td>0.0072</td>
<td>0.0073</td>
<td>0.0032</td>
<td>0.0103</td>
<td>0.0086</td>
<td>0.0094</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- Mean values for each group are provided.
- Rank indicates the order of the mean values within each group.
Largest Interoperable Group for POEBVA
s.t. the max FNMR ≤ 0.01 @ FMR = 0.01

<table>
<thead>
<tr>
<th>NF=2</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.011</td>
<td>0.0092</td>
<td>0.0089</td>
<td>0.0021</td>
<td>0.0130</td>
<td>0.0079</td>
<td>0.0049</td>
<td>0.0248</td>
<td>0.0049</td>
<td>0.0758</td>
<td>0.0292</td>
<td>0.0161</td>
<td>0.0213</td>
<td>0.0271</td>
</tr>
<tr>
<td>B</td>
<td>0.0027</td>
<td>0.0024</td>
<td>0.0072</td>
<td>0.0018</td>
<td>0.0073</td>
<td>0.0071</td>
<td>0.0017</td>
<td>0.0456</td>
<td>0.0049</td>
<td>0.0889</td>
<td>0.0259</td>
<td>0.0105</td>
<td>0.0213</td>
<td>0.0182</td>
</tr>
<tr>
<td>C</td>
<td>0.0052</td>
<td>0.0057</td>
<td>0.0052</td>
<td>0.0025</td>
<td>0.0164</td>
<td>0.0061</td>
<td>0.0039</td>
<td>0.0851</td>
<td>0.0081</td>
<td>0.1571</td>
<td>0.1048</td>
<td>0.0177</td>
<td>0.0099</td>
<td>0.0013</td>
</tr>
<tr>
<td>D</td>
<td>0.0021</td>
<td>0.0046</td>
<td>0.0045</td>
<td>0.0013</td>
<td>0.0097</td>
<td>0.0044</td>
<td>0.0035</td>
<td>0.0325</td>
<td>0.0062</td>
<td>0.0877</td>
<td>0.0442</td>
<td>0.0154</td>
<td>0.0126</td>
<td>0.0003</td>
</tr>
<tr>
<td>E</td>
<td>0.0025</td>
<td>0.0061</td>
<td>0.0056</td>
<td>0.0028</td>
<td>0.0045</td>
<td>0.0084</td>
<td>0.0035</td>
<td>0.0280</td>
<td>0.0102</td>
<td>0.0600</td>
<td>0.0362</td>
<td>0.0163</td>
<td>0.0047</td>
<td>0.0053</td>
</tr>
<tr>
<td>F</td>
<td>0.0054</td>
<td>0.0060</td>
<td>0.0052</td>
<td>0.0025</td>
<td>0.0103</td>
<td>0.0061</td>
<td>0.0038</td>
<td>0.0855</td>
<td>0.0081</td>
<td>0.1597</td>
<td>0.1088</td>
<td>0.0177</td>
<td>0.0097</td>
<td>0.0013</td>
</tr>
<tr>
<td>G</td>
<td>0.0040</td>
<td>0.0032</td>
<td>0.0085</td>
<td>0.0022</td>
<td>0.0061</td>
<td>0.0085</td>
<td>0.0007</td>
<td>0.0308</td>
<td>0.0068</td>
<td>0.0715</td>
<td>0.0693</td>
<td>0.0116</td>
<td>0.0074</td>
<td>0.0024</td>
</tr>
<tr>
<td>H</td>
<td>0.0064</td>
<td>0.0421</td>
<td>0.0393</td>
<td>0.0143</td>
<td>0.0767</td>
<td>0.0395</td>
<td>0.0234</td>
<td>0.0422</td>
<td>0.0210</td>
<td>0.0999</td>
<td>0.0724</td>
<td>0.0413</td>
<td>0.0855</td>
<td>0.0031</td>
</tr>
<tr>
<td>I</td>
<td>0.0073</td>
<td>0.0084</td>
<td>0.0252</td>
<td>0.0100</td>
<td>0.0333</td>
<td>0.0249</td>
<td>0.0083</td>
<td>0.1357</td>
<td>0.0086</td>
<td>0.1206</td>
<td>0.1170</td>
<td>0.0027</td>
<td>0.0313</td>
<td>0.0015</td>
</tr>
<tr>
<td>J</td>
<td>0.0077</td>
<td>0.0119</td>
<td>0.0259</td>
<td>0.0062</td>
<td>0.0275</td>
<td>0.0257</td>
<td>0.0070</td>
<td>0.1572</td>
<td>0.0103</td>
<td>0.0840</td>
<td>0.0576</td>
<td>0.0198</td>
<td>0.0297</td>
<td>0.0073</td>
</tr>
<tr>
<td>K</td>
<td>0.0068</td>
<td>0.0130</td>
<td>0.0108</td>
<td>0.0051</td>
<td>0.0154</td>
<td>0.0109</td>
<td>0.0049</td>
<td>0.0280</td>
<td>0.0068</td>
<td>0.0629</td>
<td>0.0275</td>
<td>0.0293</td>
<td>0.0145</td>
<td>0.0024</td>
</tr>
<tr>
<td>L</td>
<td>0.0113</td>
<td>0.0019</td>
<td>0.0248</td>
<td>0.0015</td>
<td>0.0288</td>
<td>0.0215</td>
<td>0.0086</td>
<td>0.0785</td>
<td>0.0105</td>
<td>0.0661</td>
<td>0.1123</td>
<td>0.0113</td>
<td>0.0036</td>
<td>0.0025</td>
</tr>
<tr>
<td>M</td>
<td>0.0059</td>
<td>0.0096</td>
<td>0.0106</td>
<td>0.0049</td>
<td>0.0115</td>
<td>0.0108</td>
<td>0.0039</td>
<td>0.1007</td>
<td>0.0134</td>
<td>0.1573</td>
<td>0.1929</td>
<td>0.0247</td>
<td>0.0004</td>
<td>0.0211</td>
</tr>
<tr>
<td>N</td>
<td>0.0083</td>
<td>0.0027</td>
<td>0.0086</td>
<td>0.0042</td>
<td>0.0094</td>
<td>0.0082</td>
<td>0.0086</td>
<td>0.0388</td>
<td>0.0104</td>
<td>0.0062</td>
<td>0.0353</td>
<td>0.0169</td>
<td>0.0057</td>
<td>0.0831</td>
</tr>
</tbody>
</table>

