# Federal Public Key Infrastructure Policy Authority (FPKIPA)

## Minutes of the 12 September 2006 Meeting

Federal Trade Commission, 601 New Jersey Ave, NW, Washington, DC 20001
Conference Center: Conference Room B

## A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discussion / Vote on 11 July 2006 and August 8, 2006 FPKIPA Minutes
3) FPKI Certificate Policy Working Group (CPWG) Report
    1. *Vote on the FBCA CP Omnibus Change Proposal: 2006-02*
    2. *Vote on the MIT Lincoln Laboratory LLC Mapping at Medium and Medium Hardware*
    3. *Update on Wells Fargo (Non-Identrus)WellsSecure Mapping: Provisional Certification*
    4. *Boeing Class 3 PKI Audit Findings*
    5. *FIPS 201 Memo Update*
4) SAFE-FBCA Cross-Certification Milestones
5) FPKIPA Action Item Review
6) Vote on Policy Memo on PKI Upgrades to Medium Hardware
7) SSP-WG
8) PKI Long-Range Records Management Implications
9) FPKI Operational Authority (FPPKI OA) Report
    1. *Status of FBCA/Applicant Cross-Certification Technical Testing*
    2. Status Report, *CSP Scorecard*
    3. *FBCA TWG and PD-Val Update*
    4. *Approach to Application Testing*
10) Final Meeting Items
    - Other Topics
    - *Bridge-to-Bridge Interoperability Meeting – August 29, 2006*
    - Proposed Agenda Items for next FPKIPA meeting – October 10, 2006
        1. *e-Auth PMO Briefing (Georgia Marsh)*
        2. *Permanent Status of USPS*
        3. *Adobe Update (John Hannan)*

11) Adjourn Meeting

## B. ATTENDANCE LIST

### VOTING MEMBERS

A quorum of ten (10) voting members was present of fourteen (14) voting members, or 71%, where a quorum of 66.6% was required. Another member joined the meeting in progress, for a total of 11 (78.8%). DoD was represented by Shawn O'Brien at this meeting. OMB continues to be an ex-officio member and 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) | Tim Polk) | | |
| Department of Defense | O'Brien, Shawn | | Teleconference |
| Department of Energy | Not currently a voting member | | |
| Department of Health & Human Services | Alterman, Peter | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | Morrison, Scott | | |
| Department of State | Caldwell, Sally | | |
| Department of the Treasury | Schminky, James | | |
| Drug Enforcement Agency (DEA CSOS) | Jewell, Chris | | Teleconference |
| GPO | Hannan, John | | |
| GSA | Temoshok, David | | |
| NASA | Absent | | |
| OMB | Ex-Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | Stepongzi, Mark | | |
| USPTO | Purcell, Art | | |

**OBSERVERS**

| Organization | Name | Email | Telephone |
|---|---|---|---|
| | | | |
| Department of State (ManTech) | Froehlich, Charles R. | | |
| Department of Energy | Breland, Mary Ann | | Teleconference |
| Legal Consultant | McDowell, Gene | | |
| Enspier (Secretariat) | Fincher, Judy | | |
| Wells Fargo | Drucker, Peri | | Teleconference |
| FPKI/FICC support (FC Business Systems) | Petrick, Brant | | |
| FPKI OA Program Manager | Jenkins, Cheryl | | Teleconference |

| Organization | Name | Email | Telephone |
|---|---|---|---|
| Department of the Treasury (eValid8) | Dilley, Brian | | |
| Federal Trade Commission (FTC)<br>IT Specialist<br>Infrastructure Operations Branch, ITM | Ruff, Patrick | | |
| e-Authentication PMO | Marsh, Georgia | | |
| e-Authentication PMO | Frazier-McElveen, Myisha | | |
| FICC/GSA | Spencer, Judy | | |
| GSA | Cornell, John | | |
| State of Illinois | Anderson, Mark | | Teleconference |

## C. MEETING ACTIVITY

### Agenda Item 1

### Welcome & Opening Remarks / Introductions—Dr. Peter Alterman

This meeting took place at the Federal Trade Commission, 601 New Jersey Ave, NW, Washington, DC 20001, Conference Center: Conference Room B. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:30 a.m. with attendee introductions. He expressed his thanks to Patrick Ruff of FTC for hosting the FPKIPA at the FTC Conference Center.

