# Federal Public Key Infrastructure Policy Authority (FPKIPA)

## DRAFT Minutes of the 10 July 2007 Meeting

USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room: 2P316 (inside room 2P310)

### A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 12 June 2007 FPKIPA Minutes
3. FPKI Certificate Policy Working Group (CPWG) Report
    1) Results of e-vote on FBCA CP Change Proposal: 2007-03 (SAFE-Related Changes)
    2) Discuss MIT Lincoln Laboratory Audit Letter
    3) Discuss / Vote on Revised Charter
    4) C4CP Status
    5) DoD Two-way Cross Certificate (Issued 6/28/07)
    6) Vote to Cross-Certify the DoD Interoperability Root CA at Medium Hardware
4. FPKI Operational Authority (FPKI OA) Report
    1) OA Transition Status
    2) Statistical Report Status
    3) Discuss the MIT Lincoln Laboratory Interoperability Testing
5. Vote to approve the Cross Certification of MIT Lincoln Laboratory at Medium and Medium Hardware
6. DoD Statistics on Directory Issues, e.g., HTTP vs LDAP (Briefing)
7. Update on SSPWG Activities
8. Final Meeting Items
9. Adjourn Meeting

### B. ATTENDANCE LIST

#### VOTING MEMBERS

The meeting began with a quorum of 12 voting members of 14, or 85.79%, where a two-thirds majority vote was required.

NOTE: Contact information in the published FPKIPA minutes 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 | Telephone |
|---|---|---|
| Department of Commerce (NIST) - ALTERNATE | Dave Cooper | |
| Department of Defense | Mitchell, Deborah | |
| Department of Health & Human Services | Alterman, Dr. Peter | |
| Department of Homeland Security | ABSENT | |
| Department of Justice | Morrison, Scott | |
| Department of State | Gregory, Steven | |
| Department of the Treasury | Schminky, Jim | |
| Drug Enforcement Administration (DEA CSOS) | Jewell, Chris | Teleconference |
| GPO | Hannan, John | |
| GSA (FICC Chair/SSPWG Chair)- ALTERNATE | Spencer, Judy | |
| NASA | ABSENT | |
| Nuclear Regulatory Commission | Sulser, David | |

| Organization | Name | Telephone |
|---|---|---|
| USPS - ALTERNATE | Verdun, Thomas | |
| USPTO | Robinson, Quentin | |

**OBSERVERS**

| Organization | Name | Telephone |
|---|---|---|
| Department of State (Contractor -- ManTech) | Froehlich, Charles R. | |
| FPKI/FICC Support (Contractor-- General Dynamics Information Technology) | Petrick, Brant | |
| FPKIPA Secretariat (Contractor -- Enspier Technologies/Protiviti Government Services) | Fincher, Judy, Ph.D. | |
| SSA (Contractor, Jacob & Sundstrom) | Simonetti, David | Teleconference |
| E-Authentication PMO | Frazier-McElveen, Myisha | Teleconference |
| IdenTrust | Young, Kenny | |
| FPKIPA Support (Contractor—Enspier Technologies/Protiviti Government Services) | King, Matt | |
| FPKI OA (Contractor—Enspier Technologies/Protiviti Government Services, Project Manager) | Pinegar, Tim | |
| IRS/CSC (Contractor, eValid8) | Dilley, Brian | |
| Wells Fargo | Drucker, Peri | Teleconference |
| State of Illinois | Anderson, Mark | Teleconference |
| FPKI OA/GSA (PM) | Jenkins, Cheryl | Teleconference |
| DoD PKI PMO | Ryan, George | |
| DoD PKI PMO | Villasenor, Jackie | |
| DoD PKI PMO | Major David Partridge | |
| DoD PKI PMO | Wilson, Timothy W. | |
| SSA | Franey, Russell | Teleconference |
| DHS (Contractor, Cygnacom) | Shomo, Larry | Teleconference |
| KPMG | Faut, Nathan | |

**C. MEETING ACTIVITY**

## Agenda Item 1

**Welcome / Introductions—Dr. Peter Alterman, Chair**

The FPKIPA met at the USPS Headquarters Building, 475 L'Enfant Plaza, SW, Washington, DC, Conference Room: 2P316 (inside room 2P310). Dr. Peter Alterman, Chair, called the meeting to order at 9:46 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for hosting the meeting and Mr. Thomas Verdun for acting on his behalf at this meeting.

