Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 12 December 2006 Meeting

GSA, 18th and F Street, NW, Room 7003
Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discussion/Vote on two-way DoD Cross-Certification
3) Discussion/Vote on 14 November 2006 FPKIPA Minutes
4) Review FBCA Change Proposal: 2007-01 (Discussion Only, Vote: January 9, 2007)
5) Review of Common Policy Changes
6) Update on SSP-WG Activities
7) Briefing: Rich Attribute Exchange
8) Final Meeting Items
   Other Topics
   - Election Process for New FPKIPA Chair begins in January 2007
   - Proposed Agenda Items for next FPKIPA meeting – January 9, 2006
9) Adjourn Meeting/Holiday Celebration

B. ATTENDANCE LIST

VOTING MEMBERS

A quorum of eleven (11) voting members was present, of thirteen (13) voting members, or 84.6%, where a quorum of 75% was required. The Department of Energy is currently a non-voting member because of its audit status.

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		

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

OBSERVERS

Organization	Name	Email	Telephone
GSA	Cornell, John		
FPKI	Spencer, Judith		
Department of State (ManTech)	Froehlich, Charles R.		
FICC Support (General Dynamics Information Technology)	Petrick, Brant		
Enspier Technologies	Louden, Chris		
Enspier Technologies (Secretariat)	King, Matt		
Identrust	Young, Kent		
Enspier Technologies	Pinegar, Tim		

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions—Dr. Peter Alterman

This meeting took place at GSA Headquarters, 18th and F Street, NW, Room 7003, Washington, DC. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:42 a.m. with attendee introductions. Dr. Alterman noted that the Holiday Celebration at the end of the meeting was also intended to celebrate the accomplishments of this group over the last year. He also noted the January meeting agenda will be very full because some items will not be addressed in today's meeting.

Agenda Item 2

Discussion / Vote on two-way DoD Cross-Certification—Debbie Mitchell

Earlier in the year, Debbie Mitchell reported that Dr. Peter Alterman had issued an “administration determination” in October 2006 to extend the DoD cross-certificate through the end of year 2006. The cross-certificate had originally been set to expire the end of October 2006. DoD was unable to meet its goal of two-way interoperability and cross-certification because of HSPD-12 pressures.

At the December 12 FPKIPA meeting Ms. Mitchell distributed a PowerPoint slide presentation on DoD’s progress toward achieving two-way cross certification with the Federal Bridge.

Ms. Mitchell explained that one chart showed the steps DoD needed to take to get the new root cross-certified with the FBCA. She noted that most of the tasks have been started and the goal end date was 30 March 2007. Currently, DoD expects that hardware will be acquired this week and they are planning for development testing. After a review of documentation, they found some issues, but are in the process of updating the documents (including the CPS) to resolve any issues. These updates include changes to prepare for Medium Hardware cross-certification. The DoD policy is expected to be approved in the next month.

One issue Ms. Mitchell mentioned was the need to allow acceptance of certificates issued outside of DoD. A meeting will be held this week to discuss and evaluate options. DoD is hoping to issue a cross-certificate soon and is working with the FPKI OA to move forward.

While progress has been made, DoD is not ready for cross-certification and requested a six month extension. Ms. Mitchell stated, however, that the plan is to have everything in place by 30 March 2007.

Discussion was held and Ms. Mitchell explained that DoD follows procedures that meet Medium Hardware requirements, but the policy does not reflect these procedures. She also noted that DoD wants a new interoperability root at Medium Hardware.

Mr. Tim Polk noted and Ms. Mitchell confirmed that every task on the chart had been started (except for those items that couldn’t be started due to dependencies on current tasks). Mr. Polk also noted that a six (6) month extension would provide a two month slack period in the event the current schedule was delayed. He did question whether it was realistic for the DoD policy to be approved within the stated timeline. Ms. Mitchell then replied that the CPS had already made it through the DoD process once and she expected it to pass in January 2007.

