Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 13 February 2007 Meeting

Teleconference only.

A. AGENDA

1) Welcome / Introductions
2) Discussion/Vote on 9 January 2007 FPKIPA Minutes
3) FPKIPA Charter Status
4) FPKI Operational Authority (FPKI OA) Report
   1) Monthly Statistical Report / CSP Scorecard
   2) Status of FBCA/Applicant Cross-Certification Technical Testing
   3) FPKIA Re-Design Status
5) Update on Criteria and Methodology
6) Update on SSPWG Activities
7) FPKIPA Certificate Policy Working Group (CPWG) Report
   1) Discussion/Vote on FBCA CP Change Proposal: 2007-01
   2) Agency Best Practices for Device Certificates
8) E-Authentication PMO Federation Discussion
9) Final Meeting Items
   1) Proposed Agenda Items for next FPKIPA meeting – March 13, 2007
   2) DoD Two-Way Cross Cert Status
10) Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

A quorum of eleven (11) voting members was present (via telecon) 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		Teleconference
Department of Defense	O'Brien, Shawn		Teleconference
Department of Health & Human Services	Alterman, Peter, Ph.D.		Teleconference

Organization	Name	Email	Telephone
Department of Homeland Security	Absent		
Department of Justice	Morrison, Scott		Teleconference
Department of State	Caldwell, Sally		Teleconference
Department of the Treasury	Proxy to NASA per phone call to Chair		
Drug Enforcement Agency (DEA CSOS)	Jewell, Chris		Teleconference
GPO	Hannan, John		Teleconference
GSA	Temoshok, David		Teleconference
NASA	DeYoung, Tice, Ph.D.		Teleconference
USPS	Stepongzi, Mark		Teleconference
USPTO	Purcell, Art		Teleconference

OBSERVERS

Organization	Name	Email	Telephone
SSA (Contractor – -Jacob & Sundstrom)	Simonetti, David		Teleconference
DHS (Contractor – CignaCom)	Shomo, Larry		Teleconference
FICC/GSA	Spencer, Judith		Teleconference
Department of State (Contractor -- ManTech)	Froehlich, Charles R.		Teleconference
DoD PKI PMO	Nielsen, Rebecca		Teleconference
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant		Telecoference
FPKIPA Secretariat (Contractor --Enspier Technologies/Protiviti Government Services)	Fincher, Judy, Ph.D.		Teleconference
FPKI OA (Contractor, Mitretek)	Fisher, Jim, Ph.D.		Teleconference
KPMG	Henry, Vickie		Teleconference
Contractor -- Enspier Technologies/Protiviti Government Services	Pinegar, Tim		Teleconference
E-Authentication PMO	Marsh, Georgia		Teleconference
IdenTrust	Young, Kent		Teleconference
US Nuclear Regulatory Commission (NRC)	Sulser, David		Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman

This meeting was held via teleconference due to inclement weather. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:39 a.m. with the attendee roll call.

Agenda Item 2

Discussion/Vote on 9 January 2007 FPKIPA Minutes—Judy Fincher

Judy Fincher said that all comments on the minutes had been incorporated into the redlined document that was sent to the FPKIPA listserv last week. She asked for a vote on the minutes, as amended. The vote was postponed to the end of the meeting to give one member a chance to review the minutes. He had not received the minutes due to an e-mail listserv problem, for which Dr. Alterman apologized. At the end of the meeting, a vote was taken and the minutes were approved by ten of the eleven members who formed the quorum, or 90.9%, where a 50% majority was required.

The final version of the minutes was posted to the FPKIPA website by the FPKIPA webmaster on 2/13/07.

Approval Vote for 9 January 2007 FPKIPA Minutes			
Voting members	**Vote (Motion – 2nd –)**		
	Yes	**No**	**Abstain**
Department of Commerce	X		
Department of Defense	X		
Department of Health & Human Services	X		
Department of Homeland Security	Absent-Did Not Vote		
Department of Justice	X		
Department of State	X		
Department of the Treasury	Proxy absent for this vote		
Drug Enforcement Agency (DEA CSOS)	X		
GPO	X		
GSA	X		
NASA	Absent for this vote		
USPS	X		
USPTO	X		

Agenda Item 3

FPKIPA Charter Status— Dr. Tice DeYoung

Dr. DeYoung said he had received comments from Dr. Alterman and Charles Froehlich, but had not yet incorporated them into the edited Charter document.

Charles Froehlich identified a problem with the Charter as it now stands. There are no references to the Common Policy, or to the e-governance policy. Who approves the Common Policy changes, if not the Policy Authority? Tim Polk agreed this was an oversight and that we need to incorporate both policies in the revised Charter. Mr. Froehlich also pointed out that the revised Criteria and Methodology document (Crits and Methods) contains changes not yet

reflected in the Charter, i.e., the SSPWG is now a standing subcommittee of the Policy Authority. This is not yet in the Charter.