## Agenda Item 2

**Discussion / Vote on 12 June 2007 FPKIPA Minutes—Judy Fincher**
Ten of the 14 voting members voted "yes", with two abstentions. Two members were absent. This represented 10/12 or 83%) where a simple majority vote (50%) was required. Brant Petrick posted the approved meeting minutes to the FPKIPA website on July 10, 2007.

| Approval vote for 12 June 2007 FPKIPA Minutes | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion – DoS ; 2nd – Treasury)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | | | √ |
| Department of Defense | √ | | |
| Department of Health & Human Services | √ | | |
| Department of Homeland Security | ABSENT | | |
| Department of Justice | √ | | |
| Department of State | √ | | |
| Department of the Treasury | √ | | |
| Drug Enforcement Agency (DEA CSOS) | √ | | |
| GPO | √ | | |
| GSA | √ | | |
| NASA | ABSENT | | |
| Nuclear Regulatory Commission (NRC) | √ | | |
| USPS | √ | | |
| USPTO | | | √ |

## Agenda Item 3

**FPKI Certificate Policy Working Group (CPWG) Report —Dave Cooper (NIST)**

1) Results of e-vote on FBCA CP Change Proposal: 2007-03 (SAFE-Related Changes)

The FPKIPA e-vote on this change proposal was approved by all twelve (1) of the FPKIPA voting members who voted--with the following errata.

> The language in the Change Proposal is: "If the CA distributes its key in a trusted certificate, the new trusted certificate shall be distributed as specified in Section 6.1.4."
>
> The agreed revision is: "If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4."

This change did not result in any change in the meaning of Section 5.7.3, Dr. Alterman said.

| Results of the e-vote on FBCA CP Change Proposal: 2007-03 (SAFE-Related Changes) | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –; 2nd – )** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | √ | | |
| Department of Defense | √ | | |
| Department of Health & Human Services | √ | | |
| Department of Homeland Security | DID NOT VOTE | | |
| Department of Justice | √ | | |
| Department of State | √ | | |
| Department of the Treasury | √ | | |
| Drug Enforcement Administration (DEA CSOS) | √ | | |
| GPO | √ | | |
| GSA | √ | | |
| NASA | DID NOT VOTE | | |
| Nuclear Regulatory Commission | √ | | |
| USPS | √ | | |
| USPTO | √ | | |

ACTION: Judy Fincher will send the FBCA CP Change Proposal: 2007-03 to Brant Petrick, webmaster, who will make the errata changes and post it to the FPKIPA web site (Done).

ACTION: Dr. Alterman will sign the revised FBCA CP Change Proposal: 2007-03.

ACTION: Matt King will make the changes in the FBCA CP matrix, as indicated in FBCA CP Change Proposal: 2007-03.

2) Discuss MIT Lincoln Laboratory Audit Letter

The FPKIPA received a copy of the CWPG recommendation that the MIT Lincoln Laboratory Audit Letter be accepted. No vote by the FPKIPA is required, since the revised, posted Criteria and Methodology document only requires one vote by the FPKIPA, e.g., to cross-certify.

3) Discuss / Vote on Revised Charter

Judith Spencer described the changes that had been made to the Charter, e.g., voting requirements and nomenclature changes, and asked if there were any additional changes or comments.

David Sulser requested that the word SSP "vendors" be replaced in three sections (2.3, 3.1, and 3.1.1.3) with the word SSP "providers," since not all SSP providers are commercial vendors. Further, Debbie Mitchell asked for Section 2.1 to be modified, concerning CPSes. All those voting (12/12), or 100% approved these changes to the Charter, where a 75% majority vote was required.

| **Approval Vote on the Charter as revised during the 10 July 2007 FPKIPA meeting** | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –NRC; 2nd –GPO)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | √ | | |
| Department of Defense | √ | | |
| Department of Health & Human Services | √ | | |
| Department of Homeland Security | ABSENT | | |
| Department of Justice | √ | | |
| Department of State | √ | | |
| Department of the Treasury | √ | | |
| Drug Enforcement Administration (DEA CSOS) | √ | | |
| GPO | √ | | |
| GSA | √ | | |
| NASA | ABSENT | | |
| Nuclear Regulatory Commission | √ | | |
| USPS | √ | | |
| USPTO | √ | | |

4) C4CP Status

Dave Cooper said that the C4CP was revised at the June 19 CPWG meeting, but that the CPWG would have to look at the changes made to NIST SP 800-78-1 regarding the crypto algorithms, in conjunction to changes made to the FBCA CP and Common Policy. The proposed changes in SP 800-78-1 are less stringent, allowing agencies a longer transition time to 2048 bit keys.
The CPWG is meeting in a special session with the approved SSPs and other Bridges/Bridge candidates on July 17, 2007, to discuss the impact of these proposed changes on agency operations.

