# Federal Public Key Infrastructure Policy Authority (FPKIPA)

## Minutes of the 13 March 2007 Meeting

GSA National Capital Region, 7th and D Streets, SW, Washington, DC.
Room 5700

A. AGENDA

1. Welcome / Introductions
2. Discussion/Vote on 13 February FPKIPA Minutes
3. Results of FBCA CP Change Proposal: 2007-01 E-vote
4. FPKIPA Charter Update
5. Microsoft CA Support for SHA-256
6. FBCA CP Citizenship Requirement
7. FPKI Operational Authority (FPKI OA) Report
    1) Status of FBCA/Applicant Cross-Certification Technical Testing
    2) MIT LL Interoperability Testing Status
    3) USPS
    4) DoD ECA
    5) New OA Contractors/Project Scope Change
8. Discuss Updated FBCA and C4CA Criteria and Methodology
9. Status of DoD Two-Way Cross Certification Activities
10. Update on SSPWG Activities
11. FPKI Certificate Policy Working Group (CPWG) Report
12. Audit Working Group Status Update
13. Final Meeting Items
    1) Other Topics
        i. Proposed Agenda Items for April 10, 2007
        ii. Personnel Changes at NIST
        iii. Device Certs Memo
        iv. First Responders Access Credentials (*GCN* article)
14. Adjourn Meeting

**B. ATTENDANCE LIST**

### VOTING MEMBERS

A quorum of nine (9) voting members (plus two proxies) was present of thirteen (13) voting members, or 84.6% where a quorum of two-thirds (2/3) was required.

NOTE: Contact information has been removed at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members only at some point in the future. FPKIPA minutes already posted on the website have been redacted to remove POC

information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at Judith.fincher@enspier.com.

| Organization | Name | Email | Telephone |
|---|---|---|---|
| Department of Commerce (NIST) | Polk, Tim | | |
| Department of Defense | Mitchell, Deborah | | |
| Department of Health & Human Services | Alterman, Peter, Ph.D. | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | Morrison, Scott | | |
| Department of State | Caldwell, Sally | | |
| Department of the Treasury | Proxy to NASA per phone call to Chair | | |
| Drug Enforcement Agency (DEA CSOS) | Absent | | |
| GPO | Hannan, John | | |
| GSA | Temoshok, David | | |
| NASA | DeYoung, Tice, Ph.D. | | |
| USPS | Stepongzi, Mark | | |
| USPTO | Proxy to HHS | | |

## OBSERVERS

| Organization | Name | Email | Telephone |
|---|---|---|---|
| SSA (Contractor – -Jacob & Sundstrom) | Simonetti, David | | Teleconference |
| DHS (Contractor – CignaCom) | Shomo, Larry | | Teleconference |
| FPKI OA PM/GSA | Jenkins, Cheryl | | |
| FICC/GSA | Spencer, Judith | | |
| Department of State (Contractor -- ManTech) | Froehlich, Charles R. | | |
| Wells Fargo | Drucker, Peri | | Teleconference |
| FPKI/FICC Support (Contractor--General Dynamics Information Technology) | Petrick, Brant | | |
| FPKIPA Secretariat (Contractor --Enspier Technologies/Protiviti Government Services) | Fincher, Judy, Ph.D. | | |
| Orion | Chokhani, Santosh | | Teleconference |
| NIST (CPWG Co-Chair) | Cooper, Dave | | Teleconference |
| KPMG | Faut, Nathan | | |
| KPMG | Spell, Timothy | | |
| E-Authentication PMO | Marsh, Georgia | | Teleconference |
| E-Authentication PMO | Frazier-McElveen, Myisha | | Teleconference |
| IdenTrust | Young, Kenny | | |
| IdenTrust | Jensen, Curtis | | |
| IdenTrust | Corbo, Page | | |
| US Nuclear Regulatory Commission (NRC) | Sulser, David | | |
| USPS | Voss, Larry | | |
| Joint Staff (J6) | Watson, Leatrice | | Teleconference |

| Organization | Name | Email | Telephone |
|---|---|---|---|
| SSA (Contractor – -Jacob & Sundstrom) | Simonetti, David | | Teleconference |
| DHS (Contractor – CignaCom) | Shomo, Larry | | Teleconference |
| Enspier/Protiviti Government Services (Contractor) | Farrales, Treb | | Teleconference |