Mr. John Cornell noted that the new MOA was missing from the plan and Ms. Mitchell took an action to include the MOA as a task on the schedule.

ACTION: Debbie Mitchell will add a task to the DoD schedule that addresses the new MOA.

Mr. David Temoshok stated concern over item 37 (Discussion Policy for Cross-Certification). Ms. Mitchell responded that current DoD policy states that OSD NII determines what certificates in DoD are allowed, but there is an effort to change this requirement in the policy. Ms. Mitchell then took an action to send policy statements to the FPKI PA for review when they were available.

ACTION: Debbie Mitchell will forward policy statements to the FPKI PA for review when available.

Ms. Judy Spencer noted that a decision must be made about who will have the new root. Ms. Mitchell replied that this issue is being worked and an interoperability working group has been started.

Mr. Polk then asked if the hardware order had been placed and if NSA would perform the C&A of the DoD root again. Ms. Mitchell confirmed the order had been placed and took an action to follow-up via e-mail on who will perform the C&A. Mr. Polk noted that the C&A introduced a level of risk to the schedule.

ACTION: Debbie Mitchell will confirm who will perform the C&A of the DoD root and notify the FPKI PA via e-mail.

Mr. Cornell noted that it would be beneficial to have a compliance auditor review the compliance letter.

Mr. Polk offered Mr. David Cooper’s time for review of DoD’s Certificate Policy.

Mr. Cornell noted that the C&A is required, but is completely internal to DoD. Ms. Spencer then noted that compliance audits are of more importance to us.

Ms. Mitchell stated that Access Control has not been as good as it could have been, but DoD is working to fix the issues.

Mr. Charles Froehlich noted that as of January 1, 2007, some DoS crypto people will need to use “snail mail” to process symmetric key administrative actions with NSA because some DoD sites will not allow the use of DoS certificates.

Mr. Polk noted that it is important that policy guidance supports the conversion of applications to allow certificates from outside DoD. He suggested that applications should be prioritized depending on the size of the user base. Mr. Polk believes DoD is motivated, but wants to see a proactive policy memo.

Mr. Alterman thanked Ms. Mitchell for her presentation.

Mr. Polk (Department of Commerce) moved to extend the DoD deadline by 6 months as long as DoD continued to communicate progress and share policy documents. Mr. Morrison (Department of Justice) seconded the motion.

A vote was taken and passed with a 81.8% majority (9/11), with two abstentions, where a ¾ majority vote was required.

Dr. Alterman noted that a monthly update from DoD was needed moving forward. He also took an action to write a memo to Ms. Cheryl Jenkins to extend the cross-certificate.

ACTION: Dr. Peter Alterman will write a memo to Ms. Cheryl Jenkins to extend DoD's cross-certificate.

Approval vote to extend the DoD Cross-Certificate for Six months			
Voting members	**Vote (Motion – Commerce; 2nd – Justice)**		
	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	Absent-Did Not Vote		
Drug Enforcement Agency (DEA CSOS)	X		
GPO	X		
GSA	X		
NASA	X		
USPS	X		
USPTO	X		

Agenda Item 3

Discussion / Vote on 14 November 2006 FPKIPA Minutes—Matt King

Mr. King stated that comments were received on the 14 November 2006 minutes from Brant Petrick and Charles Froehlich and that the changes had been incorporated in the red-lined document, which was circulated prior to the meeting.

The FPKIPA approved the minutes by 100%, or 11/11, where a majority vote of 50% was required.