Dave Cooper said that, in effect, the SP 800-78-1 is a "done deal," but that there will be a two-week comment period. At that point, we will need a new Change Proposal to modify the FBCA CP and Common Policy, he said. That Change Proposal, however, is on hold until after the 800-78-1 is finalized. At that point, the FPKIPA will need to get agreement from all cross-certified members and Bridges, according to Judith Spencer.

ACTION: The FPKIPA asked that Tim Polk prepare a written rationale for these changes, since the weakness of SHA-1 and 1024 bit keys is of great concern to many members and extending their lifetime may increase the threat that these algorithms be compromised.

5) DoD Two-way Cross Certificate (Issued 6/28/07)

The FPKIPA congratulated DoD on this milestone. Debbie Mitchell said that comments and questions should be addressed to Don Fuller at Donald.Fuller.ctr@osd.mil., as requested at the 8 May 2007 FPKIPA meeting Ms. Mitchell said the DoD will do a Road show to explain how the new Interoperability Root CA will work. Dr. Alterman suggested that the road show include representatives from DoS, NASA and CertiPath, and other potential users of these certificates.

6) Vote to Cross-Certify the DoD Interoperability Root CA at Medium Hardware

The CPWG approved the DoD mapping at Medium Hardware at its June 19, 2007 meeting, Dave Cooper said, and referred to the CPWG recommendation distributed before the meeting. He explained the methodology used by the CPWG to perform this mapping, which was to look at four tables that are different between the Medium and Medium Hardware levels. This methodology will be used not only for DoD, which was previously mapped at Medium, but also for all entities cross-certified at the Medium level of assurance, who have to upgrade to Medium Hardware to satisfy PIV (FIPS 201) requirements. DoD's need to be cross-certified at Medium Hardware is being driven by the PIV requirement to support 2048-bit keys.

To be able to issue PIV Auth-compliant certs, the FIPS 201 requires agencies to be operating at Medium Hardware, according to Judith Spencer.

Dave Cooper expressed a concern that the DoD's policy might be at odds with the existing DoD CA infrastructure, which supports only 1024 bit keys. He wanted to know how long DoD proposed to issue 1024 bit keys, since they could be technically out of compliance with the 2048 bit PIV requirement starting 1/1/2008.

Jim Schminky noted that the issue at hand was whether the policy mapped and that Dave's issue, while valid, was independent of the issue on the table, which was whether the policy was compliant.

Debbie Mitchell said that DoD was meeting on the SP 800-78-1 issue this week, but that she did not have an answer yet about when DoD would be able to address the issue. She said the new Interoperability Root does not have any subordinate CAs.
.

George Ryan said that the DoD retires the CA after three years.

Major David Partridge, a guest speaker at this meeting, commented on the fact that although there is a lot of legacy equipment out there, the CAs are capable of switching to 2048-bit keys. It's the use cases that exist to support the war operations that are the issue. From a technical point of view, the hardware can handle it, but in actual usage, there is a very diverse population. We have tested that all components will work with 2048 and we are aggressively pursuing it, he said.

Dr. Alterman suggested that DoD may have to disconnect the back-end CAs from the global infrastructure and go only with the Interoperability Root CA.

Dr. Alterman then asked if the DoD Medium Hardware Policy is compliant with the FBCA Medium Hardware Policy and if there were any obstacles to cross-certifying at this time.

Dave Cooper: For three years we're been saying, certs that expire after January 1, 2008 have to support 2048 bit keys. DoD is technically not capable of doing this, at this time. I have to vote against cross-certification.

John Hannan suggested we vote to approve with the stipulation that the back end CAs that don't meet the requirement by the deadline (January 1, 2008) cannot use the Interoperability Root CA.

Judith Spencer: A letter went out from the FPKIPA last year, asking what the agencies' plans are to get to 2048 by the deadline. This is an oversight on our part. We haven't been tracking with you [the agencies] in the interim.

