Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 9 January 2007 Meeting

GSA NCR Building, 7th and D Streets, SW, Room 5700
Washington, DC.

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Election Process for FPKIPA Chair
3) Compliance Audit Status/Executive Summary Sheet
4) FPKI Operational Authority (FPKIPA OA) Report
5) Discussion/Vote on 12 December 2006 FPKIPA Minutes
6) Crits and Methods Update
7) Update on SSP-WG Activities
8) FPKIPA Certificate Policy Working Group (CPWG) Report
    1) Near-Term Mapping Activities (SAFE, TAG PMA, U. of Texas)
    2) Status of MIT LL Interoperability Testing
    3) Device Cert Policy: Do we need one for the FPKIPA?
    4) New Federal Register Notice
    5) DoD Two-Way Cross Cert Status
9) Final Meeting Items
    1) Proposed Agenda Items for next FPKIPA meeting – February 13, 2006
    2) Do we need to modify the Charter to require a vote on the MOA?
    3) Update of the Charter and By-Laws
    4) Other Business: Miscellaneous
10) Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

A quorum of ten (10) voting members was present of thirteen (13) voting members, or 76.9%, 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		

Organization	Name	Email	Telephone
Department of Defense	Mitchell, Deborah		Teleconference
Department of Health & Human Services	Alterman, Peter		
Department of Homeland Security	Absent		
Department of Justice	Morrison, Scott		
Department of State	Absent		
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
SSA (Contractor – -Jacob & Sundstrom)	Simonetti, David		
DHS (Contractor – CignaCom)	Shomo, Larry		Teleconference
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		
Wells Fargo	Drucker, Peri		Teleconference
KPMG	Faut, Nathan		
Contractor -- Enspier Technologies/Protiviti Government Services	Pinegar, Tim		
eValid8 (contractor)	Dilley, Brian		
CoreStreet, Ltd. (Vendor)	Briley, Jr. , James		
State of Illinois	Anderson, Mark		Teleconference
US Nuclear Regulatory Commission (NRC)	Sulser, David		

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions—Dr. Peter Alterman

This meeting took place at the GSA National Capital Region (NCR) Building at 7th and D Street, Room 5700, Washington, DC. Dr. Peter Alterman of HHS and Chair

of the FPKIPA called the meeting to order at 9:40 a.m. with attendee introductions.

Agenda Item 2

Election Process for FPKIPA Chair—Dr. Peter Alterman, Judy Fincher

Judy Fincher (FPKIPA Secretary) explained that she had sent the instructions for the election process to all FPKIPA voting members on December 27, 2006, and again last week to the listserv. Nominees had to have written management approval and nominations were due by January 9, 2007. She read into the record the following relevant sections of the By-Laws, which govern the election process.

> *13. FPKI-PA Chair*: The FPKI-PA Chair shall hold the position for a period of two years. A sitting Chair may, by a majority vote, be allowed to hold the position for a second two-year term. In no circumstances shall a Chair hold the position for more than four consecutive years unless these By-Laws are amended. The Chair may step down prior to the end of the two-year term, as specified in the Charter. In doing so, the Chair shall give at least 60-days notice, except in emergency situations in which the Chair shall designate an alternate to perform the functions of this office until an emergency election can be held. Such emergency elections shall be held within 30 days of the effective date of the outgoing Chairperson's resignation.
>
> 14. *FPKI Chair Elections*: When electing a new Chair, the following procedures shall be followed:
>
> a. Nominations will be accepted by the outgoing FPKI-PA Chair in writing or signed email only, and only for nominees that have agreed to be nominated.
>
> b. Nominees must have their management's approval, in writing or signed email, and be willing to dedicate at least 8 hours a week to the responsibilities of the FPKI-PA Chair
>
> c. Candidates shall have the opportunity to prepare a written statement of their positions, agendas, and goals for the FPKI PA. These statements shall be provided to the Secretary, who shall post them to the FPKI PA ListServ along with the final ballot.
>
> d. Voting Members will be given five working days to vote for a new Chair, and the voting shall be done by signed email directly to the FPKI-PA Secretary.
>
> e. If no nominees receive a majority of votes (where a majority is defined to be greater than 50% of Voting Membership), then a run-off election of the top two (including ties) nominees shall be conducted, using the procedure in 14c above. This process shall be repeated until such time as one nominee receives a majority vote.