### Agenda Item 2

### Discussion/Vote on 11 July 2006 and 8 August 2006 FPKIPA Minutes—Judy Fincher

Ms. Fincher stated that she received only typographical comments on the 8 August minutes and no additional comments on the 11 July 2006 minutes. The FPKIPA approved both sets of minutes, as amended, by a 2/3 vote. (10 of 14 voting members)

| Approval vote for 11 July 2006 and 8 August 2006 FPKIPA Minutes | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –Treasury ; 2nd – Justice )** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |

|  |  |  |  |
|---|---|---|---|
| GPO | X |  |  |
| GSA | X |  |  |
| NASA | Absent |  |  |
| OMB | Ex Officio Member |  |  |
| USDA/NFC | Absent |  |  |
| USPS | X |  |  |
| USPTO | Absent at the time of this vote |  |  |

## Agenda Item 3

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

1) Vote on the FBCA CP Omnibus Change Proposal: 2006-02

Tim Polk described edits made at the last CPWG meeting (September 7, 2006). He presented a hardcopy of the revised Omnibus Change Proposal and described these changes to the FPKIPA.

- The first change is to the repository availability language in 2.2.2. This language was changed to say that mechanisms and processes are "designed" to be available 99% of the time. This is a three-word change to make this a design requirement, not a performance requirement, due to the possibility of a narrow reading by compliance auditors.

  Judy Spencer explained that auditors can only look at last year's performance and see if you made 99% uptime. Auditors could make predictions as to how a PKI might operate in the future, but that is not auditable.

- The second change was to move text on key lifetimes from 5.1.6 to 6.3.2 and delete the current first paragraph in the existing 6.3.2.

Georgia Marsh: The e-Auth PMO since January has revised the legal documents to replace the Business and Operating Rules with two sets of documents: 1) Governance and Standards, 2) the Legal Suite. These will be submitted for approval to the ESC at the end of the month. Some of the requirements initially imposed in the interim Business and Operating Rules will have changed and the Policy Authority will be asked to comment on how those changes might affect the FPKI. She emphasized that the FPKI and e-Auth PMO will continue to be aligned.

A motion was made to decide whether to vote on the Omnibus Change Proposal and this was approved by a 2/3 vote, or 10 of fourteen (14) voting members. See Voting Table, below.

| Vote to Proceed to a Vote on the FBCA CP Omnibus Change Proposal: 2006-02 | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –DoS ; 2nd – Treasury )** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |
| GPO | X | | |
| GSA | X | | |
| NASA | Absent | | |
| OMB | Ex Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | X | | |
| USPTO | Absent at the time of this vote | | |

The FPKIPA then proceeded to vote on accepting the Omnibus Change Proposal. The vote to approve the Omnibus Change Proposal was taken and passed by a 2/3 majority, or ten votes. See Voting Table, below.

| Approval vote for FBCA CP Omnibus Change Proposal: 2006-02 | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion – Justice ; 2nd – DoS)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |
| GPO | X | | |
| GSA | X | | |
| NASA | Absent | | |
| OMB | Ex Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | X | | |
| USPTO | Absent at the time of this vote | | |

ACTION: Tim Polk is to distribute the revised Omnibus Change proposal to the FPKIPA listserv after the FPKIPA meeting today.

2) Vote on the MIT Lincoln Laboratory LLC Mapping at Medium and Medium Hardware

   Tim Polk stated that the CPWG had approved the mapping of MIT LL at Medium and Medium Hardware and that its audit letter was acceptable.

   ACTION: Matt King (Enspier) will prepare the MIT LL Mapping Recommendation for NIST approval.

   ACTION: Judy Fincher will conduct an e-vote for the FPKIPA to approve the MIT LL mapping recommendation, once she receives the document.

