

Federal Public Key Infrastructure Policy Authority (FPKIPA)

DRAFT Minutes of the 14 August 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 10 July 2007 FPKIPA Minutes
3. Discuss/Vote on SSA as a Voting Member
4. Medium Hardware Policy
5. FPKI Certificate Policy Working Group (CPWG) Report
 - 1) *Review CPWG Mapping Recommendation for Treasury at Medium Hardware*
 - 2) *Discuss/Vote cross-certification of Treasury @ Medium Hardware*
 - 3) *Review CPWG Recommendation to accept the DOJ Audit Letter*
 - 4) *Review CPWG Recommendation to accept SAFE Audit Letter*
 - 5) *Discuss/Vote on FBCA CP Change Proposal: 2007-04 (Citizenship/Security Clearance)*
 - 6) *Discuss/Vote on NIST SP 800-78-1 Change Proposals:*
 - a. *Common Policy Change Proposal: 2007-01*
 - b. *FBCA CP Change Proposal: 2007-05*
 - c. *E-Governance Change Proposal: 2007-01*
6. FPKI Operational Authority (FPKI OA) Report
 - 1) *Annual Contingency Test Status*
 - 2) *Status of Directory Issues*
 - 3) *Certificate Issuance and Revocations*
 - 4) *CP/CPS Compliance Audit Update*
 - 5) *Test Environment Directory Chaining status*
 - 6) *Upcoming TWG Meeting (August 30)*
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.

We redacted contact information in the published FPKIPA minutes 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.fischer@enspier.com.

Organization	Name	Telephone
Department of Commerce (NIST) - ALTERNATE	Dave Cooper	
Department of Defense	Mitchell, Deborah	Teleconference
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	ABSENT	
Department of Justice	Morrison, Scott	

Organization	Name	Telephone
Department of State	Gregory, Steven	
Department of the Treasury- Proxy to HHS	Proxy to HHS	
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA (FICC Chair/SSPWG Chair)-ALTERNATE	Spencer, Judy	
NASA	DeYoung, Dr. Tice	
Nuclear Regulatory Commission	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO –Proxy to Commerce	Proxy to Commerce	

OBSERVERS

Organization	Name	Telephone
DoS/ PKI Program Manager, IRM/OPS/ITI/SI/IIB	McCloy, Mark A.	
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
IdenTrust	Young, Kenny	
FPKI OA (Contractor—Enspier Technologies/Protiviti Government Services, Project Manager)	Pinegar, Tim	
State of Illinois	Anderson, Mark	Teleconference
FPKI OA/GSA (PM)	Jenkins, Cheryl	
CertiPath	Takanti, Vijay	Teleconference
NRC (Contractor, VeriSign)	Evans, Frazier	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 9:40 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for hosting the meeting. The FPKIPA voted to accept the SSA/Treasury SSP as a voting member at this meeting, for a total of 15 voting members.

Agenda Item 2

Discussion / Vote on 10 July 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said that the 10 July 2007 Minutes incorrectly referred to the MIT Lincoln Laboratory having been cross-certified at Medium, whereas, the Minutes should have read, Medium and Medium Hardware. The FPKIPA voted to approve the minutes with these changes, because the CPWG successfully mapped MIT Lincoln Laboratory at Medium and Medium Hardware in September 2006.

The Charter states that approving minutes takes a majority of votes cast, not a majority of all voting members.

Ten of the 12 votes cast were “yes”, with two abstentions. Two members were absent. This represented 10/12 or 83.3% , where a simple majority vote (50%) was required. Brant Petrick posted the approved meeting minutes to the FPKIPA website on August 14, 2007.

Approval vote for 10 July 2007 FPKIPA Minutes			
Voting members	Vote (Motion –NASA ; 2nd – DoS)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
USPS	√		
USPTO –Proxy to Commerce			√

Agenda Item 3

Discuss/Vote on SSA as a Voting Member—Dr. Peter Alterman

Dr. Alterman said he had received a letter and a completed application form (a Signed PDF) from the SSA requesting membership as SSA/Treasury SSP. The principal representative will be Eric Mitchell and the alternate is Greg Elspas. The FPKIPA approved the SSA as a voting member of the FPKIPA by 85.7% (12/14) where a majority vote of ¾ was required. All members present supported the SSA/Treasury SSP joining the FPKIPA. Two members were absent.

Approval vote for SSA to Join the FPKIPA as a Voting Member			
Voting members	Vote (Motion –NASA ; 2nd – NRC)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
USPS	√		
USPTO –Proxy to Commerce	√		

Agenda Item 4

Medium Hardware Policy—Dr. Peter Alterman

Dr. Alterman said that he posted this memo to the FPKIPA website on 12 September 2006. It required that agencies currently cross-certified at Medium to upgrade to Medium Hardware by October 27, 2007. This is driven by HSPD-12, not by the FPKI PA, and the clock is ticking, he said. So far, only Treasury and DoD have completed the upgrade. The CPWG reviewed the four “delta” tables (the difference between Medium and Medium Hardware) and will do so for all other cross-certified agencies. Dr. Alterman noted that HHS is abandoning its ACES PKI solution and will obtain PKI SSP services from Cybertrust before the October 27, 2007 HSPD-12 deadline. He urged all agencies to move quickly to comply with this requirement.