| Mean | 0.0054 | 0.0010 | 0.0013 | 0.0051 | 0.0185 | 0.0012 | 0.0059 | 0.0636 | 0.0091 | 0.1648 | 0.1128 | 0.0195 | 0.0014 | 0.0224 |
| Rank | 2     | 5     | 7     | 6     | 3     | 12    | 4     | 14    | 13    | 9     | 10    | 11    | 6     | 9     | 10    |
| Med  | 0.0083 | 0.0024 | 0.0086 | 0.0035 | 0.0110 | 0.0086 | 0.0044 | 0.0419 | 0.0081 | 0.0889 | 0.0709 | 0.0173 | 0.0152 | 0.0171 |
| Rank | 6     | 1     | 8     | 7     | 2     | 12    | 4     | 14    | 13    | 11    | 9     | 10    | 6     | 9     | 10    |

| A    | 0.0011 | 0.0092 | 0.0080 | 0.0021 | 0.0079 | 0.0049 |
| B    | 0.0027 | 0.0024 | 0.0072 | 0.0018 | 0.0071 | 0.0017 |
| C    | 0.0052 | 0.0057 | 0.0032 | 0.0025 | 0.0031 | 0.0039 |
| D    | 0.0021 | 0.0046 | 0.0045 | 0.0013 | 0.0044 | 0.0035 |
| E    | 0.0025 | 0.0061 | 0.0056 | 0.0028 | 0.0054 | 0.0035 |
| F    | 0.0054 | 0.0060 | 0.0032 | 0.0025 | 0.0031 | 0.0038 |
| G    | 0.0040 | 0.0032 | 0.0085 | 0.0022 | 0.0085 | 0.0007 |
| N    | 0.0063 | 0.0077 | 0.0086 | 0.0042 | 0.0087 | 0.0056 |
## Interoperable Template Generators and Matchers