## C. MEETING ACTIVITY

### Agenda Item 1

### Welcome / Introductions—Dr. Peter Alterman

This meeting was held at GSA National Capital Region Building, 7th and D Street, SW, Washington, DC. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:42 a.m. with the attendee roll call. Dr. Alterman noted that Art Purcell of the USPTO has retired and presented him with a Certificate of Appreciation on behalf of the members of the Policy Authority. Mr. Purcell thanked the Policy Authority and treated the FPKIPA members and observers to coffee and pastries.

### Agenda Item 2

### Discussion/Vote on 13 February 2007 FPKIPA Minutes—Judy Fincher

Judy Fincher said that she had received no comments on the minutes five business days prior to the meeting, and so had sent out the minutes with the agenda and other attachments.

Due to the fact that one voting member had not received the minutes (due to a listserv problem), the vote was postponed, and an e-vote will be taken. At that time, comments of an editorial nature, which were received after the deadline, will be incorporated.

### Agenda Item 3

### Results of the FBCA CP Change Proposal: 2007-01 E-vote—Judy Fincher

Ms. Fincher reported that the FBCA CP Change Proposal: 2007-01 was approved by the e-vote that concluded 3/9/07. Those agencies voting to approve included the following: HHS, DHS, GPO, Treasury, NASA, DOS, USPS, Commerce, Justice, and GSA. DoD voted "No." Eleven of the 13 voting members (a quorum) responded to the e-vote request. Of the number who comprised the quorum, ten (10) voted "yes," or 90.9%, where a 75% majority vote was required.

ACTION: Dr. Peter Alterman will digitally sign the updated FBCA CP and Brant Petrick will post the 2007-01 Change Proposal and the updated FBCA CP to the website.

## Agenda Item 4

### FPKIPA Charter Update—Dr. Tice DeYoung

It was agreed to discuss changes to the Charter at the April 5, 2007 CPWG meeting.

## Agenda Item 5

### Microsoft CA Support for SHA-256—Tim Polk

Tim Polk prepared a PowerPoint presentation for this session on the issue of client support for SHA-256.

ACTION: Tim Polk will send his presentation on SHA-256 to the listserv.

He summarized his slides during the meeting. Eighty-bit encryption is mostly dead, he argued. The concern at NIST is that the agencies are not migrating to higher cryptographic strength fast enough. They need to be aggressive and proactive. They need to migrate, but this is fraught with difficulties. You will break things when migrating, he said. All objects have a lifetime when you must quit trusting the protection afforded by the cryptography.

He urged Policy Authority members to go to the website: www.keystrength.com to find the projected expiration dates for common cryptographic technologies, such as RSA 1024, Diffie-Hillman, and SHA-1 for digital signatures. Academic cryptographic experts maintain that 80-bit cryptographic algorithms are already dead—due to professional attacks from foreign intelligence services.

NIST's projection is that 80-bit cryptography will be really dead by the early 2010s. January 1, 2011 is the phase out date for 80-bit cryptography.

This means all certs will have to use SHA 256 and RSA 2048 by December 31, 2010, he said.

Conversely, he said, there is a strong case against migration due to the installed WIN 98 base (legacy equipment) in DoD and other agencies.

Mr. Polk said that PIV card users should migrate to RSA 2048 now. Contracts need long-term non-repudiation now. Migration to SHA-256 will be more painful.

Windows XP doesn't support SHA-256 and there is no answer from Microsoft as to when it will. Windows XP supports RSA 2048. VISTA supports SHA-256 and RSA 2048, he said.

ACTION: Dr. Alterman will organize an SHA-256 migration workshop this year.

Mr. Polk stated that it is easy to migrate CAs to 2048-bit keys even if you can't migrate to SHA-256 at the same time. The two are not linked, he said. Most people are already using SHA-1 and RSA 2048-bit keys, he said.