David Temoshok (GSA) made a motion to follow the process described in Section 13 of the By-Laws to re-elect the current Chair by a simple majority vote. The Secretary confirmed this was proper procedure for re-election of a sitting Chair. The motion was seconded by Tim Polk (Commerce).

Dr. Alterman confirmed that he had prior management approval and that the e-mail letter authorizing him to continue in this role at the same level of involvement was on file with the Secretariat.

Tim Polk said we need the attention of an involved Chair and was glad to know it would be maintained.

Dr. Tice DeYoung raised a concern about the notification timetable and Dr. Alterman asked if anyone had a problem with the timeframe of the notification period. None did, so the vote proceeded. Dr. Alterman abstained. The motion passed with 100% of those voting in favor, where a majority vote (50%) was required. The voting table appears below.

Approval vote to Re-Elect the Current Chair, Dr. Peter Alterman			
Voting members	**Vote (Motion –GSA 2nd – Commerce)**		
	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	Absent-Did Not Vote		
Department of the Treasury	Absent-Did Not Vote		
Drug Enforcement Agency (DEA CSOS)	X		
GPO	X		
GSA	X		
NASA	X		
USPS	X		
USPTO	X		

Dr. Alterman expressed his thanks to the FPKIPA for their support and said he would push forward an initiative to making PKI central to both security and commerce. He will push the “new PKI,” he said.

Agenda Item 3

Compliance Audit Status/Executive Summary Sheet— Dr. Alterman, Judy Fincher

Judy Fincher explained that the Audit Status Matrix and Executive Summary sheet had been distributed to the listserv five days prior to the meeting. She reviewed the audit status of all cross-certified members, one by one, as follows.

1) DoD Root CA and DoD ECA
Debbie Mitchell said the DoD audit was complete and that the summary letter would be presented at the February 13, 2007 FPKIPA meeting.

2) Department of State (DoS)
The DoS attestation letter is due 2/13/07.[1]

3) USPTO
Art Purcell confirmed that the audit being performed by ORC is still in process.

4) State of Illinois
The next full audit is due 8/29/07. (Illinois requires an annual audit).

5) DOE
DOE plans to have their audit finished by February 2007, so that they can be reinstated as a voting member.

6) Treasury
Dr. Alterman stated that he had been in touch with James Schminky regarding the corrective actions underway to address deficiencies in the last audit (8/28/06).

7) DHS
DHS will do a full audit by 3/1/07.

8) ACES/DST and ACES/ORC
Both of these audits are long overdue (7/29/06 and 1/14/06, respectively). David Temoshok is looking into the problem and Judith Spencer reported that Steve Duncan had sent a memo to both DST and ORC regarding the status of their audits.

[1] A soft copy of the CIO attestation letter was forwarded to the Chair and Secretariat on 1/19/07, with hard copy following via postal mail.

As an aside, Ms. Spencer also reported that she had sent a memo to ORC regarding their SSP audit and that ORC had forwarded the request to their auditor, Mitretek. She said that other SSP vendors are also behind. Their audit letters are due to the FICC/SSP-WG this month, she said.

9) Department of Justice (DoJ)
DoJ is overdue (12/6/06) on its audit (delta or attestation letter) due to an internal debate as to whether to go with an SSP for the PKI. Scott Morrison said that the long-term plan for DoJ's PKI is still being debated. We're in a no-growth, maintenance mode, he said. DoJ is considering using DoJ PKI certs for signing certs on HSPD-12 cards and will go with an SSP for their HSPD-12 (pivauth) certs. Various FPKIPA members commented that this approach is a high cost solution, since it would require vendors to go through a two-cycle process, instead of one pass.

Ms. Spencer recommended that DoJ keep its PKI and go with an SSP for HSPD-12.

Tim Polk said that DoJ is cross-certified at the "High" LOA, but that no SSPs are currently offering their services at High.

Scott Morrison said DoJ will deploy 5,000 cards via the SSP initially, during the pilot period, and will evaluate how it works before making a decision in the March timeframe.