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Criterion (s.t. FNMR ≤ 0.01 @ FMR = 0.01)</th>
<th>Value of Criterion</th>
<th>Temp. Gen’s</th>
<th>#</th>
<th>Temp. Matchers</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>POEBVA</td>
<td>group max</td>
<td>0.0087</td>
<td>A,B,C,D,E,F,G,N</td>
<td>8</td>
<td>A,B,C,D,F,G</td>
<td>6</td>
</tr>
<tr>
<td>POEBVA</td>
<td>group mean</td>
<td>0.0094</td>
<td>A,B,C,D,E,F,G,K,L,M,N</td>
<td>11</td>
<td>A,B,C,D,E,F,G,I,L,M,N</td>
<td>11</td>
</tr>
<tr>
<td>DHS2</td>
<td>group max</td>
<td>0.0081</td>
<td>B,D,N</td>
<td>3</td>
<td>A,D</td>
<td>2</td>
</tr>
<tr>
<td>DHS2</td>
<td>group mean</td>
<td>0.0095</td>
<td>B,D,K,N</td>
<td>4</td>
<td>A,C,D,F,G</td>
<td>5</td>
</tr>
</tbody>
</table>
Results 4

• Certification of an interoperable group of products requires some prior specification of the required accuracy.
  – More products will interoperate when the accuracy requirement is low and vice versa.
  – More products can be certified if the group’s mean error rate is below a threshold than if their worst interoperable pair is used for certification.
Results 5

- Performance is sensitive to the quality of the dataset.
  - Applies to both proprietary and interoperable templates.
  - Two higher quality datasets (POEBVA and POE) provide reasonable interoperability. Two lower quality datasets (DOS and DHS2) do not.
For more information

• Contact

Charles Wilson
cwilson@nist.gov
(301) 975-2080
Proprietary and Native Performance
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- **Break**
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- **Interactive Session**
- **Press wrap-up**
NPIVP Labs Preparation & Product Submission for FIPS 201 Compliance

Ramaswamy Chandramouli (Mouli)
mouli@nist.gov
IAB Meeting, March 15, 2006
Topics

- Scope of NPIVP Certification
- Lab Accreditation for PIV Testing
- Certification Process Sequence
- Products under Test
- Anticipated near-term milestones
- Tests under Development
Scope of NPIVP Certification

- **PIV Card Application**
  - For conformance to End-Point Card Application Card Command Interface (Chapter 7 of SP 800-73)

- **PIV Middleware**
  - For conformance to End-Point Client Application Interface (Chapter 6 of SP 800-73)
Lab Accreditation for PIV Testing

- Interim Designation for NPIVP Labs expire in August 2006

- **Lab Accreditation – Tasks and Roles**
  1. Proficiency Assessment – NPIVP Team
     - Proficiency Tests mailed out on Jan 25, 2006
     - Lab submission of Tests due on Mar 15, 2006
     - Complete Review of submissions by Apr 15, 2006
  2. Assessment per ISO/IEC 17025 – NVLAP’s CMVP Team
     - Review of Quality Manuals, Procedures, Records etc
     - CMVP Manual 150-17 will be updated to include the two PIV Tests.
     - Expected Completion Date for Labs Accreditation – 7/31/06
Certification Process Sequence – PIV Card Application

Vendor submits to NPIVP Lab

- Undergoes SP 800-85A Interface Conformance Tests using NIST Toolkit

- NPIVP Interface Validation Certificate – PIV Card Application

- FIPS 140-2 Validation
Certification Process Sequence – PIV Middleware

Vendor submits to NPIVP Lab

Undergoes SP 800-85A Interface Conformance Tests using NIST Toolkit

NPIVP Interface Validation Certificate – PIV Middleware
Products Under Test

PIV Card Application
- 4 Products under Test

PIV Middleware
- 3 Products under Test

Test Status Codes
Certification in Progress
Certification under Review
NPIVP Validated

(Pre-Validation Lists for PIV Components/Sub-Systems)
Anticipated near-term milestones

- **PIV Card Application**
  - Completed Test Reports for 3 products expected by March 17, 2006

- **PIV Middleware**
  - Completed Test Reports for 2 products expected by March 31, 2006
Tests Under Development
(Data Model Format and Content Tests)

• Test Objective and Mechanics
  - Validation of the process/systems that populates the card.
  - Tests are run against data populated on a Card.