Steve Gregory (DoS) asked if this cross-certification will ensure that DoD has a fully functioning CA that we can communicate with. And, when can we use it?

Dave Cooper: You can communicate with the DoD Interoperability Root CA once they populate their directory, which should be by the end of this week, according to Debbie Mitchell.

Debbie Mitchell: DoD will do proofs of concept and pilots with agencies wishing to use DoD certs. We never said we would support all agencies.

The FPKIPA agreed that the DoD is compliant now for the Interoperability Root CA with 2048 bit keys until the end of the year. So, for the moment, the DoD Medium Hardware Policy is compliant with the FBCA Medium Hardware policy, as shown in the mapping performed by the CPWG.

The FPKIPA then proceeded to a vote on cross-certifying DoD at Medium Hardware. DoD recused itself from this vote, since it was the object of the vote.

Nine of the eleven voting members present voted "Yes." There was one "No" vote and one abstention, or 9/11 in favor (81.8%) where a 75% majority vote was required. The vote supported the cross-certification of the DoD at Medium Hardware.

| **Approval Vote to Cross Certify the DoD Interoperability Root CA at the Medium Hardware Level of Assurance** | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion –Treasury; 2nd –GSA)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | | √ | |
| Department of Defense | Recused for this vote | | |
| Department of Health & Human Services | √ | | |
| Department of Homeland Security | ABSENT | | |
| Department of Justice | √ | | |
| Department of State | | | √ |
| Department of the Treasury | √ | | |
| Drug Enforcement Administration (DEA CSOS) | √ | | |
| GPO | √ | | |
| GSA | √ | | |
| NASA | ABSENT | | |
| Nuclear Regulatory Commission | √ | | |
| USPS | √ | | |
| USPTO | √ | | |

## Agenda Item 4

**FPKI Operational Authority (FPKI OA) Report—Tim Pinegar (for Ms. Cheryl Jenkins)**

1) OA Transition Status—The FPKI OA is now fully transitioned, apart from a few minor administrative details.

2) Statistical Report Status

Mr. Pinegar said that three of the 10 identified issues have been resolved and that they are actively working with three others (GPO, Treasury SSP, and ORC SSP). They are still waiting for a response from DEA, Justice, Illinois, and NASA/Treasury SSP.

During the past month, the FPKI OA issued the following certificates:

i. The new Basic Wells Fargo x-cert (to add new/transitional OID)
ii. The DoD bidirectional iRoot x-cert
iii. SSA-Treasury/SSP cert
iv. Entrust SSP cert
v. VA eGov cert.

3) Discuss the MIT Lincoln Laboratory Interoperability Testing
The FPKI OA distributed the MIT Lincoln Laboratory Interoperability test report via the Secretariat prior to this meeting. The Secretariat has a copy for the record. This clears the way for a vote to cross-certify MIT Lincoln Laboratory at Medium and Medium Hardware because the mapping was completed (Sept. 06) and the audit report was satisfactory.

## Agenda Item 5

**Vote to approve the Cross Certification of MIT Lincoln Laboratory at Medium and Medium Hardware—Dr. Peter Alterman**

The FPKIPA voted unanimously to approve the cross-certification of MIT Lincoln Laboratory at Medium and Medium Hardware, or 100%, where a 75% majority vote was required.

| **Approval Vote to Cross Certify MIT Lincoln Laboratory at Medium and Medium Hardware** | | | |
|---|---|---|---|
| **Voting members** | **Vote (Motion – DoS; 2nd – Treasury)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | √ | | |
| Department of Defense | √ | | |
| Department of Health & Human Services | √ | | |
| Department of Homeland Security | ABSENT | | |
| Department of Justice | √ | | |
| Department of State | √ | | |
| Department of the Treasury | √ | | |
| Drug Enforcement Administration (DEA CSOS) | ABSENT FOR THIS VOTE | | |
| GPO | √ | | |
| GSA | √ | | |
| NASA | ABSENT | | |
| Nuclear Regulatory Commission | √ | | |
| USPS | √ | | |
| USPTO | √ | | |

ACTION: Judy Fincher is to draft an e-mail for Dr. Alterman to send to MIT Lincoln Laboratory, notifying them of their successful cross-certification at Medium and Medium Hardware. (Done)

ACTION: John Cornell is to modify the FBCA MOA template to incorporate the E-Auth PMO requirements.

ACTION: John Cornell is to initiate drafting of the MIT Lincoln Laboratory MOA.