3) Update on Wells Fargo (Non-Identrus) WellsSecure Mapping: Provisional Certification

   Georgia Marsh of the e-Auth PMO joined in the discussion to emphasize the importance of granting Wells Fargo a provisional cross-certification at Basic, as the CPWG has proposed.

   Tim Polk distributed the Wells Fargo (Non-Identrus) Mapping Recommendation in hardcopy at the meeting. The CPWG has recommended that Wells Fargo be mapped at Basic and be granted a provisional cross-certification for six (6) months. In part, this is due to the e-Auth PMO's business requirements.

   He described the remaining four (4) issues:

   - The Wells Fargo cryptographic module (CM) is not conformant with FIPS 140. Their CM (Arcot) is currently going through the FIPS 140 evaluation process and Mr. Polk expects it to be approved.
   - Incompatibilities between the FBCA CP and the Wells Fargo (Non-Identrus) CP related to re-validation process requirements as implemented at Local RAs. The FBCA requires the original registration process to be repeated periodically (every 15 years for Basic). The CPWG and Wells Fargo are reviewing the re-validation process to determine whether our requirements are satisfied.
   - Whether Wells Fargo maintains subscriber identity information as required by the FBCA. If this information is not maintained, Wells Fargo will need to modify their procedures.
   - The compliance audit was performed against the initial (Identrus) CP/CPS, but the new CPS has been significantly enhanced to reflect FBCA requirements. A new compliance audit against the revised CP/CPS is needed.

The CPWG recommended issuing a cross-certificate for the remainder of the three-year period upon satisfaction of the following requirements:

- The Arcot CM completes the FIPS 140 validation process
- Wells Fargo submits a revised CPS that corrects the identified issues 2) and 3), above
- Wells Fargo submits and the CPWG approves the compliance audit for the WellsSecure CA, performed against their revised CP/CPS.

Discussion then ensued about the CPWG recommendation and the e-Auth PMO's business case.

Peter Alterman: We want PKI to be used to support e-Auth. Why can't we simply wait until they meet all the requirements identified in the CPWG recommendation?

Georgia Marsh: Wells Fargo is a member of the e-Auth Federation and is active in Federal PKI policy issues. Most of the Relying Party applications identified in the handout are e-Auth level 3. For the past year the e-Auth PMO has been working with Wells Fargo to deploy Relying Parties within the Federation.

Ms. Marsh provided a PowerPoint handout that illustrated the impact on existing agency applications (AAs) that plan to use the Wells Fargo certificates. These AAs will be affected if we can't get Wells Fargo to deploy Relying Parties (RPs) within the Federation, she said:

- GSA's E-Offer/E-Mod is already live
- Three other agency applications (State, Treasury, HHS) go live on September 30, 2006
- Three other AA's (EPA, DOI, and State) are scheduled for implementation using Wells Fargo certificates in 2007.

She assured the FPKIPA that Wells Fargo will address the remaining issues and that the e-Auth PMO will support this happening.

Tim Polk noted that for Relying Parties to be able to use these certificates, Wells Fargo must be cross-certified at a minimum at Basic (e-Auth Level 3).

David Temoshok asked Tim Polk to explain how FIPS 140 applies to non-US Government agencies and asked the Secretariat to make sure this topic was included in the minutes.

Tim Polk: FIPS regulations do not apply to non-US Government entities. The cryptographic module requirement is "out of scope" for FIPS 140. Wells Fargo is not in violation of FIPS 140, but they would be if they applied to become a Shared Service Provider (SSP).

David Temoshok: The Policy Authority may be asked to justify granting an exception to Wells Fargo regarding compliance with FIPS 140.

Tim Polk: NIST fully believes it is in everyone's greater interest to use validated products and that it is appropriate to have this requirement in the FBCA CP. Nevertheless, from a FIPS point of view, there is no issue.

Tim Polk: Can we accept this relaxation of the FIPS 140 requirement in a six-month provisional cross-certificate?

Peri Drucker (Wells Fargo): We're pushing Arcot to get their cryptographic module (CM) through the FIPS 140 validation process.

Judy Spencer: If we took out the FIPS 140 CM validated requirement from the FBCA CP, what would people present as their CM?