Dr. DeYoung said he plans to send out the red-lined, edited document, incorporating those changes, as well as his own, to the FPKIPA listserv in March and hopes the FPKIPA can vote on the revised Charter at the April 10, 2007 FPKIPA meeting.

Agenda Item 4

FPKI Operational Authority (FPKI OA) Report—Dr. Jim Fisher

In the absence of Cheryl Jenkins, Dr. Jim Fisher of Mitretek Systems, the Technical Lead for the FPKI OA, made the report.

1) Monthly Statistical Report / CSP Scorecard
   Dr. Fisher said the January report had been distributed this morning, two days before it was due. He also noted that the November and December reports had not been distributed. Anyone needing a copy or having questions about how their agency is represented in these reports should email him at jlf@mitretek.org. He flagged a new issue which has arisen at the FPKI OA: cross-cert pairs were out of date and not matching.

2) Status of FBCA/Applicant Cross-Certification Technical Testing
   Dr. Fisher said the FBCA prototype was re-keyed. Therefore, any entity under testing that had not had a new cert issued from the new FBCA prototype needed to do so. He said that the MIT LL cert had been issued from the prototype and that he will issue a cert to the DoD ECA.

3) FPKIA Re-Design Status
   Dr. Fisher said he briefed the FBCA-TWG on February 8 on the Re-Design of the FPKI architecture and that there had been no items raised that invalidated the architecture. Therefore, the Architecture Re-Design document is now in the hands of an independent reviewer and the response is due in one week. If the independent reviewer concurs, then the new FPKIA equipment will be ordered. The current ATO ends at the end of June and a technology re-fresh is needed. The OA will need to get the new equipment through the C&A process before the end of June. He said that the old and new architectures would operate simultaneously for a period of time.

   Dr. DeYoung wanted to know if the re-design addressed path discovery related issues and problems.

Dr. Fisher said that for this to work properly, you need the right certificate in the directory tree. The focus of the re-design is on redundancy and resiliency, he said. He said he planned to consolidate the existing six CAs into one physical box and to put in place a High Security Module (HSM) that would handle 20 private keys.

Dr. DeYoung then asked if the new architecture would require full directory chaining.

Dr. Fisher: The re-design is looking at the use of referrals, instead of directory chaining.

Dr. Alterman asked if the directory chaining was working for the MIT LL, which is currently undergoing technical interoperability testing in the OA prototype environment.

Dr. Fisher: The next step is to get directory chaining working between the two entities by having MIT run their tests. We have to make sure their product is working through the Bridge, he said. He said MIT is anxious to get it done and estimated the testing would be completed by the end of February.

ACTION: Cheryl Jenkins will provide a weekly update on the MIT LL interoperability testing status to Dr. Alterman.

Entities wishing to receive certs from the re-keyed prototype bridge, should send an e-mail to Darron Tate and Jim Fisher with a cc to Cheryl Jenkins.

ACTION: An e-mail from Cheryl Jenkins to the FPKIPA listserv explaining how to receive certs from the re-keyed prototype bridge is needed.

Agenda Item 5

Update on Criteria and Methodology—Rebecca Nielsen

Rebecca Nielsen of Booz, Allen and Hamilton, contractor to the Department of Defense, reported on the activities of a sub-group of the CPWG which has been re-writing the Criteria and Methodology (Crits and Methods). There are now four major sections to the document.

1) The Introduction, clarifying that the document now addresses both the FBCA and C4CA cross-certification process.
2) The Cross-Certification Process, simplifying the application process and requiring government review of non-mappable sections (1 and 9)

3) Additional Requirements for Bridge-to-Bridge Cross-Certification, focusing on how each bridge does its own member process. This is largely based on our experience in cross-certifying with the first bridge, CertiPath.
4) Maintenance Phase (still in draft).

The goal is to streamline the process and make it reflect actual practice. She said the CPWG hoped to complete the revisions by the end of March and present it to the Policy Authority for a vote at the April 10, 2007 FPKIPA meeting.

She said that sections 1-3 are largely completed, although some graphics will be added depicting the FPKIPA architecture, the organizational chart and cross-certification process

Agenda Item 6

Update on SSPWG Activities—Judith Spencer

Ms. Spencer said that the SSP Roadmap, a document intended as an updated vendor guide to the SSP certification process, is nearly completed and is now being reviewed for a final time by the SSPWG. When that process is completed, she will provide it to the FPKIPA for review and comment. The original SSP Roadmap was written before any vendors went through the process and therefore there have been changes in the process over the years. The major changes are that the SSPWG now reports directly to the FPKIPA and the requirement that the CPWG/SSPWG review the Registration Practices Statement (RPS) for each Agency implementation has been removed. Other federal requirements, such as those embodied in HSPD-12, NIST SP 800-79 and FISMA, now address that requirement. It simply is not needed, given the controls that are in place, she said.