Mr. Polk said that by 1 January 2011 all agencies should be using SHA-256 on all digital signatures. Therefore, 3-year certs need to migrate by the end of this year.

Santosh Chokhani discussed using self-signed certs as trust anchors. In this out-of-band scenario, signatures are not meaningful. They are merely cryptographic check sums.

Mr. Polk said the best strategy is to buy time by issuing two year certs until January 1, 2009, then issue 2048-bit keys with SHA-1.

Tim Polk said he was meeting at IETF next week with Microsoft and hoped to get an answer regarding Windows XP supporting SHA-256.

ACTION: Tim Polk is to present his slide presentation on SHA-256 migration to the HSPD-12 Executive Steering Committee (ESC).

David Temoshok suggested that Tim Polk draft a White Paper on SHA-256 migration that could be disseminated widely through the government.

ACTION: David Simonetti will share his White Paper on the migration from SHA-1 to SHA-256--written for the SSA--with Tim Polk. (Done, 3/13/07)

Debbie Mitchell raised the issue of jumping directly to ECC to promote interoperability with the rest of the federal community. Tim Polk said that ECC is the "better technology" in the end, but that there are licensing problems. If we can't migrate to ECC before 2015, that leaves us vulnerable for five years, he said.

Putting off an easy transition to make a hard leap is not feasible. Waiting seven or eight years is a high risk, he said. There are no painless answers

and there are hard decisions to be made. Platform migration may be required.

ACTION: Dr. Alterman will sponsor a team meeting with the vendors and involve Judy Spencer, Tim Polk, and Dave Cooper.

Microsoft needs to back port SHA-256 and ECC Suite B to Windows XP, Mr. Polk said. We can't use it until we have someone to talk to, he said.

## Agenda Item 6

### FBCA CP Citizenship Requirement—Dr. Peter Alterman, Judith Spencer

Dr. Alterman reported on a series of meetings held between the FPKI/NIST staff, DoD and CertiPath. CertiPath's European customers, notably BAE Systems and Airbus, are urging the use of security clearances for trusted roles in lieu of the citizenship requirement for Medium and Medium Hardware. Dr. Alterman and Judith Spencer are drafting a Change Proposal with alternative language to propose the use of NATO-recognized security clearances instead of the citizenship requirement. If DoD agrees, this will be a policy change. DoD's attorneys are looking at US Government bi-lateral agreements regarding security clearances. DoS, DOE, NASA and DoJ are also interested. He expects this to come before the Policy Authority this year.

These customers do not want to use the Commercial Best Practice (CBP) policy because they are afraid some US federal agencies will not accept CBP policy certs from them.

## Agenda Item 7

### FPKI Operational Authority (FPKI OA) Report—Cheryl Jenkins

1) Status of FBCA/Applicant Cross-Certification Technical Testing

   Ms. Jenkins said that MIT LL and ECA are currently doing technical testing.

2) MIT LL Interoperability Testing Status
   She expects to set up the directory and set up certs with them this week.

   ACTION: Once the MIT LL interoperability testing is completed, Ms. Jenkins will send the interoperability report to Judy Fincher for an e-vote.

3) USPS

The FPKI OA is waiting on a Letter of Authorization (LOA) before it can cross certify with USPS. There are remaining policy issues (e.g., name space) that must be resolved before Dr. Alterman can issue the LOA.

4) DoD ECA
The FPKI OA is having discussions with DoD regarding the use of the AIA extension. We need the AIA extension field in the cross-cert, she said.

5) New OA Contractors/Project Scope Change
Ms. Jenkins noted that the protest had been overturned and that Enspier/Protiviti Government Services is the new FPKI OA contractor. Enspier will be operating jointly with Mitretek (now Noblis) until May 31, 2007. The Project Lead is Tim Pinegar and the Technical Lead is Steve Matney.

The protest changed the schedule. The re-design and the ISO 27001 ISMS will slip to FY08. The goal is to maintain the ATO, which expires on 30 June 2007, she said.