## Agenda Item 6

**DoD Statistics on Directory Issues, e.g., HTTP vs LDAP (Briefing)—Major David Partridge**

Major David Partridge, Lead Engineer, GDS, presented the findings of a DoD comparison of HTTP vs. LDAP in delivering the payload to the FPKIPA. The Secretariat distributed the presentation prior to the meeting.

He presented statistics to demonstrate that 81% of traffic was successful (in retrieving CRLs) using HTTP, compared to 56%, using LDAP. Using HTTP for SIA, AIA and CRL DP values in certificates provides improved behavior of Microsoft CryptoAPI, HTTP caching capabilities, HTTP compression capabilities and HTTP resumption of downloads. Furthermore, he said, distributed architectures are not possible with LDAP.

The typical DoD CAC card requires 120 MB uncompressed, but only 36MB when compressed, he said.

This solution is government-owned, he said, and can be shared with other federal agencies, who can customize it for their own purposes. The plan is to make it a stand-alone appliance, out of the box, with no reliance on LDAP. This solution takes advantage of caching and compression and will go out to the infrastructure by the end of August or early September, he said.

He said DoD wanted to pursue this solution with RFC and FIPS 201 authors, to convince them to specify an HTTP solution.

Judith Spencer: FIPS 201 requires both HTTP and LDAP.

Major Partridge: It may be more beneficial to specify one or the other. There is no advantage to multi-value attributes.

Dave Cooper: Although Microsoft works well with HTTP, that is not the case for other clients. Some cannot do AIA, SIA with HTTP. We need LDAP too, else some clients will break. LDAP is used for CRL Distribution Points, he said.

ACTION: Cheryl Jenkins will have Major Partridge present the HTTP vs. LDAP briefing to the FBCA TWG at the August 2007 meeting.

For further information contact Major David Partridge at:

David.partridge@disa.mil
703-882-1674 (DoD PKI PMO)
703-601-6546 (effective September 1, 2007).

## Agenda Item 7

**Update on SSPWG Activities—Ms. Judith Spencer**

**June 28, 2007 SSPWG Meeting**

Judith Spencer reported on the work accomplished at the last SSPWG meeting, June 28. We reviewed the :

- There were minor issues with the IdenTrust CPS and accompanying mapping matrix that needs to be updated before OCD testing. Brant Petrick has sent a notice to IdenTrust asking for a date in the August 5-10 timeframe to perform OCD testing.
- The OCD with ORC is scheduled for July 12, 2007 at GSA. She noted one outstanding issue remains and that there have been many changes to the ORC CPS.
- Updated Common Policy matrix (to parallel the 3647 format Common Policy already posted to the FPKIPA web site.
- Repository Requirements and OCD Criteria documents and posted both to the FPKIPA web site.

The SSPWG feels we need an MOU-like agreement with the SSPs, saying what they will do, e.g., reporting.

Ms. Spencer will be hosting a quarterly meeting with the SSPs to keep the lines of communication open, because of the C&A process (done by GSA). The POA&M (Plan of Action and Milestones) are due in August from all of the Shared Service Providers.

Ms. Spencer feels that everything is on track but does not anticipate there will be any new SSPs.

She said that the SSPWG has to make sure all the CPSs are compliant with the Common Policy. Some will come back in at High and will need to be mapped against the new CPS mapping matrix.

She reported that several SSPs are building a core offering to offer to states and commercial entities that may issue credentials compatible with FIPS 201. But, she said, they will not express our OIDs.

David Sulser: Vendors doing clones also will market these solutions to federal agencies for services external to FIPS 201—if they do not want to do ACES.

Jim Schminky: Regarding the Managed Service Offering (MSO), Treasury does not want to pay for certs provided on the card that they are not using, e.g., Entrust comes with four certs. GPO shares the same concern.

ACTION: Judith Spencer will talk to Mike Butler of the MSO Program Office about long-term plans to provide `a la cart as well as soup to nuts MSO services.

## Agenda Item 8

**Final Meeting Items—Dr. Peter Alterman, et al.**
**(1) FPKIPA White Paper on Rich Attribute Exchange with PKI Certificates—Dr. Alterman**
Dr. Alterman said that the White Paper "Rich Attribute Exchange with PKI Certificates", was posted to the FPKIPA web site. This paper was prepared by Enspier at Dr. Alterman's request to explore ways to deliver attribute information to RPs. Dr. Alterman sent it to the OASIS PKI Technical Implementation Committee for review and comment.

