Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 10 April 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 March 2007 FPKIPA Minutes
3. Results of the E-vote on MIT LL Interoperability Testing
4. Discussion / Vote on the Criteria and Methodology document
5. FPKI Operational Authority (FPKI OA) Report
    1) Status of FBCA/Applicant Cross-Certification Technical Testing
    2) MIT LL Interoperability Testing Status
    3) USPS Update
    4) FPKI OA Statistical Report
    5) New OA Contractors/Project Scope Change
6. Status of DoD Two-Way Cross-Certification Activities
7. Update on SSPWG Activities
8. FPKI Certificate Policy Working Group (CPWG) Report
    1) Discuss SAFE Bridge Mapping
    2) Vote to Extend Wells Fargo Provisional Basic Cross-Certificate
9. Final Meeting Items
    1) Other Topics
        i. Rewrite of the C4CA CP
        ii. Status of revised FPKIPA Charter
        iii. FPKI Audit Working Group
        iv. NRC
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

A quorum of ten (10) voting members was present of thirteen (13) voting members, or 77%, 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)	Absent		
Department of Defense	Mitchell, Deborah		Teleconference
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	Schminky, Jim		
Drug Enforcement Agency (DEA CSOS)	Jewell, Chris		Teleconference
GPO	Hannan, John		

Organization	Name	Email	Telephone
GSA	Temoshok, David		
NASA	DeYoung, Tice, Ph.D.		Teleconference
USPS	Stepongzi, Mark		
USPTO	Absent		

OBSERVERS

Organization	Name	Email	Telephone
eValid8 Corporation	Dilley, Brian		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.		
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant		
FPKIPA Secretariat (Contractor --Enspier Technologies/Protiviti Government Services)	Fincher, Judy, Ph.D.		
E-Authentication PMO	Marsh, Georgia		Teleconference
E-Authentication PMO	Frazier-McElveen, Myisha		
IdenTrust	Jensen, Curtis		Teleconference
US Nuclear Regulatory Commission (NRC)	Sulser, David		
USPS	Weaver, Bill		Teleconference
State of Illinois	Anderson, Mark		Teleconference
Enspier/Protiviti Government Services (Contractor)	Pinegar, Tim		Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman

This meeting was at the GSA National Capital Region Building (7th and D Streets, SW) in Washington, DC. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:40 a.m. with the attendee roll call. Brant Petrick acted as FPKIPA Secretary due to the sudden illness of Ms. Fincher.

Agenda Item 2

Discussion / Vote on 13 March 2007 FPKIPA Minutes—Dr. Peter Alterman

Dr. Alterman asked if all members had ample time to review the minutes (with no objections), and then requested a vote by the FPKIPA members.

Dr. DeYoung from NASA made the motion to accept the minutes, and Ms. Sally Caldwell from DoS second the motion. The following agencies voted to approve the minutes: GSA, GPO, USPS, DoJ, HHS, NASA, DoD, DEA, Treasury, and DoS. The following agencies were absent: DOC, DHS, and

USPTO. Ten of the thirteen voting members (a quorum) voted “yes”, or 77%, where a majority vote was required.

These “approved” meeting minutes will be posted to the FPKIPA website by COB tomorrow.

Agenda Item 3

Results of the E-vote on MIT LL Interoperability Testing—Dr. Peter Alterman

The e-vote on the MIT LL interoperability testing has been temporarily postponed until the FPKI OA finishes testing with MIT LL, prepares the report, and emails it to the FPKIPA members (refer to agenda item #5).

Agenda Item 4

Discussion / Vote on the Criteria and Methodology document—Dr. Peter Alterman

The main changes to the revised FBCA/C4CA Criteria and Methodology document: we added another requirement to the mapping process, we now review operational practices and business practices, we now identify the customer community, voting is now streamlined, and we added the C4CA to this document. Dr. Alterman asked if there were any questions or problems with this revised document. Since there were no objections, Dr. Alterman requested a vote.

Ms. Debbie Mitchell from DoD made the motion to accept the revised document, and Dr. DeYoung from NASA seconded the motion. The following agencies voted to approve the revised document: GSA, GPO, USPS, DoJ, HHS, NASA, DoD, DEA, Treasury, and DoS. The following agencies were absent: DOC, DHS, and USPTO. Ten of the thirteen voting members (a quorum) voted “yes”, or 77%, where a 75% majority vote was required.

This “approved” FBCA/C4CA Criteria and Methodology document will be posted to the FPKIPA website by COB tomorrow.

Agenda Item 5

FPKI Operational Authority (FPKI OA) Report—Ms. Cheryl Jenkins

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

Ms. Jenkins said that the FPKI OA is working with MIT LL and is testing the new interoperability root CA with DoD. The DoD is populating the AIA field, and research is being conducted to populate the SIA extension. A certificate request will be submitted to the FPKI OA once they populate the SKI extension.

2) MIT LL Interoperability Testing Status

MIT LL uses a Novell directory and this requires configuration scripts from the vendor to make it work. The FPKI OA needs to complete two remaining tests with them this week and will then email the test report to the FPKIPA members for an e-vote (upon successful completion).