• Test Guideline Document (SP 800-85B)

• Scope of Tests
  1. All data for BER-TLV Conformance (Appendix A of SP 800-73)
  2. Format and Content of Biometric Record (SP 800-76)
  3. Format & Content of Digital Signature Blocks (FIPS 201) – covers signed objects such as CHUID, biometric data
Tentative Publication Schedule
(Data Model Format and Content Tests)

• Draft SP 800-85B – April 10th
• Final SP 800-85B – April 28th

Further Info?

Mouli (Ramaswamy Chandramouli) - mouli@nist.gov
Hildy (Hildy Ferraiolo) - hferraio@nist.gov
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- Break
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- Interactive Session
- Press wrap-up
HSPD #12
Document Revision Status

National Institute of Standards and Technology
March 15, 2006
Current Activities

• FIPS 201-1 accommodation of OMB Memorandum M-05-24
• Special Publication 800-73 adjustments to accommodate Special Publication 800-76
• Reformatting of Special Publication 800-85 to separate card command conformance testing from data model conformance testing
• Request to agencies recommendations regarding need revision of FIPS 201-1 and associated guidelines
FIPS 201-1 Accommodation of OMB Memorandum M-05-24

• Provides for interim issuance of credentials based on National Criminal History Check and requires electronic indication of interim issuance on the PIV card.
• FIPS 201-1 signed by the NIST Director and forwarded to DoC for signature.
• Still awaiting signature by the Secretary of Commerce.
Special Publication 800-73
Adjustments to Accommodate
Special Publication 800-76

• Biometric storage format changes
• Incorporation of previously posted errata
• Elimination of requirement to provide user PIN before permitting access to public PKI certificate information
• Public comments received.
• Publication Imminent
Reformatting of Special Publication 800-85

- Separates card command conformance testing from data model conformance testing
- SP 800-85A will be posted on March 17th & SP 800-85B will be posted on April 10th in http://csrc.nist.gov/piv-program.
Revision of FIPS 201-1 and Associated Guidelines

• Request to agencies recommendations regarding need revision of FIPS 201-1 and associated guidelines
  – Need for change
  – Impact on standards stability
  – Priority and schedule determination

• Looking at candidate distribution channels
Agenda

• **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)

• **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)

• **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)

• **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)

• **GSA update on FIPS 201 Evaluation Program** (April Giles)

• Break

• **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)

• **Physical Access Synergy of PAI IWG/SCA/SIA** (Tony Cieri & Team Leads)

• **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)

• **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)

• **Common Handheld Device RFI Vendor Presentation** (Frank Jones)

• Interactive Session

• Press wrap-up
FIPS 201 Evaluation Program

Office of Technology Strategy

April Giles
15 March 2006
Presentation Agenda

- Card/Reader Interoperability Task
- Lab Development Task
- APL Early Applications
- ’s
Card/Reader Interoperability Task

• **Update**
  – 95% complete
  – Test fixture prototype delivered
  – Card/reader requirements on 6\textsuperscript{th} draft
Lab Development Task

• Update
  – 50% complete
  – CONOPS, CM Plan, Approval Procedure Template completed
  – Test Procedure Template completed
  – Marketing Strategy completed
  – 3/17 Categories completed

• Next major milestone
  – Test Fixture update
  – Website tool update
  – New RTM in review
APL Early Applications

- Starting 17 March 06
- Submit applications
  - FIFO
  - Maximum per category
  - Approval process validation
  - Must be flexible
April Giles

Contact information:

Email:  april.giles@gsa.gov

Website:  http://www.smart.gov/fips201apl

Phone:  1.202.501.1123
Agenda

• Winter Fox Exercise Report Out (Winter Fox Team Lead by PFPA/NCR)
• NIST Update on Biometric Support for PIV (Ramaswamy Chandramouli & Elaine Newton)
• NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance (Ramaswamy Chandramouli)
• NIST update on HSPD-12 Document Revision Progress (Curt Barker)
• GSA update on FIPS 201 Evaluation Program (April Giles)