Tim Polk: CMs should be FIPS 140 validated, else validated against a comparable ISO standard. We can't impose FIPS requirements on foreign entities. We would be OK using ISO standards for this.

Tim Polk: The requirement is for Level 1 FIPS 140 validation; it would be level 2 or 3 for their CA.

Peri Drucker: We are not changing anything operationally since we received the original cross certificate at Medium for the Identrus CA. She briefly described Wells Fargo's response to the four issues identified by the CPWG; then added: No coding changes are required for the non-Identrus CA; there are only gaps in the descriptions in the CPS.

John Hannan suggested the FPKIPA vote to approve the provisional cross certificate at Basic, even though the FIPS 140 validation is required by the FBCA CP.

Tim Polk: On the balance of things, we can achieve Basic. We can tolerate a breach of policy for six months because the CM (Arcot) does meet our requirements, although it has not yet been formally approved.

Peter Alterman: Moreover, there is a compelling business need for the federal government.

Tim Polk: We could wait three months if there was no business need. The e-Auth PMO has a compelling business requirement. This is an acceptable way to proceed without undue risk to member agencies. We will proceed with prudence and pragmatism.

Jim Schminky: FPKIPA approval should be contingent on getting a clean copy of the latest CP/CPS before issuing the provisional cross-certificate.

Tim Polk: Before we issue the provisional cross-certificate for six months, we will get a clean copy of the CP/CPS from Peri Drucker (Wells Fargo).

John Hannan: Is this vote contingent on changes that have been agreed to?

Both Peter Alterman and Tim Polk answered, Yes.

Peter Alterman then accepted a motion to accept the CPWG Mapping Recommendation, as amended by David Temoshok.

David Temoshok: He suggested an amendment to read: "The Policy Authority recognizes the compelling federal business need to proceed with this exception vote."

Judy Spencer: Section 1.5.4 of the Omnibus Change Proposal which we just adopted stipulated, "No waivers."

Peter Alterman: This is not a waiver: only an exception.

Judy Spencer: This will only affect the e-Auth Federation, not the FPKIPA member agencies.

Georgia Marsh: She stated that there is a disconnect. The e-Auth Federation is made up of all agencies that have these requirements.

Ms. Spencer suggested that Federation representatives should hook up with their representatives on the Policy Authority.

Tim Polk was asked to give his interpretation of the "no waiver" FBCA policy.

Tim Polk: Wells Fargo may not waiver any aspect of their policy and if they do so, it must be in their CP.

The FPKIPA then voted to accept the motion to accept the CPWG mapping recommendation, as amended by David Temoshok:

> "The FPKIPA votes to approve the CPWG Mapping Recommendation for mapping Wells Fargo (Non-Identrus) WellsSecure at Basic for six months, provided they give us a clean copy of their CP/CPS prior to the issuance of the cross-certificate. This motion is in response to the compelling business requirements as stipulated by Wells Fargo and the e-Auth Federation, which represents all Federal agencies."

The vote to accept the amended motion was approved by a 78% majority of FPKIPA members, or eleven voting members, where a 2/3 majority was required. See Voting Table below.

| **Vote to accept the Amended Motion for Mapping Wells Fargo at Basic (Non-Identrus)** | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –Commerce; 2nd – Treasury)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |
| GPO | X | | |
| GSA | X | | |
| NASA | Absent | | |
| OMB | Ex Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | X | | |
| USPTO | X | | |

The FPKIPA then voted to approve mapping of Wells Fargo at Basic. A majority of 78.8% voted in favor of the motion (or eleven voting members), where a 75% majority vote was required. See Voting Table, below.

| **Vote to Approve Mapping Wells Fargo (Non-Identrus) at Basic** | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –GSA ; 2nd –Justice )** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |
| GPO | X | | |
| GSA | X | | |
| NASA | Absent | | |
| OMB | Ex Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | X | | |

| | | | |
|---|---|---|---|
| USPTO | X | | |

Dr. Alterman stated that the FPKIPA now needs to vote on cross-certifying WellsSecure at Basic for a period not to exceed six months, but only after the CPWG receives the revised Wells Fargo (non-Identrus) CP/CPS.