The new team will roll out a patch in the late March-early April timeframe to stop the memory leak in the directory. This memory leak is what has been causing intermittent directory outages. We are monitoring the directory now and this will continue. We will tweak the tool to the PCA of each cross-certified entity, she said.

ACTION: Judith Spencer, Cheryl Jenkins, and Dr. Alterman will meet with the E-Auth PMO to discuss directory issues and avoid duplication of efforts.

ACTION: Cheryl Jenkins will post the new FPKI OA support contract project lead information to the listserv.

## Agenda Item 8

**Discuss Updated FBCA and C4CA Criteria and Methodology—Judith Spencer, Dr. Peter Alterman**

Dr. Alterman said that a CPWG editing committee has extensively revised the FBCA Criteria and Methodology document. It will be sent out for review and we plan to vote on it next month, he said.

ACTION: Judy Fincher is to send out the revised FBCA and C4CA Criteria and Methodology document to the FPKIPA listserv on 3/14/07 for a vote at the April 10, 2007 meeting. (Done)

## Agenda Item 9

### Status of DoD Two-Way Cross Certification Activities

Debbie Mitchell submitted an update to the FPKIPA listserv prior to the meeting via e-mail and described the major activities during the meeting. DoD is finalizing discussions on Certificate extensions and modifications to DoD Cert profiles (AIA, SIA, CRL distribution point). DoD may re-point to the Global Directory Service, she said. There have been changes to the CPS and the CP has been upgraded to Medium Hardware. It is in the signature process. She noted that some changes to the infrastructure might be required.

She continues to provide monthly updates to the Policy Authority, until such time the DoD is two-way cross-certified.

## Agenda Item 10

### Update on SSPWG Activities—Judith Spencer

Ms. Spencer said she is doing a final scrub of the revised Common Policy and expects to introduce it at the next Policy Authority meeting.

ACTION: Judith Spencer will send out the revised Common Policy to the FPKIPA listserv and to the vendors.

The largest remaining item to handle are the changes that will need to be made to the Common Policy if OMB does not give legacy PKIs relief on the FIPS 201 requirement to express the Common Policy OIDs by January 1, 2008.

OMB has requested that Ms. Spencer update the existing memo from the Policy Authority to describe what the impact will be (cost and infrastructure changes) if the FIPS 201 is not revised to give relief to the federal legacy PKIs. She and Tim Polk are writing the update this week. She received input from both DoD and DoS to draft the impact analysis section of the revised memo.

## Agenda Item 11

### FPKI Certificate Policy Working Group (CPWG) Report—Tim Polk

Tim Polk said the last three meetings of the CPWG had been devoted to the SAFE Bridge bi-directional mapping and that the CPWG is meeting with representatives from SAFE on March 15 to discuss our comments on their mapping of us and our mapping of them.

## Agenda Item 12

**Audit Working Group Status Update—Dr. Peter Alterman**

During the past year, the Audit WG has been working to rationalize the IT security audit requirements. Dr. Alterman funded two activities to map the FBCA CP to the NIST SP 800-53 security controls; and, to map the 800-53 controls to the FBCA CP. The initiative was to determine what portion of 800-53 requirements are met (or not met) in the annual PKI audit against the FBCA CP.

This comparison of the FBCA CP against the security controls in NIST SP 800-53 (Moderate level) will provide commercial entities with guidance to enable their PKI audits to more closely align with the security requirements FISMA imposes for federal agencies.

ACTION: Dr. Alterman will send out a memo to the FPKI Policy Authority and non-federal cross-certified members with the FBCA to NIST SP 800-53 mapping tables attached. This memo will make a compelling case that the annual audit agencies perform will satisfy a certain portion of the 800-53 requirements, saving time and money in performing the annual PKI audits (or delta audits).

Dr. Alterman is also funding a further refinement of the mapping tables to include the mapping to ISO 27001 (ISMS). He has contracted with Richard Wilsher to map the FBCA CP and SP 800-53 to ISO 27001 before 30 June 2007. This will go a long way towards meeting the ISO System Security requirements and will help as we move into the international security environment.