Agenda Item 5

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

- 1) Review CPWG Mapping Recommendation for Treasury at Medium Hardware

Mr. Cooper said the CPWG successfully mapped Treasury Level 3 at Medium and Treasury Level 4 at High in 2002. The CPWG then successfully mapped Treasury Level 3 at Medium Hardware at the 2 August 2007 meeting. The FPKIPA accepted this recommendation, but Dr. Alterman noted that no vote is required any longer to approve a CPWG mapping recommendation (as per the revised Criteria and Methodology); the FPKIPA only votes on cross-certification unless there are compelling reasons to take a vote when there are mapping or audit concerns.

2) Discuss/Vote cross-certification of Treasury at Medium Hardware

Treasury had previously been cross-certified at Medium and High, corresponding to Treasury Level 3 and 4, respectively. There are only four tables in the mapping matrix that distinguish Medium from Medium Hardware. The CPWG successfully mapped Treasury at Medium Hardware, using this “delta” mapping approach, on August 2, 2007. The vote to cross-certify Treasury at Medium Hardware passed by 85.7% (12/14) where a majority vote of ¾ was required. Treasury recused itself from this vote, so was not included in the total of voting members.

Approval vote to Cross Certify Treasury at Medium Hardware			
Voting members	Vote (Motion –NASA ; 2nd – NRC)		
	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 –Proxy to HHS	RECUSED		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO –Proxy to Commerce	√		

3) Review CPWG Recommendation to accept the DOJ Audit Letter

The FPKIPA accepted the CPWG recommendation; no vote was required.

4) Review CPWG Recommendation to accept SAFE Audit Letter

While the SAFE audit was good, the CPWG found the relationship between the auditor and author of the CPS was not clear-cut. The auditor worked for the same organization (Orion, a division of Entrust) as the author of the CP, although there was no direct reporting relationship. This recommendation is based on the premise that, going forward, no one associated with the operation or documentation of the PKI can also be the auditor.

The FPKIPA agreed to accept the CPWG recommendation if this stipulation is incorporated into the MOA.

5) Discuss/Vote on FBCA CP Change Proposal: 2007-04 (Citizenship/Security Clearance)

This Change Proposal has been discussed thoroughly by the CPWG and the FPKIPA in prior meetings. The only difference in this version of Change Proposal: 2007-04 is that it

incorporates language from the DoD and Department of State (DoS) lawyers that all parties agreed to. The FPKIPA approved the FBCA CP Change Proposal: 2007-04 by an 80% vote (12/15) where a $\frac{3}{4}$ majority vote was required.

Approval vote on FBCA CP Change Proposal: 2007-04			
Voting members	Vote (Motion –DoS; 2nd – USPS)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO –Proxy to Commerce	√		

ACTION: Brant Petrick (WebMaster) will post the revised, final version of the FBCA CP Change Proposal: 2007-04 to the FPKIPA website.

6) Discuss/Vote on NIST SP 800-78-1 Change Proposals:

The purpose of the following three Change Proposals is to modify the three policies (FBCA CP, Common Policy CP, and E-Gov CP) to bring them into alignment with the new, relaxed SHA and RSA requirements. The revised NIST SP 800-78-1 guidelines allow SHA-1 to be used for three more years and RSA 1024 to align with 800-78-1, also. There was discussion about voting all three as one vote, but several members insisted on keeping the votes on the three policies separate.

Dave Cooper clarified that agencies may use 2048 bit keys and SHA-256 now if they choose.

David Sulser said that it is also true that an agency using SHA-256 now can decide not to rely on agencies using SHA-1

Judith Spencer pointed out that SHA-1 attacks had not been duplicated in the real world, only on paper, which had been able to detect collisions.

Dave Cooper said that trying to come up with the collision against an existing signature is not feasible.

Judith Spencer said that NIST reserves the right to withdraw 800-78-1 with the relaxed SHA-1 requirements if and when SHA-1 is broken. She said this is a calculated risk, that SHA-1 will be broken between 2010 and 2014. However, if we require only SHA-256 by

January 1, 2008, nothing will work unless all agencies install VISTA before the end of December 2007. Support for SHA-256 does not exist on the XP platform, she said.

Judith Spencer said that the FPKIPA would pressure NIST to change the 800-78-1 requirements if Microsoft Service Pack 3 due out next year supports SHA-256.

Dr. Tice DeYoung objected to relaxing the SHA-256 and 2048-bit key requirements. It is tantamount to weakening the entire PKI infrastructure, he said. Dr. DeYoung reported that he had heard a rumor that Microsoft would back –fill for Windows XP in Service Pack 3 and Service Park 1 for VISTA. After 31 December of this year agencies can issue two-year credentials. What this basically gives us is a year in which to keep the pressure on Microsoft to fix the shortcomings in their XP and VISTA OSes.

Judith Spencer said that agencies having to meet HSPD-12 requirements simply would not issue two-year certificates.

ACTION: Dr. Tice DeYoung will make a presentation at the next FPKIPA meeting on the Entrust “shim” solution, September 11, 2007.