ACTION: Tim Polk will schedule a conference call to review the CP/CPS when it is received.

The e-vote would follow CPWG acceptance of the revised CP/CPS.

Judy Spencer pointed out the need to revoke the existing Wells Fargo certificate.

Dr. Alterman summarized:  As soon as Wells Fargo submits its revised CP/CPS, the CPWG will review it to ensure that all agreed changes have been made. At that time,   Dr. Alterman will authorize an e-vote to cross certify with WellsSecure CA and revoke all other Wells Fargo certs.

ACTION: Dr. Alterman will call for an e-vote—after the CPWG accepts the revised WellsSecure (non-Identrus) CPS—to cross-certify with Wells Fargo.

4) Boeing Class 3 PKI Audit Findings

Boeing has been successfully mapped and has completed interoperability testing, but its audit letter needs revision.  The CPWG has requested that Boeing's auditors refer to the FPKIPA "Audit Cookbook" at http://www.cio.gov/fpkipa/crosscertFPKI.htm:Procedures for Cross-Certifying with the Federal Public Key Infrastructure

> **S**ubmit a copy of the summary of your PKI's audit, stating that your operations comply with your CPS and that your CPS is in conformance with your CP.

The CPWG and Dr. Alterman are also trying to determine whether Boeing has a business requirement to be cross certified directly with the FBCA.  Boeing is already cross certified with CertiPath, a bridge that is cross certified with the Federal Bridge.

Jacqueline Knoll (Boeing) has told Dr. Alterman that NASA (Johnson Space Center) is insisting that Boeing be directly cross certified with the Federal Bridge.  Tim Polk is looking into this issue. He stated that the Policy Authority may be required to determine if there is a compelling business requirement for a separate cross certification for Boeing.

5) FIPS 201 Memo Update

Tim Polk reported that the NIST FIPS 201 Committee agrees that the FPKIPA's request—that agencies using Medium Hardware certificates not have to assert the Common Policy OIDs by January 1, 2008—is important. NIST is preparing a memorandum for the ESC. Mr. Polk is working with Bill MacGregor (NIST FIPS 201 Committee Chair) to make sure that NIST is proactive, e.g., presents a recommendation and asks for concurrence, rather than asking the ESC to solve the policy issue on its own.

Judy Spencer: This affects only the legacy PKIs who don't want to abandon their PKIs. It does not affect SSPs. It is cost prohibitive. The FPKIPA is asking that NIST modify FIPS 201 so that existing PKIs can continue to operate at Medium Hardware or High. If this doesn't happen, we will have to modify the Common Policy. If NIST gets OMB to concur with the FPKIPA position, OMB is expected to issue interim guidance.

Tim Polk: The existing FIPS 201 requirement is in essence a penalty for early adopters.

Tim Polk hopes to report back before the next FPKIPA meeting.

Judy Spencer urged that cross-certified agencies brief their representatives on the ESC so that they can influence the ESC decision.

## Agenda Item 4

### SAFE-FBCA Cross-Certification Milestones—Dr. Peter Alterman

Background
On 8/7/06 Dr. Alterman and Judy Fincher (Secretariat) met with Jerry Zagar of Northrop Grumman, who is in charge of technical policy for SAFE, the pharmaceutical PKI bridge. As a result of that meeting, Dr. Alterman reported that SAFE will be cross certifying with the Federal Bridge at Medium CBP and Medium Hardware CBP in the October 2006 timeframe—or the first open slot in the CPWG calendar. SAFE currently has 18 cross-certified members and two operational applications (HHS/National Cancer Institute and FDA).

At that meeting, both the Federal Bridge and CertiPath agreed we would follow Part III (Bridge-to-Bridge) of the Criteria and Methodology document.

At the 12 September 2006 FPKIPA Dr. Alterman presented the SAFE-FBCA Cross-Certification Milestones PowerPoint slide developed by Mr. Zagar of SAFE. We have a preliminary mutual agreement with SAFE, he stated.

Art Purcell wanted to know if there was a compelling business reason for the cross certification with the SAFE bridge.