ACTION: Nathan Faut (KPMG) will share the "Rich Attribute Exchange with PKI Certificates" White Paper with the Higher Education group.

**(2) FICC Meeting—Debbie Mitchell**
Ms. Mitchell reported that at the last FICC meeting Bill McGregor (NIST) indicated it was highly unlikely that the FIPS 201 will be changed to give relief to legacy PKIs regarding the requirement to express the Common Policy OIDs by January 1, 2008.

Judith Spencer agreed. It could take 18 months before we see an update to FIPS 201 and we will have to get back to them then. She said that OMB now agrees with the need to change FIPS 201. If this change does happen, Ms. Spencer will ask for a policy memo/bulletin from NIST.

ACTION: The FPKIPA agreed to modify the Common Policy so that legacy PKI agencies that are cross-certified with the Federal Bridge at Medium Hardware or Higher are considered compliant with the Common Policy and as such can continue to assert their own policy OIDs in certificates, rather than the Common Policy OIDs. This will take the form of a Change Proposal from DoD.

Jim Schminky suggested that this Change Proposal be voted on as soon as possible, so that the same personnel are in place before the upcoming election cycle.

## Agenda Item 9

**Adjourn Meeting**

The meeting adjourned at 11:55 AM. The next FPKIPA meeting is scheduled for 14 August 2007 (9:30 AM - Noon) at the USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC.