## Agenda Item 13

**Final Meeting Items**

- **Other Topics**
  - **Proposed Agenda Items for April 10, 2007**
    - DoD Two-Way Cross-Certification Update
    - Vote on the revised Crits and Methods
    - Review the revised Charter
    - Review the revised Common Policy
  - **Personnel Changes at NIST**
    The FPKI Policy Authority also congratulated Tim Polk on his new post as Area Director for Security for the IETF. This is an 80% time commitment, which means that Dr. Dave Cooper will handle the day-to-day PKI NIST support. Tim Polk described other personnel changes occurring at NIST. Kurt Barker, the

Division Chief for Security, is leaving the end of April and Bill Burr has delayed his departure until the end of the year and will be the group leader for security. Donna Dotson is Acting Division Chief.

- **Device Certs Memo**
  This memo was discussed at last month's Policy Authority meeting and members agreed at the 13 March meeting that it does not require a vote because it is not a policy. Brant Petrick will post it to the website once he receives the clean copy from Judy Fincher (Done, 3/19/07).

- **First Responders Access Credentials (*GCN* article)**
  Debbie Mitchell reported that the *GCN* has an article saying that the State of Pennsylvania is issuing HSPD-12 "compliant" credentials for access control. See http://www.gcn.com/online/vol1_no1/43272-1.html.

  ACTION: Dr. Alterman will send a letter to the POC for the State of Pennsylvania, the POC for VeriSign and to the *GCN* with a cc: to Judy Fincher explaining that the State of Pennsylvania is not issuing HSPD-12 "compliant" credentials, but credentials that are "compatible."