Tim Polk pointed out that DoJ is also a candidate for using a "delta" C&A process. Mr. Morrison said DoJ has a contractor in place with the availability to do a "Delta".

ACTION: Dr. Alterman will send a friendly e-mail, urging DoJ to keep its PKI.

Debbie Mitchell asked if the DoJ decides to use a SSP for PKI and discontinue the DoJ domain, would they remain voting members of the FPKIPA.

Dr. Alterman and Dr. Tice DeYoung concurred that DoJ would remain a voting member. Dr. DeYoung said that a provision for this has been added to the Charter, Section 3.1.3 (also refer to Section 3.1.1, since DoJ is considered a Charter member of the FPKIPA).

A discussion then ensured as to whether agencies who obtain their PKI services from an HSPD-12 SSP would remain eligible to sit on the Policy Authority and vote.

Dr. Alterman responded that they could request membership.

David Temoshok said that the Charter would have to be modified to permit this.

Judith Spencer said the key point is whether the Federal agency has the interest, e.g., demonstrate by an application to become a member and by showing up for the meetings.

Dr. DeYoung's concern was that if they're not running an operational PKI, i.e., have "a dog in the fight," would they even know what was going on?

David Temoshok said the Policy Authority includes discrete PKI policies and that there is an alignment of policy and procedure among people who have the responsibility to do that.

This is another potential role for the Policy Authority, Dr. Alterman said. The Policy Authority could become more powerful as we move on.

Tim Polk said that if an agency operates equipment under the Common Policy or under their own PKI, they have compelling reasons and experience to participate in the Policy Authority. Mr. Polk questioned the wisdom of including agencies as voting members of the Policy Authority who are letting someone else run their operations.

This discussion is continued in **Agenda Item 9**, below. The audit status update of cross-certified entities continues here.

10) GPO
The next delta or attestation letter is due 8/18/07.

11) Wells Fargo
The WebTrust audit started on 11/13/06 and results should be ready early in 2007.

12) USPS
The next delta or attestation letter is due 10/2/07.

13) CertiPath
CertiPath's next full audit is due 4/17/07.

14) DEA CSOS
The next delta or attestation letter is due 4/12/07.

15) NASA
Dr. DeYoung pointed out that NASA is still running a legacy PKI, in addition to the PKI that is outsourced to Treasury. The last audit for the NASA legacy PKI

was in February 06 and the next delta or attestation letter is due in February 07, and is currently being worked on.

Ms. Fincher pointed out that the Executive Summary Sheet has been modified to reflect current and future audit status requirements. All cross-certified members should review this document to make sure they concur with the information contained therein.

Agenda Item 4

FPKI Operational Authority (FPKI OA) Report—Dr. Peter Alterman, Judith Spencer

Dr. Alterman reported for the FPKI OA in the absence of Ms. Cheryl Jenkins, who was unable to attend due to illness.

1) Ownership of the FPKI OA
Ownership of the FPKI OA has been transferred from the E-Authentication PMO to the Office of Governmentwide Policy. Dr. Alterman noted that the FPKI OA Directory had been down often in the past month. He reported that he had had a meeting with Mary Mitchell (Deputy Associate Administrator, Office of Technology Strategy) in December to discuss issues related to the hiatus in funding (and resulting disruption of contractor support) that occurred last year. He said that with OGP in charge and with the new OA support contractor in place, these issues should not occur in the future. Ms. Mitchell has committed to full support and funding for the Policy Authority, he said.

Judith Spencer said that we have to be very careful because, like most of you, the GSA is under a Continuing Resolution and does not have a budget. The final decision on who will be on the annual Continuing Resolutions and who will get a budget will be made on February 15, she said. The OGP will be responsible for providing financial support for NIST support, the Policy Authority and the FPKI OA.

ACTION: Judith Spencer will touch base with OMB to make sure they know there's an appropriation for the Policy Authority line item.

She urged all cross-certified agencies to have their CIOs tell Karen Evans that they support the FPKIPA appropriation.

Dr. Alterman announced that because GSA has committed to supporting the Policy Authority, "we're going to move forward to recompete the Policy Authority support contract."