Ms. Spencer also reported that the SSPWG has started the review of the GPO CPS and will continue to do so at its next meeting, March 7, 2007. At that meeting, the SSPWG will review version 1.8 of their CPS and corresponding matrix.

Agenda Item 7

FPKIPA Certificate Policy Working Group (CPWG) Report—Tim Polk

1. Discussion/Vote on FBCA CP Change Proposal: 2007-01

   Mr. Polk described this Change Proposal as the result of DoD pressure to harmonize the FBCA and Common Policy CPs. It consists primarily of three things:

1) Scrubbing CRL issuance
2) Fixing dates in section 6.1.5 Key Sizes
3) Adding security requirements for OCSP Responders.

Mr. Polk also described the companion document to the Change Proposal, prepared by Matt King, which showed which matrices/tables were impacted by this Change Proposal. Both the Change Proposal and matrix impact document were distributed five days in advance of the FPKIPA meeting. Half of the proposed changes have no impact on the matrices/tables. There are some tables that have to be modified and a couple of new tables are required, he said.

He said he was asking for a vote only on the official Change Proposal: 2007-01, not the accompanying matrix impact document.

This Change Proposal has been out for some time, he said, and every comment that has been received has been discussed and incorporated.

Judith Spencer said that one change to the FBCA CP involving re-key and renewal had also been incorporated in the Common Policy Framework CP that she is currently re-writing. You don't have to revoke the old key. When we vote on the Common Policy 3647 re-write, we will vote on that change, as well, she said, and noted that this change had been proposed by Larry Shomo (DHS).

The current status of the Common Policy is that there are six remaining comment bubbles (from Dave Cooper, NIST) that must be addressed in the re-write, she said. Then we will be ready for the Policy Authority to vote on the revised, 3647-format Common Policy, she said.

She then raised another issue that proved to be a show stopper for the vote at this meeting on the FBCA Change Proposal: 2007-01. It dealt with the changes the CPWG made to section 6.1.5 Key Size.

The revision states that:

"CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire on or after 12/31/~~08~~ 10 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA."

"CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that

are issued after 12/31/08 and expire on or after 12/31/2010 shall be generated using, at a minimum, SHA-224."

Ms. Spencer asked if the language should stay in the Change Proposal.

Dr. Jim Fisher noted there is at least one cross-certified entity that has a root cert that expires after 2010. Self-signed certs are only trusted because they are exchanged out-of-band, he said.

Tim Polk responded that this is not a big concern, but that the CPWG needs to decide if self-signed certs should be included in this reference. We prefer not to focus on self-signed certs at this time, only end-user certs, he said.

Dr. Fisher noted that for this entity, 2032 is the date when their RSA key expires.

Mr. Polk responded that they will have to do a key rollover fairly soon, and added that we should let them know via e-mail that they can't continue to use that key until 2032 and that they have to roll over their key. However, he said, we need to keep an eye on that requirement vis-à-vis self-signed certs, even though we only process CA certs.

Ms. Spencer again raised her concern with section 6.1.5., the 6th paragraph, which reads:

"End-entity certificates that expire before 12/31/08 shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End-entity certificates that expire on or after 12/31/08 shall contain public keys that are at least 2048 bit for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Shouldn't the language regarding "End-entity certificates that expire on or after 12/31/08" be changed to 12/31/10? she asked, explaining that this would impact legacy PKIs, but not the people under Common, she said.

Mr. Polk agreed she had a valid point and that the vote could not go forward today.

ACTION: The CPWG will edit the FBCA Change Proposal: 2007-01 at the next CPWG meeting on Tuesday, February 20, 2007, and post the revised Change Proposal on Wednesday, February 21, to the FPKIPA listserv. FPKIPA members will then have five days to review the Change Proposal and an e-mail vote will be initiated on 28 February 2007, before the next Policy Authority meeting on 13 March 2007.

2. Agency Best Practices for Device Certificates

Tim Polk submitted this draft policy statement for FPKIPA review five days prior to the meeting. The policy is in Q&A format and is intended for adoption by the FPKIPA.

He received two comments.

Charles Froehlich (DoS) requested that another Q&A be added: "Why is a separate certificate policy for device certificates necessary?" The proposed answer is, "Both the FBCA CP and the FCPF provide for issuing certificates to devices, in the latter case to include a specific policy OID. Therefore, agencies do not necessarily need to develop and/or cross-certify a separate policy specifically for device certificates."