• Break

• Smart Card Alliance (SCA) Conference (Randy Vanderhoof)
• Physical Access Synergy of PAIWG/SCA/SIA (Tony Cieri & Team Leads)
• Backend Authentication Scheme Working Group (BASWG) Update (Tim Baldridge)
• Interagency Partnership Working Group (IPWG) Update (Ron Martin)
• Common Handheld Device RFI Vendor Presentation (Frank Jones)
• Interactive Session
• Press wrap-up
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- Break
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- Interactive Session
- Press wrap-up
Update from Physical Access Council

1. Contributed to new IAB working committee formed to review industry-generated FIPS and PACS documents
2. SP 800-73: The PAC had reviewed and commented on the IBIA and SIA comments
3. Reviewed draft DHS document describing the IDMS to PACS API
4. Review and discussion on GSA proposed card/reader requirements for interoperability performance testing
5. Produced a slide deck on open issues for Physical Access systems and FIPS 201
6. Now holding steering committee elections
Next Event

5th Annual Smart Cards in Government Conference
Sheraton National Hotel, Arlington
April 18 – 20, 2006

• Government Smart Card Conference and Exhibition
• Next IAB Meeting: April 18th 9:00 until 12:00 + lunch
• Topics include: HSPD 12, ePassport, Registered Traveler, REAL ID, First Responder, Western Hemisphere Traveler
• Two Tracks: Technology and Implementation & Policy
• 40 exhibitors
• Pre-conference FIPS 201 Implementation Workshop

Fees:
• Government Rate =
  – Combo 4 Day - $875, 3 Day Conf - $595, 1 Day Conf - $295
• Non Government Rate =
  – Combo 4 Day - $1125, 3 Day Conf - $795, 1 Day Conf - $395
• Members Rate =
  – 3 Day Conf 1st member - no charge, each add’l member $545

For info, visit www.smartcardalliance.org
FIPS 201 Implementation Workshop

Pre-conference Workshop – Monday April 17th
Sheraton National Hotel, Arlington, VA

• Full day tutorial presented by Smart Card Alliance
• Addresses the major technical and policy issues from an industry perspective facing federal agencies in implementing FIPS 201
  – PIV Card Requirements
  – PIV Data Elements and Mandatory Components
  – Biometrics and Enrollment
  – ID Management and Card Issuance
  – PIV Applications for Physical and Logical Access
  – Implementation Best Practices and Management

• Registration open to government and industry
  – See Next Event information at www.smartcardalliance.org for further details
For More Information

• **Physical Access Council**
  – Bob Merkert, SCM Microsystems, Council Chair - rmerkert@scmmicro.com
  – Dwayne Pfeiffer, Northrop Grumman, Council Vice Chair - dwayne.pfeiffer@ngc.com
  – Steve Rogers, Integrated Engineering, Council Secretary - steve@smart-id.com

• **Smart Card Alliance**
  – Randy Vanderhoof, rvanderhoof@smartcardalliance.org
  – Cathy Medich, cmedich@smartcardalliance.org

www.smartcardalliance.org
1-800-556-6828
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- **Break**
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- **Interactive Session**
- **Press wrap-up**
Physical Access Synergy of PAIIWG/SCA/SIA

Tony Cieri & Team Leads
Background/Status

• Work Group- PAILWG/SCA/SIA
• SIA Understanding Background and Documentation
• Meeting with GSA/NIST
• SIA Analysis
• Work Continues- More Comprehensive Report at Next IAB
PACS Installed Base Assessment

125kHz Prox
Mag Stripe
Other

Other
Magnetic Stripe 16 digits

Upgrade Or Replace

37 bit Wiegand For 32 bit Mifare Cards
37 bit Wiegand w/ Facility Code 19 Data Bits
26 bit Wiegand w/ Facility Code 16 Data Bits