2) OA Support Contract
Dr. Alterman said that the protest of the award of the FPKI OA contract is in process. John Cornell, the GSA lawyer, responded to the complaint from ORC; the complainant (ORC) then sent back their comments to GSA. Mr. Cornell was to send his response today to the latest round of ORC comments.

This is still on schedule to be resolved in 90 days (from the time of the complaint). The GSA decision is due 20 February 2007.

3) Encryption Requirements
Dr. Alterman said the FPKIPA would take up encryption requirements this year.

4) Device Certs
Dr. Alterman noted that HHS has set up a PKI for device certificates and that HHS has already held the key ceremony, which was video taped.

Agenda Item 5

Discussion/Vote on 12 December 2006 FPKIPA Minutes—Judy Fincher

Ms. Fincher stated that comments were received on the 12 December 2007 minutes from Brant Petrick and Charles Froehlich and that the changes had been incorporated into the redlined document, which was circulated prior to the meeting.

The FPKIPA approved the minutes by 100%, or 10/10, where a majority vote of 50% was required, as shown on the voting table, below.

The final version of the minutes was posted to the FPKIPA website by the FPKIPA webmaster on 1/9/07.

Approval vote to approve the 12 December 2006 FPKIPA Minutes			
Voting members	**Vote (Motion –GPO ; 2nd –USPS)**		
	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	Absent-Did Not Vote		
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 6

Crits and Methods Update—Judith Spencer

Ms. Spencer reported on the outcome of the last CPWG meeting, January 4, 2007, where the Crits and Methods were revised.

A sub-group of the CWPG has done a complete re-write of the Crits and Methods, she said. The original document was derived from a Canadian document, before we had cross-certification experience, external partners (commercial entities and bridges), and interoperability issues. The current version is largely the work of Dr. Alterman and the DoD Consultant from Booz Allen Hamilton (Rebecca Nielsen), who created the strawman document that was reviewed last week.

The CPWG at its 4 January 2007 meeting worked through the document, including extensive comments from Charles Froehlich. We went through the document, line by line, tightening, streamlining and adding a new section on Operational Strategy, which Rebecca Nielsen (Booz Allen Hamilton) is drafting. The latest version of the Crits and Methods are more aligned with existing practice to make sure we follow procedures. In the past, we gave people a "by," e.g., during the application process. We are now more organized in the acceptance of applicants and have incorporated processes we have been following for Bridge-to-Bridge applicants regarding operational requirements, bona fides, etc. By March 2007 the draft should be ready for Policy Authority review.

ACTION: The CPWG will schedule another editing session when Rebecca Nielsen (Booz Allen Hamilton) finishes the new operational requirements section and makes the other edits identified by the CPWG at its 4 January 2007 meeting.

Agenda Item 7

Update on SSP-WG Activities—Judith Spencer

Ms. Spencer, Chair of the SSP-WG and Chair of the FICC, provided an update on her activities and those of the SSP-WG.

Audit Letters
We sent letters to three SSP vendors (VeriSign, CyberTrust and ORC), requesting updates of their audits.

GSA has asked ORC to provide an updated C&A package since GSA is doing an update of all systems that fall under their purview for NIST SP 800-53, she said. The other two (VeriSign and CyberTrust) were just finished, so we are just pulling ORC into alignment with the process.

Other SSPs on the Certified Providers List
She also reported that Exostar and Entrust have applied to be SSPs and that the same requirements were levied on them during the evaluation process by the SSP-WG and FICC. They are provisionally listed on the Certified Providers List on the FICC web site.

So far, we have four fully approved SSPs (VeriSign, CyberTrust, ORC, and Treasury) and two provisional SSPs (Exostar and Entrust). We have Treasury's audit letter, she said.

GPO SSP Application
John Hannan said that the GPO is now waiting for the mapping of its CPS against the Common Policy by the SSP-WG, in order to progress its application to be an SSP. That meeting has been scheduled for January 18, 2007. The SSP-WG has requested that GPO clarify some questions regarding the CPS and to make some changes before the SSP-WG mapping review, in order to streamline the process.

Once GPO passes the OCD and performs a C&A on their system, they will then be listed as an SSP, according to Tim Polk.