## CURRENT ACTION ITEMS

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 189 | We need to revise the MOA to accommodate E-Auth Federation requirements. Defer to after the E-auth PMO changes the Legal and Business Rules. | Peter Alterman, John Cornell, Georgia Marsh (or PMO rep) | 20 July 2006 | 31 Jan. 2007 | Open |
| 193 | Dr. Peter Alterman and the head of the OA will negotiate terms for the cross-certification process and add this language to the By-Laws document. This will be brought to the Policy Authority for a vote. (To coincide with Action Item # 189) | Dr. Peter Alterman, Cheryl Jenkins | 10 Jan. 2006 | Oct.-Nov. 2006 | Open |
| 212 | Ms. Cheryl Jenkins is to develop an Approach to Application Testing for PD-Val. | Cheryl Jenkins | 14 March 2006 | 8 Aug. 2006 | Open |
| 234 | The SSP re-write committee headed by Dr. Peter Alterman will create a new section 4 of the Crits and Methods (C&M) document for SSPs. This will bleed into the FPKIPA Charter and By-Laws. Dr. Alterman said the C&M re-write will be analogous to what we did with ACES, i.e., we ask for their bona fides: memo of application, 800-79 compliance statement, and audit summary. | Peter Alterman, Rebecca Nielsen et al | 11 July 2006 | 31 Jan. 2007 | Open |
| 237 | Dr. Alterman and Steve Duncan will talk about how the migration of FPKI agencies to Medium Hardware will affect the ACES agencies. | Peter Alterman, Steve Duncan | 8 August 2006 | 12 Sept. 2006 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 246 | Dr. Alterman will write a White Paper on why we want to cross-certify with SAFE, the pharmaceutical bridge. | Peter Alterman | 12 Sept. 2006 | 10 Oct. 2006 | Open |
| 253 | Dr. Alterman and/or the CPWG are to call a special meeting of the Legal and Policy Working Group to explore supporting PKI applications. | Peter Alterman, Tim Polk | 12 Sept. 2006 | 10 Oct. 2006 | Open |
| 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 |
| 259 | Debbie Mitchell will forward policy statements to the FPKI PA for review when available. | Debbie Mitchell | 12 Dec. 2006 | 9 Jan. 2007 | Open |
| 260 | Debbie Mitchell will confirm who will perform the C&A of the DoD root and notify the FPKI PA via email. | Debbie Mitchell | 12 Dec. 2006 | 9 Jan. 2007 | Open |
| 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 |
| 276 | Judith Spencer, Cheryl Jenkins, and Dr. Alterman will meet with the E-Auth PMO to discuss directory issues and avoid duplication of efforts. | Judith Spencer, Cheryl Jenkins, Dr. Alterman, Georgia Marsh | 13 March 2007 | 30 March 2007 | Open |
| 279 | Dr. Alterman will send out a memo to the FPKI Policy Authority and commercial cross-certified members with the FBCA to NIST SP 800-53 mapping tables attached. This memo will make a compelling case that the annual audit agencies perform will satisfy a certain portion of the 800-53 requirements, saving time and money in performing the annual PKI audits (or delta audits). | Dr. Peter Alterman | 13 March 2007 | 31 March 2007 | Open |
| 280 | Dr. Alterman will send a letter to the POC for the State of Pennsylvania, the POC for VeriSign and to the GCN with a cc: to Judy Fincher explaining that the State of Pennsylvania is not issuing HSPD-12 credentials, but credentials that are “compatible.” | Dr. Peter Alterman | 13 March 2007 | 23 March 2007 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 281 | Tim Polk will send his presentation on SHA-256 to the listserv. | Tim Polk | 13 March 2007 | 5 April 2007 | Open |
| 282 | Dr. Alterman will organize an SHA-256 migration workshop this year. | Dr. Peter Alterman | 13 March 2007 | Sept. 2007 | Open |
| 283 | Tim Polk is to present his slide presentation on SHA-256 migration to the HSPD-12 Executive Steering Committee (ESC). | Tim Polk | 13 March 2007 | May 2007 | Open |
| 285 | Judith Spencer and DoD will go off-line to discuss name uniqueness. She suspects there is name collision. | Judith Spencer, Debbie Mitchell | 8 May 2007 | 22 May 2007 | Open |
| 297 | Ms. Fincher is to issue an e-vote on 6-12-07 by COB on FBCA CP Change Proposal: 2007-03 (SAFE-related Changes), for closure by COB, Friday, June 22, 2007. | Judith Fincher | 12 June 2007 | 22 June 2007 (COB) | Open |
| 298 | Dr. Peter Alterman will contact SAFE to get a CEN requirements expert on the line with the CPWG to resolve the issue of CEN cryptographic requirements comparability with FIPS 140. Successful resolution of this issue will allow the CPWG to approve the SAFE Bridge Mapping | Dr. Peter Alterman | 12 June 2007 | 22 June 2007 | Open |
| 299 | Judy Fincher will make the editing corrections to the SAFE letter, add an internal mailing address and correct the signature bloc of Dr. Peter Alterman., and send it to Dr. Alterman and Ms. Judith Spencer. | Judy Fincher | 12 June 2007 | 13 June 2007 | Done |
| 300 | Dr. Tice DeYoung will produce an issues paper for discussion at a meeting of the SSPWG. | Dr. Tice DeYoung | 12 June 2007 | 28 June 2007 | Open |
| 301 | Dr. Alterman will sign the revised FBCA CP Change Proposal: 2007-03. | Dr. Alterman | 10 July 2007 | 20 July 2007 | Open |
| 302 | Matt King will make the changes in the FBCA CP matrix, as indicated in FBCA CP Change Proposal: 2007-03. | Matt King | 10 July 2007 | 20 July 2007 | Open |

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 303 | The FPKIPA asked that Tim Polk prepare a written rationale for these changes, since the weakness of SHA-1 and 1024 bit keys is of great concern to many members and extending their lifetime may increase the threat that these algorithms be compromised | Tim Polk | 10 July 2007 | 14 August 2007 | Open |
| 304 | John Cornell is to modify the FBCA MOA template to incorporate the E-Auth PMO requirements. | John Cornell | 10 July 2007 | 14 August 2007 | Open |
| 305 | John Cornell is to initiate drafting of the MIT Lincoln Laboratory MOA. | John Cornell | 10 July 2007 | 14 August 2007 | Open |
| 306 | Judith Spencer will talk to Mike Butler of the MSO PMO about long-term plans to provide a la cart as well as soup to nuts MSO services | Judith Spencer | 10 July 2007 | 14 August 2007 | Open |
| 307 | Nathan Faut (KPMG) will share the Rich Attribute Exchange with PKI Certificates White Paper with the Higher Education group. | Nathan Faut | 10 July 2007 | 20 July 2007 | Open |
| 308 | The FPKIPA agreed to modify the Common Policy so that legacy PKI agencies that are cross-certified with the Federal Bridge at Medium Hardware or Higher are considered compliant with the Common Policy and as such can continue to assert their own policy OIDs in certificates, rather than the Common Policy OIDs. This will take the form of a Change Proposal from DoD | Debbie Mitchell, Rebecca Nielsen | 10 July 2007 | 14 August 2007 | Open |