<table>
<tr><th colspan="4">Approval vote for 14 November 2006 FPKIPA Minutes</th></tr>
<tr><th rowspan="2">Voting members</th><th colspan="3">Vote (Motion – DoS ; 2nd – GPO)</th></tr>
<tr><th>Yes</th><th>No</th><th>Abstain</th></tr>
<tr><td>Department of Commerce</td><td>X</td><td></td><td></td></tr>
<tr><td>Department of Defense</td><td>X</td><td></td><td></td></tr>
<tr><td>Department of Health & Human Services</td><td>X</td><td></td><td></td></tr>
<tr><td>Department of Homeland Security</td><td colspan="3">Absent- Did not Vote</td></tr>
<tr><td>Department of Justice</td><td>X</td><td></td><td></td></tr>
<tr><td>Department of State</td><td>X</td><td></td><td></td></tr>
<tr><td>Department of the Treasury</td><td colspan="3">Absent- Did not Vote</td></tr>
<tr><td>Drug Enforcement Agency (DEA CSOS)</td><td>X</td><td></td><td></td></tr>
<tr><td>GPO</td><td>X</td><td></td><td></td></tr>
<tr><td>GSA</td><td>X</td><td></td><td></td></tr>
<tr><td>NASA</td><td>X</td><td></td><td></td></tr>
<tr><td>USPS</td><td>X</td><td></td><td></td></tr>
<tr><td>USPTO</td><td>X</td><td></td><td></td></tr>
</table>

Agenda Item 4

Review FBCA Change Proposal: 2007-01 (Discussion Only, Vote: January 9, 2007)—Tim Polk and Judith Spencer

Ms. Judy Spencer provided an overview of FBCA Change Proposal: 2007-01. She explained that the harmonization effort over the last six months resulted in seven pages of changes including:

- Reformatted Common Policy into RFC 3647 format
- Added or moved language
- Included FBCA policy language to fill any holes resulting from the move to the new format
- Reviewed the document and revised text with better wording.

A goal is that the FBCA and Common policies be as close as possible, she said. Mr. Polk asked that each of the members review the document and identify any "deal breakers."

Dr. Tice DeYoung noted the 30 day time period and algorithm sizes as differences. Mr. Tim Polk noted the biggest issue was SHA-256 and disaster recovery requirements. He also noted that it's important to understand what members will be out of compliance with the new changes and when the changes could be fixed. Mr. Polk stated that a vote in January was desired unless there are major issues. If there are major issues, it is hoped they could be discussed and possibly fixed by the 4 January 2007 CPWG meeting.

Ms. Spencer noted that some issues with legacy PKIs will not be settled until the FIPS 201 issues are resolved.

Agenda Item 5

Review of Common Policy Changes—Tim Polk and Judith Spencer

Ms. Judy Spencer noted that the Common Policy Changes were sent to the SSP vendors and only comments from IdenTrust were received.

Agenda Item 6

Update on SSP-WG Activities—Judith Spencer

Ms. Spencer, in her role as Interim Chair of the SSP-WG, sent letters to certified SSP providers reminding them that their yearly compliance audits need to be completed for 2006. She has a response from one of the certified SSP providers and expects to hear from others soon. Entrust and Exostar are in the process of submitting their C&A documentation to the GSA ISSM. Ms. Spencer noted the same GSA ISSM is performing the C&A review and is very thorough.

Agenda Item 7

Briefing: Rich Attribute Exchange—Chris Louden

Mr. Chris Louden, CTO of Enspier Technologies, presented a briefing on Rich Attribute Exchange. He explained that current systems only provide information about the identity of a user and rich attribute exchange is about getting and exchanging more information about the users.

He explained that application owners really need more information than just identity to make access control decisions. In HSPD-12, the card is used to look up more information about a user and then take actions – this is referred to as "back-end authentication." Mr. Louden also provided an example of E-Authentication and how systems in E-Auth need and use more information to make access control decisions. He noted the E-Auth TWG is discussing rich attribute exchange.

Mr. Louden then explained that discovery of attributes can be achieved in several ways. In one option, a user could configure what attributes are available. Pointers in certificates could be another way to direct applications to attributes about users. Finally, designated attribute authorities could be established to maintain attributes about users.