David Sulser (NRC) asked if OMB has a problem with Treasury and GPO becoming SSPs, since OMB has stated there will be no more self-signed PKIs in the federal government and that all agencies that do not currently have legacy PKIs will have to use SSPs.

Dr. Alterman said that OMB is aware of the Treasury SSP, but has not officially made a decision. He also noted that there are agencies that are running self-signed PKI's that have not come to the table, i.e., joined the Policy Authority. He stated that he was not in the business of being the PKI police.

Judith Spencer: Their IG's may raise this issue, e.g., CIA. She also noted that there is a Committee for National Security Systems that oversees the use of PKI in the classified environment. Members include DoD, DoS, Commerce (Bill Burr), Justice, NASA and Judith Spencer. There is a synergy and communications of sorts between the two bodies.

SSP Roadmap
Judith Spencer noted that she has updated the SSP Roadmap. The version that appears on the FICC website is out of date and does not accurately reflect the policy and practices of the FICC and SSP-WG.

She also noted that the SSP-WG is also writing a Crits and Methods document for SSPs.

ACTION: Judy Fincher is to create an Executive Summary Sheet for SSPs, noting that the ATO is unique to the SSP process.

Agenda Item 8

FPKIPA Certificate Policy Working Group (CPWG) Report

1. Near-Term Mapping Activities (SAFE pharmaceutical bridge, TAG PMA).

   Tim Polk noted these mappings are underway and that the SAFE mapping will be reviewed by the CPWG on January 16, 2007. The Americas Grid (TAG) Policy Management Agency (PMA) is expected to upgrade their policy to come in at C4 (Citizen and Commerce).

2. Status of MIT LL Interoperability Testing
   This testing has not been completed due to FPKI OA resource issues.

3. Device Cert Policy: Do we need one for the FPKIPA?
   Tim Polk said that if an agency is issuing device certs for internal operations, you do not need to issue under a policy that maps to the Federal Bridge. We have a device cert policy in the Common Policy and in ACES, he said. The use of device certs is OK and consistent with OMB Directive M-05-24 (no device certificates), provided you do not go outside your own agency. He noted that HHS had provided one to the CPWG for internal agency use. In conclusion, he said that the FPKIPA does not need a device cert policy other than that already provided in the Common Policy, ACES and FBCA CP (rudimentary coverage). The CPWG has nothing planned at this time regarding an inter-agency policy, he said.

4. New *Federal Register* Notice

   Tim Polk reported on a new *Federal Register Notice* that NIST has been asked to respond to. We're still trying to determine exactly what our role is, he said. He noted that Bill McGregor of NIST is on the email list.

The DHS/TSA has issued a news release stating that the

> "final rule for the Transportation Worker Identification Credential (TWIC) program, which enhances port security by checking the backgrounds of workers before they are granted unescorted access to secure areas of vessels and maritime facilities." The rule was posted publicly on TSA's web site January 1, 2007, and has been delivered to the Federal Register for posting in the coming days. The rule lays out the enrollment process, disqualifying crimes, usage procedures, fees and other requirements for workers, port owners, and operators. These guidelines allow the industry, government and public to prepare for the implementation of this important security program..."

It pertains to plans by the DHS/TSA to use a contactless TWIC card, biometrics and PINS to authenticate workers at US ports, starting in March 2007.

It is not yet clear if or how this new initiative will impact the FPKIPA.

Tim Polk, along with Bill Burr and Donna Dodson, will examine the *Federal Register* notice to determine whether the existing cryptography and authentication (security) infrastructure (FIPS 201) can accommodate the new DHS rule.

It's the "strongest security statement I've ever seen," Mr. Polk stated. It says that biometric information *cannot* be compromised, he said. The rule will require the TWIC card to authenticate the reader (in the future).

See the Press Release at:
http://www.tsa.gov/press/releases/2007/press_release_01032007.shtm

The Press Release also appears in Appendix B of these minutes.

Dr. Alterman felt strongly that the security requirement language has to be changed. He asked NIST to get DHS/TSA to clarify how they're going to do this. We want the TWIC card to be FIPS 201 compatible, he said.

Tim Polk said the real issue is the security impact. The FIPS 201 PIV card has never had to authenticate the reader. This is a non-trivial matter and a very hard task, he said.