3) USPS Update

USPS has a team in Eagen, MN modifying a number of active directory objects in the CA and renaming various fields. The Postal OIG is actively involved in observing the process. Currently Postal has temporarily decommissioned their external CA while making the modifications. USPS anticipates that this work will be finished either today or at the latest this Friday. Once the USPS issues are resolved, a Letter of Authorization will be issued and then a cross-certificate.

4) FPKI OA Statistical Report

The FPKI OA e-mailed the FPKIPA listserv the statistical report for February 2007. The FPKI OA received no feedback from the FPKIPA. In the report, three agencies (DHS, DoJ, and GPO) critically impact the architecture to date. Their agency representatives need to contact the FPKI OA to update their certificates and resolve their issues. Critical impacts will break the FPKI Architecture and require immediate attention. Also listed in the report were moderate impacts. Those agency representatives need to contact the FPKI OA to resolve their issues. A moderate impact may cause some issues in assorted areas, but will not break the architecture.

5) New OA Contractors/Project Scope Change

Ms. Jenkins said that Enspier/Protiviti Government Services is the new FPKI OA contractor. We're hoping to move the FPKIA Lab next week from Noblis to Enspier, she said. Once moved, there will be a ten-day impact on the architecture. This will affect only the lab environment and not the production environment. The FPKI OA will notify the FPKIPA listserv with the actual move date.

The FPKI OA ran into budgetary issues and will need to scale back policy compliance work and concentrate on FISMA controls. The FPKI Architecture will undergo Certification & Accreditation (C&A) starting 30 June 2007. The C&A should be finished by 30 September 2007. Ms. Jenkins will send out a notice this week about the directory upgrade.

Ms. Mitchell requested the address of the Enspier lab and the FPKI OA point of contacts. The new FPKI OA policy and CPWG support contact is Mr. Don Campbell. The technical lead contact is Mr. Steve Matney, and the Lab Manager contact is Terry McBride. Ms. Jenkins is still working with Enspier to finalize all the point of contact information. When available, Ms. Jenkins will forward this information to the FPKIPA listserv.

Agenda Item 6

Status of DoD Two-Way Cross-Certification Activities—Ms. Debbie Mitchell

Ms. Mitchell submitted an update to the FPKIPA listserv prior to the meeting via e-mail and described the major activities during the meeting. DoD reached agreement on Certificate extensions and modifications to DoD Cert profiles (AIA, SIA, CRL distribution point). The DoD root test environment was stood up in their Lab. DoD exchanged their initial certificate with the FPKI OA; however, there were problems with the SKI extension. DoD is working out internal issues with the Appendix to the CPS. The expected completion date is the end of April. The draft MOA was sent to the OGC for comment and review. There are ongoing meetings to beef-up the directory support for the interoperability root. The CP change for Medium Hardware was approved by the CPMWG, but waiting on the signature.

Ms. Mitchell continues to provide monthly updates to the FPKIPA, until such time the DoD is two-way cross-certified.

Agenda Item 7

Update on SSPWG Activities—Ms. Judith Spencer

Ms. Spencer said she emailed the revised Common Policy last week to the Shared Service Providers (SSP) and potential SSPs. There have been no comments received from agencies or vendors. We did receive one comment from a vendor (IdenTrust) on the mapping matrix, she said.

The remaining item is the change(s) that 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 1 January 2008. Ms. Spencer will email the white paper/letter to the FPKIPA listserv this week. If any agencies have an issue(s) with the revised Common Policy requirements (as it pertains to Legacy PKIs), please notify Ms. Spencer.

Mr. Schminky said there is still language missing in Section 6.3.2 (Key Usage Periods), and Ms. Spencer said she will review it again. Ms. Spencer wants a vote on the revised Common Policy (in RFC 3647 format) on the 8 May 2007 FPKIPA meeting agenda.

We have reviewed CPS submissions from IdenTrust and the GPO at recent SSPWG meetings. A letter from the Chair of the SSPWG is forthcoming to IdenTrust on their latest CPS submission.

We updated the SSP Roadmap document, based on experience, lessons learned, and additional requirements levied on them (in the Maintenance Phase). This document has been posted to the FPKIPA website.

GSA only performs C&A on the SSP vendor core CA systems. This C&A can be accepted by agencies procuring SSP services. GSA is actively monitoring FISMA reporting requirements by making sure SSP vendors are complying with these requirements. GSA will be hosting a meeting with SSP vendors in the near future about these FISMA requirements.

Ms. Spencer is still waiting on a delinquent audit letter from one of the certified SSP vendors.

Some of the SSP vendors brought to our attention that industry wants the same level of capability and interoperability with the Federal government as it applies to HSPD-12. The SSP vendors want to stand-up clones of their SSP offerings for commercial customers. The CAs would cross-certify with the FBCA (using HSPD-12 compatible certificates and NIST SP 800-73 compatible smart cards). Agencies could read these smart cards and choose to accept (or not accept) these industry credentials. Exostar has sold this technology to the State of Virginia first responders, VeriSign has sold this concept to the State of Pennsylvania first responders, and the State of Maryland is in the process of discovering their options.