Notes:
This process represents some of the more common evaluation checks. It is not a complete list. Each PACS is unique and must be uniquely evaluated.
A Facility Code is a data field (typically 8 bits) resident on the card and in the PACS controller, assigned by the supplier, that must match in order to grant access. It is often hard coded into the controller and prevents card interoperability.
The first 3 fields of the FASC-N are specified to be 14 digits. Most PACS controllers receive data in bits. The minimum number of bits to represent a unique 14 digit number is 47. The most common card/controller formats are 26 bit Wiegand (16 data bits), 37 bit Wiegand (19 data bits), and 32 bit Wiegand.
Card Validation Checks include Expiration Dates, HMAC and other data fields on the card. Conventional PACS store the Expiration Date in the PACS controller and do not support parsing out a field in the data stream from the card for this check. Many of the PIV requirements, especially the longer bit lengths of the card number, will consume greater memory in the PACS controller. This can reduce the card capacity of the controller. Interoperability may also increase card capacity requirements. Many PACS controllers have limited or no memory expansion capability.
Agenda

- Winter Fox Exercise Report Out (Winter Fox Team Lead by PFPA/NCR)
- NIST Update on Biometric Support for PIV (Ramaswamy Chandramouli & Elaine Newton)
- NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance (Ramaswamy Chandramouli)
- NIST update on HSPD-12 Document Revision Progress (Curt Barker)
- GSA update on FIPS 201 Evaluation Program (April Giles)
- Break
- Smart Card Alliance (SCA) Conference (Randy Vanderhoof)
- Physical Access Synergy of PAILWG/SCA/SIA (Tony Cieri & Team Leads)

• Backend Authentication Scheme Working Group (BASWG) Update (Tim Baldridge)

• Interagency Partnership Working Group (IPWG) Update (Ron Martin)
• Common Handheld Device RFI Vendor Presentation (Frank Jones)
• Interactive Session
• Press wrap-up
Backend Authentication Work Group (BAS) WG: IAB Update

15 March 2006
Tim Baldridge, BAS WG co-chair
IAB BAS WG Task

Challenge #1: Other Federal Agency Visitors
- FIPS 201 (section 6.2) requires card issuers to provide the capability for credentials to be authenticated by other Federal Agencies

Challenge #2: Electronic Way to Review NACI Status of Visitors
- M-05-06 Identity Credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable form identity credentials issued to individuals who have a completed investigation. (Will be in FIPS 201-1)
- NACI status may indicate incomplete at PIV issuance
- How is visitor NACI complete status verified
The Unassigned Task

• Determination of Trustworthiness
  – PIV II Cards with Biometric verification determine the low watermark for validation of Federal Personnel
  – Many Agencies have a demonstrated requirement for additional information from the PCI for a specific visitor to determine suitability of the visitor for a requested access
Focus of BAS WG Efforts

BAS WG has identified four areas to this challenge:

1. Ability to Authenticate and validate PIV Credentials of Visitors
2. Ability to take information obtained from Authenticating Visitors or backend PIV infrastructure and registering this information within the Local Physical Access Systems
3. Ability to verify and authorize PIV Cardholders during daily use within the Local Physical Access System
4. Ability for Backend PIV infrastructure to make available information on changes in card validity (e.g. terminations, lost/stolen, etc..) of PIV cardholders

The Group must minimally address #1 and #4
Approaches

- Government members of the BAS WG detailed two approaches
  1. Gateway Approach (proposed by DoD)
  2. OCSP Approach (proposed by NIST)

- The next series of slides outlines the use case scenarios for each proposal to meet “focus areas” #1 and #4.
PIV Backend Authentication Scheme—FD #1 (OCSP Approach)

*Assumes the PIV issuing authority is link to Agencies PKI in virtual real-time.
PIV Backend Authentication Scheme—FD #1 (Gateway Approach)

- **Issuing Authority**
- **PIV Cardholder**
  - Visual Auth
  - PIN Auth
  - PKI Auth
- **Web Authentication Station**
- **Other Federal Agencies**
  - PIV Status
  - NACI Status
  - Facial Image
  - Biometric Match Results
  - Other
- **Federated Backend Gateway**
- **Agency Backend Gateway**
  - CHUID
- **Optional**

---

**Key**

- Optional

---

**CHUID**
PIV Backend Authentication Scheme—FD #4 (Gateway Approach)

Other Federal Agencies

Federated Backend Gateway

Lost, Stolen, & Terminated Card list

Agency Backend Gateway

Physical Access Control System

Issuing Authority

PIV Cardholder
PIV Backend Authentication Scheme—FD #4 (OCSP Approach)