Judith Spencer noted that card reader manufacturers have just re-tooled and now they will be asked to re-tool again.

5. DoD Two-Way Cross Cert Status

   Debbie Mitchell (DoD) provided a verbal summary of the progress that DoD is making in bringing up the interoperability root and two-way cross-certifying with the Federal Bridge, as requested by the Chair at the last FPKIPA meeting.

   She sent a summary slide (DoD Two-Way Cross-Certification with the Federal Bridge) via e-mail to the FPKIPA Secretary just prior to the 9 January 2007 FPKIPA meeting. The Secretary distributed it to the FPKIPA listserv after the meeting. We're moving in a forward direction, she said. The slide summarizes the progress the DoD has made regarding movement towards two-way cross-certification with the Federal Bridge. Refer to this slide, attached at the end of this document for the summary detail.

Agenda Item 9

Final Meeting Items

1. Proposed Agenda Items for next FPKIPA meeting – February 13, 2006
   Larry Shomo suggested the FPKIPA vote on the revised FBCA CP Change Proposal: 2007-01 at the next FPKIPA meeting. FPKIPA members would have two chances to submit comments to the CPWG for review (January 16 and February 1) before the next FPKIPA meeting.

   It was decided that if there are no show-stopping comments, we will vote on the FBCA CP Change Proposal: 2007-01 at the next FPKIPA meeting.

   Debbie Mitchell expressed concern with section 4.9.7, regarding off-line CA's. Currently, the DoD has no problem with this language, but that may change when DoD begins using OCSP responder certificates at some point in the future. DoD may move to a delegated Trust Model.

   ACTION: Debbie Mitchell is to send Dr. Alterman an e-mail, summarizing DoD's concerns with the FBCA Change Proposal: 2007-01. (Done)

2. Do we need to modify the Charter to require a vote on the MOA?

The general consensus was that the FPKIPA did not need to vote on the MOA. It was felt that the existing process whereby the GSA lawyer (John Cornell) negotiates the MOA with the applicant and provides it to Dr. Alterman for signature is satisfactory. Members did not want to vote on each MOA.

Judith Spencer said that we could therefore not revise the Crits and Methods to require the Policy Authority to vote on each MOA.

Tim Polk pointed out that we have a MOA template and that agencies should provide comments if they have concerns with it.

ACTION: John Cornell is to review the MOA template in light of E-Authentication PMO pressures.

3. Update of the Charter and By-Laws

Continuing the discussion regarding agencies using SSPs for their PKI services, Tim Polk suggested that maybe the By-Laws should be modified to say that agencies can vote only if they have regular attendance. Voting members should have a compelling reason to participate. If they don't participate in operating their PKI and overseeing and writing the Policy of that group, we don't want them as voting members, he said.

Judith Spencer said this is the reason for the FICC/FPKIPA partnership. The FICC is the place where everyone plays—FIPS 201 says so. They should have minimal involvement in the FPKIPA.

Dr. Alterman said that our concern is that an agency using an SSP for its PKI services may decide it wants to become a member of the Policy Authority. We should consider this. Why wouldn't we want their participation?

Tim Polk responded that the GSA is doing a Managed Service Offering and that their interests are represented here in the Policy Authority by David Temoshok.

Judith Spencer said that the Department of the Interior might also make the commitment and want to participate in the Policy Authority.

David Temoshok said this is a governance issue described currently in Section 3.1.3 of the FPKIPA Charter: "Agencies Acquiring Certificate Services from Service Providers Cross Certified with the FBCA."

This section states that:

> Vendors providing PKI certificate services are recognized and included under the e-Authentication architecture umbrella and the Common Policy Framework through both the GSA Access Certificates for Electronic Services (ACES) program (Federal Employee Profile) and the Federal Identity Credentialing Committee Shared Service Provider(SSP) program. In addition, commercial certificate service providers may be cross-certified with the Federal Bridge CA.
>
> Federal Agencies acquiring PKI certificate services using any of these mechanisms are eligible for voting membership on the PA under the following circumstances:
>
> i. The Agency expresses a desire to be a voting member of the PA, evidenced by completion of an application for membership and submission of relevant documentation for review, as described below.
>
> ii. The Agency operates its own Registration Authority, with its own certification practices statement for the registration function.
>
> iii. The Agency exercises a policy management responsibility that includes, but does not have to be limited to, authorizing and reviewing an independent, third party audit of the policies, procedures and operations of its RA functions in conformance with the Certificate Policy of the service provider.