Dr. Alterman again pointed to the fact that there are “two killer apps” at HHS (the National Cancer Institute and FDA).

Shawn O’Brien wanted to know the status of the Criteria and Methodology revision (Part III, Bridge-to-Bridge).

Dr. Alterman stated that he is working to incorporate comments provided by Rebecca Nielsen and will send it out soon.

ACTION: Dr. Alterman will write a White Paper on why we want to cross certify with SAFE, the pharmaceutical bridge.

## Agenda Item 5

### FPKIPA Action Item Review—Judy Fincher

The Secretariat (Judy Fincher) and Dr. Alterman have scrubbed the action item list and it is ready for FPKIPA review.

ACTION: Judy Fincher will send the revised action items list to the FPKIPA.

## Agenda Item 6

### Vote on Policy Memo on PKI Upgrades to Medium Hardware—Dr. Peter Alterman

This memo was distributed to the FPKIPA prior to the 12 September 2006 meeting and was discussed extensively at the last FPKIPA meeting.

The memo asks agencies running at Medium (Medium on hardware) to add the Medium Hardware OID to your OIDs—unless you are running at High.

It will be necessary for agencies to update their CPs to capture this change, but the full CP revisions will not be reviewed by the CPWG—only the sections that are changed, according to Tim Polk.

The FPKIPA voted by a majority of 78% (11/14) to accept this Policy Memo.
See Voting Table Below.

| Approval vote for Policy Memo on PKI Upgrades to Medium Hardware | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion – Commerce ; 2nd –State )** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | X | | |
| Department of Defense | X | | |
| Department of Energy | Not currently a Voting Member | | |
| Department of Health & Human Services | X | | |
| Department of Homeland Security | Absent | | |
| Department of Justice | X | | |
| Department of State | X | | |
| Department of the Treasury | X | | |
| Drug Enforcement Agency (DEA CSOS) | X | | |
| GPO | X | | |
| GSA | X | | |
| NASA | Absent | | |
| OMB | Ex Officio Member | | |
| USDA/NFC | Absent | | |
| USPS | X | | |
| USPTO | X | | |

## Agenda Item 7

### SSP-WG—Judy Spencer

In the absence of Steve Duncan, SSP-WG Chair, Judy Spencer made the report.

*Conversion of the Common Policy to 3647 Format*
Judy Spencer is in the process of converting the Common Policy Framework CP to RFC 3647 format. She is working with Enspier (the contractor) and the CPWG to create new CPS matrices. She has made “material changes” to the Policy and added new requirements in Representations and Warranties, legal issues, etc. She stated that the SSP-WG is meeting with the SSPs and SSP candidates on September 21, 2006 to present the changes. We need to make sure the SSP community can be compliant before we adopt new policy, she said. We don’t want to put in language that breaks them.

Tim Polk described his “short list” of changes made to the Common Policy to bring it into alignment with FIPS 201:

- Naming structures
- FASC-n in certs, as required in FIPS 201
- Process changes, e.g., addition of Common High
- CRL issuance frequency
- Soft shutdown requirements
- Cert lifetime and length of keys

ACTION: Judy Spencer will talk to Treasury and GPO off-line about the potential impact of the changes made to the Common Policy.

ACTION: Judy Spencer will send the revised Common Policy and matrices by COB Friday, September 15, 2006.

*Review the Entrust Mapping*
Entrust has re-submitted its CPS mapping matrix and the SSP-WG has scheduled a review meeting on September 20, 2006 at NIH/Fernwood Road.

*Mapping of Exostar*
On September 8, 2006, the SSP-WG reviewed the Exostar mapping and found six items that were “Not Comparable,” she said.

*Comparison of Common Policy to FIPS 201*
Judy Spencer reported that she is also doing a comparison of the Common Policy and FIPS 201. We need to determine where we are more stringent or where we contradict one another. She would like to see the FPKIPA issue a White Paper that informs the HSPD-12 community as to what to do.