Mr. Louden's goal in making the presentation was to raise awareness of this issue.

Discussion was held about the topic. Mr. David Temoshok noted that, while attribute exchange does raise privacy issues, the Privacy Act does not preclude disclosure, but simply requires notice (via a System of Record Notice, or SORN). Mr. Temoshok suggested the FPKI PA should consider policy implications of exchange of privacy information.

Ms. Spencer suggested that HSPD-12 is where this issue should be addressed. Mr. Polk noted, however, there may be related pieces about which the FPKI PA should be aware.

Mr. Louden suggested that the FPKI PA simply needs to be aware of the attribute exchange issue and consider it moving forward. It was noted that there were some efforts in the IETF and SAML to develop ways to convey attribute information.

In the end, the consensus was that issue of rich attribute exchange should not be addressed by the FPKI PA. Rich attribute exchange, however, is viewed as an important issue and the FPKI PA should maintain awareness of various activities related to this topic to understand potential impacts to FPKIPA work now or in the future.

Agenda Item 8

Final Meeting Topics

Other Topics

- **Election Process for New FPKIPA Chair begins in January 2007**

  Dr. Alterman reminded the group that the election process for the new FPKI PA Chair begins in January and we are hoping completion of the process by February. He pointed out that the position requires 90% of one's time and three FTE's in contractor support.

- **Proposed Agenda Items for next FPKIPA meeting – January 9, 2006**

  Dr. Alterman noted that he expected the SAFE mapping to start in January.
  Dr. Alterman also noted that an audit letter is needed for MIT LL and a January vote is expected.
  CertiPath is interested in end-to-end testing and more information is expected in Q1 of calendar year 2007.
  A lot of work is being done on Adobe and an update is expected in January 2007.

A cross-certificate application is expected in January 2007 from the University of Texas.

Agenda Item 9

Adjourn Meeting / Holiday Celebration

Dr. Alterman thanked all members for their hard work this year and the meeting adjourned at 11:22 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
187	Mr. Tim Polk and Ms. Judy Spencer will meet with DoD to conceptualize a plan to help DoD internally to upgrade its CA's and shore up its infrastructure (repositories).	Judy Spencer, Debbie Mitchell	10 Jan. 2006	Sept. 2006	**Open**
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	Oct.-Nov., 2006	**Open** **OBE?**
191	Mr. Art Purcell will be put on the work team to provide information on federal regulations that govern storage of the documents that will be posted to the shared Document Management Services system on behalf of the Policy Authority.	Cheryl Jenkins, Art Purcell	10 Jan. 2006	14 Feb. 2006	**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**
211	Ms. Judy Spencer is to speak with Acting Federal Acquisition Service Commissioner G. Martin Wagner regarding leasing other space at the Willow Woods facility for the FPKIA operations center.	Judy Spencer	14 March 2006	31 March 2006	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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, et al	11 July 2006	8 August 2006	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
248	Judy Spencer will talk to Treasury and GPO off-line about the potential impact of the changes made to the Common Policy.	Judy Spencer	12 Sept. 2006	20 Sept. 2006	Open
252	Cheryl Jenkins will send out that document along with cost estimates provided by FBCA-TWG member agencies. She will ask FPKIPA members to tell her if you can establish a Test Environment in the FY 2007 time frame.	Cheryl Jenkins	12 Sept. 2006	22 Sept. 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	20 Nov. 2006	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

No.	Action Statement	POC	Start Date	Target Date	Status
256	Dr. Peter Alterman is to write an ISMS contract award, to delay further its start.	Dr. Peter Alterman	14 Nov. 2006	12 Dec. 2006	Open
257	Debbie Mitchell will find out who does the DoD C&A.	Debbie Mitchell	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
261	Dr. Peter Alterman will write a memo to Ms. Cheryl Jenkins to extend DoD's cross-certificate.	Peter Alterman	12 Dec. 2006	9 Jan. 2007	Open