Since we are in the process of the annual yearly update of the By-Laws and Charter, perhaps we should examine 3.1.3 to make sure this is how we want to do this. Then, we should communicate with the agencies, preferably via the FICC, Mr. Temoshok said.

ACTION: Dr. Tice DeYoung volunteered to edit the Charter, based on comments and suggestions for changes submitted by FPKIPA members.

ACTION: FPKIPA members should send their comments and suggestions for changes to the Charter—with particular attention to Section 3.1.3, to Dr. Tice DeYoung by 31 January 2007, in time for him to present these changes to the FPKIPA meeting, February 13, 2007.

Judith Spencer said that changes to the By-Laws would fall out of changes made to the Charter and would be addressed later.

4. Other Business: Miscellaneous

ACTION: Cheryl Jenkins/Darron Tate (Mitretek) will distribute the Point of Contact List to the FPKIPA listserv.

ACTION: Tim Polk will ask Dave Cooper to check that the Wells Fargo ARCOT cryptographic module is in the evaluation queue at NIST.

Judy Fincher pointed out that the May meeting will be held on May 8, not May 15, as stated on the agenda.

Dr. DeYoung announced that the NASA financial disclosure forms (OG-450's) will be signed by PKI certs this year.

Agenda Item 10

Adjourn Meeting

The meeting was adjourned at 11:30 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	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.	Peter Alterman, Rebecca Nielsen	11 July 2006	31 Jan. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	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.	et al			
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
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	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
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

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	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	Closed
262	Dr. Alterman will send a friendly e-mail, urging DoJ to keep its PKI.	Peter Alterman	9 Jan. 2007	19 Jan. 2007	Open
263	Judith Spencer will touch base with OMB to make sure they know there's an appropriation for the Policy Authority line item	Judith Spencer	9 Jan. 2007	19 Jan. 2007	Open
264	The CPWG will schedule another editing session when Rebecca Nielsen (Booz Allen Hamilton) finishes the new operational requirements section and makes the other edits identified by the CPWG at its 4 January 2007 meeting.	CPWG	9 Jan. 2007	16 Jan. 2007	Open
265	Judy Fincher is to create an Executive Summary Sheet for SSPs, noting that the ATO is unique to the SSP process.	Judy Fincher	9 Jan. 2007	31 Jan. 2007	Open
266	Debbie Mitchell is to send Dr. Alterman an e-mail summarizing DoD's concerns with the FBCA Change Proposal: 2007-01.	Debbie Mitchell	9 Jan. 2007	12 Jan. 2007	Closed
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
268	Dr. Tice DeYoung volunteered to edit the Charter, based on comments and suggestions for changes submitted by FPKIPA members.	Tice DeYoung	9 Jan. 2007	13 Feb. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
269	FPKIPA members should send their comments and suggestions for changes to the Charter—with particular attention to Section 3.1.3, to Dr. Tice DeYoung by 31 January 2007, in time for him to present these changes to the FPKIPA meeting, February 13, 2007.	FPKIPA members	9 Jan. 2007	31 Jan. 2007	Open
270	Cheryl Jenkins/Darron Tate (Mitretek) will distribute the Point of Contact List to the FPKIPA listserv.	Cheryl Jenkins Darron Tate	9 Jan. 2007	31 Jan. 2007	Open
271	Tim Polk will ask Dave Cooper to check that the Wells Fargo ARCOT cryptographic module is in the evaluation queue at NIST.	Tim Polk Dave Cooper	9 Jan. 2007	31 Jan. 2007	Open

Appendix B

This press release is from the following URL:
http://www.tsa.gov/press/releases/2007/press_release_01032007.shtm

DHS Issues Credentialing Rule to Secure Access To U.S. Ports

Press Office
Transportation Security Administration
January 3, 2006
TSA Media Inquiries Only – (571) 227-2829
U.S. Coast Guard Media Inquiries Only – (202) 372-4620
All Other Inquiries – (866) 289-9673

WASHINGTON – The Department of Homeland Security (DHS) today announced the issuance of the final rule for the Transportation Worker Identification Credential (TWIC) program, which enhances port security by checking the backgrounds of workers before they are granted unescorted access to secure areas of vessels and maritime facilities. The rule was posted publicly on TSA's web site January 1, 2007, and has been delivered to the Federal Register for posting in the coming days.