## Agenda Item 8

### PKI Long-Range Records Management Implications—Gene McDowell

Gene McDowell, former chair of the Legal and Policy working Group and ex-representative to NOAA, reported on the study he is undertaking for the FPKIPA on the long-range records management implications for PKI.

He noted that there are two FPKI and NARA[1] publications on PKI:

- Administrative Records
- Transaction Records.

Mr. McDowell said that we need a third document in the series for long-term records. The IETF is working on federal standards and briefed the FPKI Legal and Policy Working Group in June, 2004. The consensus of that meeting was that a policy development effort is needed for data format, data retrieval, data storage, etc. Both Treasury and State have expressed strong interest in development of such a policy.

The problem would be solved by stipulating policy for long-term records management which would withstand litigation, e.g., proof of the validity of digital signatures. Failure to do so would deprive the Federal government of a legally viable PKI trust infrastructure, he said.

This proposed study should take into consideration both cost and effectiveness of competing approaches. NARA has made much progress since 2004, he noted.

[1] NARA is the US National Archives and Records Administration.

His proposed approach would be to create an inter-agency PKI long-range records management policy. This would require the participation of NARA and agencies with long-range records management processes, as well as non-federal entities. It would require the inter-operation of agencies, he said.

Judicial criteria, such as identity and non-repudiation at a defined level, should be consistent across the federal and non-federal environments, he said.

To pull this study effort together, he proposed the following processes would need to be put in place:

- o Recruitment
- o Development of Identity-relevant standards
- o Joint meetings with the FBCA-TWG, etc.
- o Holding LPWG meetings.

We should explore the feasibility of completing this work with only available volunteers, as well as a professional consulting firm, such as was done on the previous two studies with COHAS Associates.

The whole development process will probably take two years and would result in the Records Management Guidance for Federal PKI Records—Long-Term Review and Policy.

## Agenda Item 9

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

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

Ms. Jenkins noted that interoperability testing with Boeing has been completed and that the report had been sent to Judy Fincher for forwarding to the FPKIPA. Ms. Jenkins requested an e-mail vote to approve the Boeing Interoperability Report.

ACTION: Judy Fincher is to forward the Boeing Interoperability Report to the FPKIPA and ask for an e-mail vote.

She also noted that the DoD is moving towards becoming two-way cross certified and that the OA is testing with them at the end of September 2006.

MIT Lincoln Laboratory is to commence testing next week, she said.

#### 2) Status Report, CSP Scorecard

Ms. Jenkins said that the August FPKI OA Monthly Statistical Report will contain the Score Card, as requested by the FBCA-TWG. The level of operational impact is color-coded (Red, Yellow, Green) so you can easily identify the issues, she said.

## 3) FBCA TWG and PD-Val Update

Ms. Jenkins said that the requirements for deploying a test environment for directory testing have been several months in the making and that the FBCA-TWG had developed a consensus document.

ACTION: 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.

She noted that the Test Environment crashed for three days, but that she will get all test results before we deploy.

Regarding the Path Discovery and Validation methodology, she noted that the e-Auth PMO had chosen not to use that methodology as a pre-requisite for joining the e-Auth Federation.

She also noted that another FBCA-TWG product (guidance for Relying Parties) is now posted on the FPKIPA web site.

## 4) Approach to Application Testing

Ms. Jenkins stated that there is no agreement within the FBCA-TWG or PD-Val WG whether to expand the focus to PKI applications (apps). While most PKI apps are internal, the CertiPath apps are external facing. They want us to include PKITS test cases in industry testing and are looking for a Trust Model for OCSP, she said.

A special meeting is needed soon for the Audit and Legal Working Group to explore if and how to expand its scope to support PKI apps.

John Hannan: Is application verification in a B2B environment difficult?

Cheryl Jenkins: She replied that she wants one meeting before the end of the calendar year '06 to explore this topic.

ACTION: Dr. Alterman and/or the CPWG is to call a special meeting of the Legal and Policy Working Group to explore supporting PKI applications.

## Agenda Item 10

**Final Meeting Items**

- **Other Topics**
  - **Bridge-to-Bridge Interoperability Meeting – August 29, 2006**

    A sub-group of the CPWG met with CertiPath on August 29, 2006 to discuss bridge-to-bridge (B2B) interoperability issues.