*Assumes the PIV issuing authority is link to Agencies PKI in virtual real-time.
Status

• Industry Review (began Tuesday, Feb 28)
  – Conducted conference call with approximately 35-45 Industry participants
  – The Government members work was presented
  – Industry provide ONLY 3 sets of comments on proposed approaches

• Final Recommendations (target: April IAB)
  – Government members will review Industry recommendations to decide which approach to recommend to the full IAB.
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- Break
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAILWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- Interactive Session
- Press wrap-up
COLLABORATION

Ron Martin, CPP
Components of Collaborative Process

Identity Management is a broad capability and requires an integrated solution

- Defining functional/business requirements
- Defining Business Architecture
- Determining budget requirements
- Reviewing policies
- Creating new policies where needed

- Determining laws, regulations, mandates to be followed
- Policy, Planning, Politics and Management

80%

- Hardware/Software
- Storage
- Entity Management
- Credentialing
- Access Management
- Application Integration
- Facilities

20%

NT + OP = EOP

Technology
Collaboration

226 Days to Implementation

- X – 30 days C&A Process (196)
- X – 60 Days Adapt process and systems (136)
- X – 90 Days Policy alignments (46)

IPWG transition to IAB

- Draft policy documents
- Draft Trusted Agent Program
- SP 800-79 C&A Program Model
- Background-Suitability Services
- GSA Organizational Overviews
- IDMS defined
HSPD – 12

Resistance is Futile!

LOGICAL & PHYSICAL ACCESS WILL BE ASSIMILATED INTO THE SMART CARD!
Agenda

- **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
- **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
- **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
- **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
- **GSA update on FIPS 201 Evaluation Program** (April Giles)
- Break
- **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
- **Physical Access Synergy of PAlIWG/SCA/SIA** (Tony Cieri & Team Leads)
- **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
- **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
- **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
- Interactive Session
- Press wrap-up
Common Handheld Device RFI Vendor Presentation

Frank Jones

DMDC
• **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
• **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
• **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
• **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
• **GSA update on FIPS 201 Evaluation Program** (April Giles)
• **Break**
• **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
• **Physical Access Synergy of PAIIWG/SCA/SIA** (Tony Cieri & Team Leads)
• **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
• **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
• **Common Handheld Device RFI Vendor Presentation** (Frank Jones)

**Interactive Session**

• **Press wrap-up**
Interactive Session

- What do agencies intend to have on their cards and what type of card do they intend to issue on 27 October 2006?

- Will agencies be ready to comply with OMB 05-24?
Will agency plans comply with OMB 05-24?

• October 27, 2005:
  A. Adopt and accredit a registration process
  B. Initiate NACI or other suitability or national security investigation prior to credential issuance
  C. Include language implementing Standard in applicable new contracts

• October 27, 2006:
  A. Issue and require use of identity credentials for all new employees and contractors
  B. Implement technical requirements of Standard
  C. Risk based facility access
  D. Use of digital certificates

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
   Director

• **Winter Fox Exercise Report Out** (Winter Fox Team Lead by PFPA/NCR)
• **NIST Update on Biometric Support for PIV** (Ramaswamy Chandramouli & Elaine Newton)
• **NIST update on Labs Preparation and Product Submissions for FIPS-201 Compliance** (Ramaswamy Chandramouli)
• **NIST update on HSPD-12 Document Revision Progress** (Curt Barker)
• **GSA update on FIPS 201 Evaluation Program** (April Giles)
• Break
• **Smart Card Alliance (SCA) Conference** (Randy Vanderhoof)
• **Physical Access Synergy of PAILWG/SCA/SIA** (Tony Cieri & Team Leads)
• **Backend Authentication Scheme Working Group (BASWG) Update** (Tim Baldridge)
• **Interagency Partnership Working Group (IPWG) Update** (Ron Martin)
• **Common Handheld Device RFI Vendor Presentation** (Frank Jones)
• Interactive Session
  • **Press wrap-up**
Press Wrap-up