## Agenda Item 14

**Adjourn Meeting**

**The meeting adjourned at 12 noon.**

## CURRENT ACTION ITEMS

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 189 | We need to revise the MOA to accommodate E-Auth Federation requirements. Defer to after the E-auth PMO changes the Legal and Business Rules. | Peter Alterman, John Cornell, Georgia Marsh (or PMO rep) | 20 July 2006 | 31 Jan. 2007 | **Open** |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 193 | Dr. Peter Alterman and the head of the OA will negotiate terms for the cross-certification process and add this language to the By-Laws document. This will be brought to the Policy Authority for a vote. (To coincide with Action Item # 189). | Dr. Peter Alterman, Cheryl Jenkins | 10 Jan. 2006 | Oct.-Nov. 2006 | **Open** |
| 212 | Ms. Cheryl Jenkins is to develop an Approach to Application Testing for PD-Val. | Cheryl Jenkins | 14 March 2006 | 8 Aug. 2006 | Open |
| 234 | The SSP re-write committee headed by Dr. Peter Alterman will create a new section 4 of the Crits and Methods (C&M) document for SSPs. This will bleed into the FPKIPA Charter and By-Laws. Dr. Alterman said the C&M re-write will be analogous to what we did with ACES, i.e., we ask for their bona fides: memo of application, 800-79 compliance statement, and audit summary. | Peter Alterman, Rebecca Nielsen et al | 11 July 2006 | 31 Jan. 2007 | Open |
| 237 | Dr. Alterman and Steve Duncan will talk about how the migration of FPKI agencies to Medium Hardware will affect the ACES agencies. | Peter Alterman, Steve Duncan | 8 August 2006 | 12 Sept. 2006 | Open |
| 246 | Dr. Alterman will write a White Paper on why we want to cross certify with SAFE, the pharmaceutical bridge. | Peter Alterman | 12 Sept. 2006 | 10 Oct. 2006 | Open |
| 253 | Dr. Alterman and/or the CPWG are to call a special meeting of the Legal and Policy Working Group to explore supporting PKI applications. | Peter Alterman, Tim Polk | 12 Sept. 2006 | 10 Oct. 2006 | Open |
| 254 | Dr. Peter Alterman authorized the Secretariat (Judy Fincher) to conduct an e-vote on the MIT Lincoln Laboratory interoperability report when issued. | Judy Fincher | 14 Nov. 2006 | 31 Jan. 2007 | Open |
| 255 | Dr. Peter Alterman asked that all member agencies and cross-certified entities fix their certificate profiles | All cross-certified entities | 14 Nov. 2006 | 12 Dec. 2006 | Open |
| 258 | Debbie Mitchell will add a task to the DoD schedule that addresses the new MOA. | Debbie Mitchell | 12 Dec. 2006 | 9 Jan. 2007 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 259 | Debbie Mitchell will forward policy statements to the FPKI PA for review when available. | Debbie Mitchell | 12 Dec. 2006 | 9 Jan. 2007 | Open |
| 260 | Debbie Mitchell will confirm who will perform the C&A of the DoD root and notify the FPKI PA via email. | Debbie Mitchell | 12 Dec. 2006 | 9 Jan. 2007 | Open |
| 262 | Dr. Alterman will send a friendly e-mail, urging DoJ to keep its PKI. | Peter Alterman | 9 Jan. 2007 | 19 Jan. 2007 | Open |
| 267 | John Cornell is to review the MOA template in light of E-Authentication PMO pressures. | John Cornell | 9 Jan. 2007 | 31 Jan. 2007 | Open |
| 272 | Cheryl Jenkins will provide a weekly update on the MIT LL interoperability testing status to Dr. Alterman. | Cheryl Jenkins | 13 Feb. 2007 | 20 Feb. 2007 | Open |
| 273 | An e-mail from Cheryl Jenkins to the FPKIPA listserv explaining how to receive certs from the re-keyed prototype bridge is needed. | Cheryl Jenkins | 13 Feb. 2007 | 20 Feb. 2007 | Open |
| 274 | Dr. Peter Alterman will digitally sign the updated FBCA CP and Brant Petrick will post the 2007-01 Change Proposal and the updated FBCA CP to the website. | Dr. Peter Alterman, Brant Petrick | 13 March 2007 | 19 March 2007 | Closed |
| 275 | Once the MIT LL interoperability testing is completed, Ms. Jenkins will send the interoperability report to Judy Fincher for an e-vote. | Cheryl Jenkins, Judy Fincher | 13 March 2007 | 30 March 2007 | Open |
| 276 | Judith Spencer, Cheryl Jenkins, and Dr. Alterman will meet with the E-Auth PMO to discuss directory issues and avoid duplication of efforts. | Judith Spencer, Cheryl Jenkins, Dr. Alterman, Georgia Marsh | 13 March 2007 | 30 March 2007 | Open |
| 277 | Cheryl Jenkins will post the new FPKI OA support contract project lead information to the listserv. | Cheryl Jenkins | 13 March 2007 | 30 March 2007 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 278 | Judith Spencer will send out the revised Common Policy to the FPKIPA listserv and to the vendors. | Judith Spencer | 13 March 2007 | 23 March 2007 | Open |
| 279 | Dr. Alterman will send out a memo to the FPKI Policy Authority and commercial cross-certified members with the FBCA to NIST SP 800-53 mapping tables attached. This memo will make a compelling case that the annual audit agencies perform will satisfy a certain portion of the 800-53 requirements, saving time and money in performing the annual PKI audits (or delta audits). | Dr. Peter Alterman | 13 March 2007 | 31 March 2007 | Open |
| 280 | Dr. Alterman will send a letter to the POC for the State of Pennsylvania, the POC for VeriSign and to the GCN with a cc: to Judy Fincher explaining that the State of Pennsylvania is not issuing HSPD-12 credentials, but credentials that are "compatible." | Dr. Peter Alterman | 13 March 2007 | 23 March 2007 | Open |
| 281 | Tim Polk will send his presentation on SHA-256 to the listserv. | Tim Polk | 13 March 2007 | 5 April 2007 | Open |
| 282 | Dr. Alterman will organize an SHA-256 migration workshop this year. | Dr. Peter Alterman | 13 March 2007 | Sept. 2007 | Open |
| 283 | Tim Polk is to present his slide presentation on SHA-256 migration to the HSPD-12 Executive Steering Committee (ESC). | Tim Polk | 13 March 2007 | May 2007 | Open |