    One outcome of this meeting was the decision to sponsor a B2B Interoperability Workshop, November 1-2, 2006, at Exostar in Herndon, VA. The purpose of this workshop is to develop B2B interoperability guidelines. These would be presented at the PKI R&D Workshop in April 2007.

    Participants in the workshop would be NIST (Tim Polk and Dave Cooper) and representatives from the following Bridges: FBCA (Dr. Alterman, Judy Spencer, Cheryl Jenkins) CertiPath, SAFE, HEBCA, and their vendors/operators: VeriSign's Nick Piazzola (CertiPath's vendor/operator) and CyberTrust's Russ Weiser (SAFE's vendor/operator).

- **Proposed Agenda Items for Oct. 10, 2006 FPKIPA Meeting at USPS**
  - E-Auth PMO Briefing (Georgia Marsh)
    - MOA development (alignment of the PMO and FPKI)
    - Update FPKIPA on e-Auth initiatives and policy
  - Permanent Status of USPS
  - Adobe Update (John Hannan/GPO)

## Agenda Item 11

**Adjourn Meeting**

The meeting adjourned at noon.

## 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** |
| 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 |
| 212 | Ms. Cheryl Jenkins is to develop an Approach to Application Testing for PD-Val. | Cheryl Jenkins | 14 March 2006 | 8 Aug. 2006 | Open |
| 221 | Mr. Randy Speed is to inform the FPKIPA when the NFC no longer has any certificates, so that the NFC cross-certification can be revoked. | Randy Speed | 9 May 2006 | 30 Sept. 2006 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 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 |
| 241 | Tim Polk is to distribute the revised Omnibus Change proposal to the FPKIPA listserv after the FPKIPA meeting today. | Tim Polk | 12 Sept. 2006 | 15 Sept. 2006 | Open |
| 242 | Matt King (Enspier) will prepare the MIT LL Mapping Recommendation for NIST approval. | Matt King (Enspier) | 12 Sept. 2006 | 15 Sept. 2006 | Open |
| 243 | Judy Fincher will conduct an e-vote for the FPKIPA to approve the MIT LL mapping recommendation, once she receives the document. | Judy Fincher | 12 Sept. 2006 | COB, 25 Sept. 2006 | Done |
| 244 | Tim Polk will schedule a conference call to review the CPS when it is received. | Tim Polk | 12 Sept. 2006 | 22 Sept. 2006 | Open |
| 245 | Dr. Alterman will call for an e-vote--after the CPWG accepts the revised WellsSecure (non-Identrus) CPS—to cross-certify with Wells Fargo. | Peter Alterman, Judy Fincher | 12 Sept. 2006 | 25 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 |
| 247 | Judy Fincher will send the revised action items list to the FPKIPA. | Judy Fincher | 12 Sept. 2006 | 18 Sept. 2006 | Done |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 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 |
| 249 | Judy Spencer will send the revised Common Policy and matrices by COB Friday, September 15, 2006. | Judy Spencer | 12 Sept. 2006 | 15 Sept. 2006 | Open |
| 250 | Judy Fincher is to forward the Boeing Interoperability Report to the FPKIPA and ask for an e-mail vote | Judy Fincher | 12 Sept. 2006 | 18 Sept. 2006 | Done |
| 251 | Judy Fincher is to archive the SAFE letter (in the Secretariat archives) and send the original to Cheryl Jenkins for deposit in the FPKI archives. | Judy Fincher | 12 Sept. 2006 | 18 Sept. 2006 | Done |
| 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 | Mark Stepongzi of USPS will host the October 10, 2006 meeting of the FPKIPA. | Mark Stepongzi | 12 Sept. 2006 | 10 Oct. 2006 | Open |
| 255 | Patrick Ruff of the FTC will host either the November 14 or December 12, 2006 meeting of the FPKIPA at the FTC Conference facility (601 New Jersey Avenue, NW, Washington, DC 20001) | Patrick Ruff | 12 Sept. 2006 | 10 Oct. 2006 | Open |