VeriSign wants to be mapped so they can cross-certify their Medium Hardware CA with the FBCA.

Agenda Item 8

FPKI Certificate Policy Working Group (CPWG) Report—Dr. Peter Alterman

1) Discuss SAFE Bridge Mapping

The CPWG has devoted several meetings to the SAFE Bridge bi-directional mapping and that a couple of issues remain with their policy and with our policy. There were no deal breakers. We will be meeting with SAFE representatives again to discuss and resolve the issues.

2) Vote to Extend Wells Fargo Provisional Basic Cross-Certificate

Dr. Alterman requested a vote to extend the Wells Fargo provisional Basic assurance cross-certificate, since the cross-certificate expires at the end of the month. The Wells Fargo HSM has not received NIST certification yet. There are many E-Government applications using Wells Fargo certificates. Wells Fargo provided the CPWG with a compliance audit letter that was acceptable. Wells Fargo is now rewriting their CP/CPS in RFC 3647 format, which should be finished by the end of this month. Pending receipt of a revised CP/CPS for Basic assurance from Wells Fargo, Dr. Alterman would like the FPKIPA to extend the Basic cross-certificate for an additional four months. If after four months, Wells Fargo does not get their HSM through the NIST certification process, the FPKIPA will give them an additional two months to procure a different HSM vendor or we would pull their cross-certificate. Wells Fargo currently uses a software-signing module.

Mr. Jim Schminky from Treasury made the motion to extend the cross-certificate with the stipulation, and Mr. Mark Stepongzi from USPS second the motion. The following agencies voted to approve extending the cross-certificate: GSA, GPO, USPS, DoJ, HHS, NASA, DoD, DEA, Treasury, and DoS. The following agencies were absent: DOC, DHS, and USPTO. Ten of the thirteen voting members (a quorum) voted “yes”, or 77%, where a 75% majority vote was required. This topic needs to be added to the FPKIPA 14 August 2007 meeting agenda for discussion. Dr. Alterman will draft the letter to Wells Fargo and will send a signed email to Ms. Jenkins to extend (re-issue) the Wells Fargo cross-certificate.

Agenda Item 9

Final Meeting Items

1) Other Topics

i. **Rewrite of the C4CA CP**
Dr. David Cooper (NIST) revised the Citizen and Commerce Class Certificate Policy (C4CA CP) using the RFC 3647 format. The Research community (GRID) is interested in cross-certifying with the C4CA, and has already been mapped to the original C4CA CP. The Research community would account for 500,000 GRID certificates at this level of assurance.

ii. **Status of revised FPKIPA Charter**
Dr. DeYoung would like all FPKIPA members to review the revised FPKIPA Charter, and be ready to vote on it at the 8 May 2007 FPKIPA meeting. Section 6 of the FPKIPA Charter now references the updated Criteria & Methodology document. Dr. DeYoung has also revised the FPKIPA By-Laws and said he sent it to the FPKIPA listserv last night. Dr. Alterman wants the agenda for the FPKIPA 8 May 2007 meeting to include a vote on the revised FPKIPA Charter and the FPKIPA By-Laws.

iii. **FPKI Audit Working Group**
We have been very active, mapping the FBCA CP to the NIST SP 800-53 security controls, mapping the NIST SP 800-53 controls to the FBCA CP, and mapping the FBCA and NIST 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 us as we move into the international security environment with the European Union, Australia, and Japan.

iv. **NRC**

NRC gets their PKI services from a certified SSP vendor. NRC's upper management submitted documentation to Dr. Alterman, requesting to become a voting member of the FPKIPA. NRC is currently an active member of the SSPWG, and administers their SSP RPS. Dr. Alterman informed Mr. David Sulser that NRC would also need to become an active member of the FPKI CPWG.

Dr. DeYoung from NASA made the motion for NRC to become a FPKIPA voting member, and Mr. Schminky from Treasury second the motion. The following agencies voted to approve NRC as a FPKIPA voting member: GSA, GPO, USPS, DoJ, HHS, NASA, DoD, DEA, Treasury, and DoS. The following agencies were absent: DOC, DHS, and USPTO. Ten of the thirteen voting members (a quorum) voted "yes", or 77%, where a 75% majority vote was required. Dr. Alterman welcomed NRC to club.

Agenda Item 10

Adjourn Meeting

The meeting adjourned at 11:15 AM. The next FPKIPA meeting is scheduled for 8 May 2007 (9:30 AM) at the GSA National Capital Region Building in Washington DC.

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
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	Peter Alterman, Rebecca Nielsen et al	11 July 2006	31 Jan. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	for their bona fides: memo of application, 800-79 compliance statement, and audit summary.				
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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
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	Closed
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

No.	Action Statement	POC	Start Date	Target Date	Status
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