Mr. Polk agreed to add this to the draft policy statement.

He also received a vendor comment, requesting that he draw out more clearly that the policy is dealing with infrastructure certs, e.g., internal security components.

Rebecca Nielsen asked that he clarify what you are concerned about.

Mr. Polk said he would add language regarding certs that don't need to be validated by you internally.

John Hannon (GPO) commented that issuing this policy is a "reasonable thing to do" and "a good idea, in general." However, he added that we need to look at all aspects of the issue.

Shawn O'Brien (DoD representative to the FPKIPA for this meeting), asked if DoD had to concur with the policy as written. DoD has not worked out the details of its own policy yet, regarding when we need to interact with the FPKIPA and when we need to go on our own, he said.

Mr. Polk said it does not constrain DoD's options or "force you down any particular path."

Mr. Polk said he wants to post this policy to the FPKIPA website under "Other Policies." However, he added, it's clear we are not voting today.

Dr. Alterman said he had received an email (also sent to Tim Polk) from Scott Rea (Educause) regarding the SSP profile document and the implication with Microsoft implementation. This is related to device certs

and also to encrypting file systems, an issue which soon will be brought to the FPKIPA's attention.

Agenda Item 8

E-Authentication PMO Federation Discussion—Georgia Marsh

Ms. Marsh began her presentation with a thank you to the Policy Authority for helping to get Wells Fargo cross-certified. She said Wells Fargo is now live with eOffer.

She then described an OMB initiative spearheaded by Carol Bales, Portfolio Manager for E-Authentication that seeks to create synergies between HSPD-12, E-Authentication and the FPKIA. She assembled a task force comprised of Judith Spencer, Georgia Marsh, Dr. Alterman and Chris Louden (Enspier/Protiviti Government Services) to determine how to align the different programs.

She also acknowledged the role of the FPKIPA in providing cross-certs for E-Authentication Levels 3 and 4 and described efforts to further align the two programs.

Mr. Marsh also mentioned she was trying to convene a small group comprised of members of the FPKIPA and E-Authentication programs to facilitate alignment efforts. This group has not been convened yet, she said.

She predicted that alignment across the Federal Identity management solutions will occur and that joint solutions for the agencies will make them more affordable.

Judith Spencer agreed that this is the right move and that it needs to be done.

Ms. Marsh said that she had met with the Burton Group at RSA last week and that the Burton Group was preparing a Lessons Learned White Paper. She said the Burton Group would be included in the OMB-sponsored alignment meeting next week.

Although she has proposed that Dr. Alterman become an *ex officio* member of the Executive Steering Committee (ESC), it now appears that "Councils that operate the Federation may overtake the ESC."

Georgia Marsh then asked Tim Polk for an update on the status of NIST 800-63. Mr. Polk said he hoped to complete the public comment period by the end of March and would provide an advance copy to the PMO as soon as it makes sense. Mr. Polk said that 800-63 would broaden options for the PMO and would "have a real impact on you."

Ms. Marsh then explained that the E-Authentication PMO is moving to a fee-for-service model by October 2007, and that she has formed a Business Model Working Group to try to 1) identify the services we will be offering and 2) determine how to bundle the services for the agencies, so that it is cost-effective. She hopes to have those services defined by the end of March 2007. She has planned both an Industry Day and Customer Day to present this Business Model.

Art Purcell said that his agency is interested in possibly acquiring services from the E-Authentication service offering and asked for a point of contact. Ms. Marsh confirmed that she was the POC for agency questions about the Business Model.

Agenda Item 9

Final Meeting Items

- Proposed Agenda Items for the next FPKIPA Meeting – March 13, 2007

  Dr. Alterman asked members to send any agenda items they would like to see discussed to Judy Fincher at Judith.fincher@enspier.com.

- DoD Two-Way Cross Cert Status

  Debbie Mitchell submitted an update to the FPKIPA listserv prior to the meeting via e-mail, but this item was not presented at this teleconference because she was on travel. It is attached at the end of these minutes. She will provide another update at the 13 March 2007 meeting, as agreed with Dr. Alterman, e.g., monthly status reports until such time the DoD is two-way cross-certified.

Agenda Item 10

Adjourn Meeting

The meeting was adjourned at 11:10 a.m.

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 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 is 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 it is issued ~~next week (November 20, 2006).~~	Judy Fincher	14 Nov. 2006	31 Jan. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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	Jan. 9, 2007	Open
259	Debbie Mitchell will forward policy statements to the FPKI PA for review when available.	Debbie Mitchell	12 Dec. 2006	Jan. 9, 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