The rule lays out the enrollment process, disqualifying crimes, usage procedures, fees and other requirements for workers, port owners, and operators. These guidelines allow the industry, government and public to prepare for the implementation of this important security program.

The TSA and the U.S. Coast Guard held four public meetings around the nation and received more than 1,900 comments regarding the initial draft of this federal rule. Comments were filed by workers, port facility owners and operators, small businesses and others who would be affected by the new program. All comments were carefully considered in the development of the final rule.

The rule is expected to impact more than 750,000 port employees, longshoreman, mariners, truckers and others who require unescorted access to secure areas of ports and vessels. Specific measures include:

- Security threat assessment – TWIC applicants will undergo a comprehensive background check that looks at criminal history records, terrorist watch lists, immigration status, and outstanding wants and warrants. If no adverse information is disclosed, TSA typically completes a security threat assessment in less than ten days.

- Technology – The credential will be a Smart card containing the applicant's photograph and name, an expiration date, and a serial number. In addition, an integrated circuit chip will store the holder's fingerprint template, a PIN chosen by the individual, and a card holder unique identifier.

- Eligibility – Individuals lacking lawful presence and certain immigration status in the United States, connected to terrorist activity, or convicted of certain crimes will be ineligible for a TWIC.

- Use – During the initial rollout of TWIC workers will present their cards to authorized personnel, who will compare the holder to his or her photo, inspect security features on the

TWIC and evaluate the card for signs of tampering. The Coast Guard will verify TWIC cards when conducting vessel and facility inspections and through spot checks using hand-held readers to ensure credentials are valid. Until card reader technology is tested and a regulation issued on access control, facility owners and operators will not be required to utilize TWIC readers for facility access.

- Cost – The fee for TWIC will be between $139 and $159, and the TWIC cards will be valid for 5 years. Workers with current, comparable background checks including a HAZMAT endorsement to a commercial driver's license, merchant mariner document or Free and Secure Trade (FAST) credential will pay a discounted fee, between $107 and $127. The exact amount of the fee will be established and published once an enrollment support contract is finalized in early 2007. A subsequent Federal Register Notice will be issued at that time.

- Biometric data – Applicants will provide a complete set of fingerprints and sit for a digital photograph. Fingerprint checks will be used as part of the security threat assessment. Fingerprint templates extracted from the biometric data will be stored on the credential.

- Privacy and information security – The entire enrollment record (including all fingerprints collected) will be stored in the TSA system, which is protected through role-based entry, encryption and segmentation to prevent unauthorized use. Employees of a vendor under contract to TSA known as "Trusted Agents" will undergo a TSA security threat assessment prior to collecting biometric and biographic data of TWIC enrollees. All enrollee personal data is deleted from the enrollment center work stations once the applicant completes the process.

TWIC enrollment will begin in March of 2007, initially at a small number of ports. The implementation will comply with the schedule established in the SAFE Port Act. Additional TWIC deployments will increase and continue throughout the year at ports nationwide on a phased basis. Workers will be notified of when and where to apply prior to the start of the enrollment period in their given area. After issuance of TWIC cards to a port's workers has been accomplished, DHS will at each port establish and publish a deadline by which all port workers at that port will thereafter be required to possess a TWIC for unescorted access.

While developing the regulation for TWIC in the summer and fall of 2006, TSA completed name-based security threat assessments on port employees and longshoremen. These assessments against terrorist watch lists and immigration data sets were an interim measure and did not include the criminal history records check that will be a part of TWIC.

» **Click here** to read the Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector final rule. (1Mb, pdf)

» **Click here** for more information on port security available on the U.S. Coast Guard's Homeport site.