- a. Common Policy Change Proposal: 2007-01
The FPKIPA vote to approve this Change Proposal passed by 80% (12/15), where a majority vote of ¾ was required.

Approval vote on Common Policy Change Proposal: 2007-01			
Voting members	Vote (Motion –GSA 2nd – DoS)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA		√	
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO –Proxy to Commerce	√		

- b. FBCA CP Change Proposal: 2007-05
 The FPKIPA vote to accept this change proposal failed by 66.7% (10/15), where a majority vote of $\frac{3}{4}$ was required.

Approval vote on FBCA CP Change Proposal: 2007-05			
Voting members	Vote (Motion –DoS; 2nd – GSA)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA		√	
Nuclear Regulatory Commission (NRC)			√
SSA	√		
USPS	√		
USPTO –Proxy to Commerce	√		

- c. E-Governance Change Proposal: 2007-01
 The FPKIPA vote to approve this Change Proposal passed by 80% (12/15), where a majority vote of $\frac{3}{4}$ was required.

Approval vote on E-Governance Change Proposal: 2007-01			
Voting members	Vote (Motion –DoS; 2nd – GSA)		
	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 –Proxy to HHS	√		
Drug Enforcement Agency (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA		√	
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO –Proxy to Commerce	√		

Agenda Item 6

FPKI Operational Authority (FPKI OA) Report— Cheryl Jenkins, Tim Pinegar

- 1) Annual Contingency Test Status (Cheryl Jenkins)
Ms. Jenkins said she had performed a “table top” contingency test last week at the GSA. This was done to train people in case we have a disaster, she said. The report is due to her on August 15 and she will submit it to the CIO Council on August 17, 2007.
- 2) Status of Directory Issues (Tim Pinegar)
The goal, Mr. Pinegar said, is to clean up the Directory and start producing the monthly statistical report in September.

Of the 16 issues that have been identified over the past 6 months, there are now five remaining.

1. DEA Chaining issue
 2. DHS Cross-cert issue
 3. Treasury Cross-cert issue
 4. State of Illinois cert profile issue. Their cert expired as of today, Ms. Jenkins said.
 5. A NASA issue that cannot be addressed until they migrate to their SSP CA (NOCA).
- 3) Certificate Issuance and Revocations (Tim Pinegar)
Mr. Pinegar said the OA had issued six certs: GPO, VA, NASA/Treasury SSP, SSA/Treasury SSP, Wells Fargo and DoD Interoperability Root.
 - 4) CP/CPS Compliance Audit Update (Cheryl Jenkins)
Ms. Jenkins said she had received an extension from the Policy Authority due to budgetary issues. She expects to have all the FPKI OA CPSes updated to 3647 format by early November and should have the auditor onboard.
 - 5) Test Environment Directory Chaining status (Cheryl Jenkins)
Ms. Jenkins reiterated the need for test environments that mirrors what we are doing in the production environment. She is waiting to hear from the agencies as to what their plans are. She noted that DoD is doing applications testing, working through PIV card and validation issues. And, she said, GPO had been very responsive submitting information on their test environment.

Ms. Jenkins said that Terry McBride, the new lab test manager, sent an e-mail to the FPKIPA asking who was chained to the Directory before Enspier took over early this year.

- 6) Upcoming TWG Meeting (August 30) (Cheryl Jenkins)
Ms. Jenkins said the next meeting of the FBCA TWG would be held August 30 at Enspier. She asked cross-certified members to send their technical representatives. The following topics will be discussed at that meeting:
 1. The re-Design of the FPKIA. She notes that Enspier had added business and technical drivers for why we need a re-design. The draft is under review, she said.
 2. Cost Analysis for Test Environments
 3. Service Level Agreement (SLA)

Agenda Item 7

Update on SSPWG Activities—Judith Spencer

OCD with IdenTrust

Ms. Spencer said that the SSPWG held an Operational Capabilities Demonstration (OCD) with IdenTrust last week and that she and Dave Cooper are drafting a letter to IdenTrust with the results of the OCD.

ORC Issues

We are continuing to work through outstanding issues with ORC. ORC has CRLs with a one-year lifetime (under the ACES cross-certificate). This affects the SSPWG because the SSP ORC certificates come under the ACES root.

August 27, 2007 Meeting with the SSPs

Ms. Spencer said she is holding the quarterly meeting with the SSPs on August 27. There are real trust issues to be addressed, she said. Within 18-24 months over a million credentials will rely on the Common Policy root. We have to stipulate how this works, so we do not run into interoperability issues. Tim Polk has drafted "Proposed Rules of the Road," which consists of guidance to SSPs. This document, which seeks to provide clarity on subordination to the Common Policy root, will be presented to the SSPs at the 27 August 2007 SSP Quarterly meeting during the 10:30 a.m. session. The earlier session will be devoted to GSA walking the SSPs through the C&A process.

Agenda Item 8

Final Meeting Items

Liberty Alliance Initiative

Judith Spencer reported on a Liberty Alliance initiative she is supporting as a voting member from GSA Office of Governmentwide Policy (OGP). Last week she attended the founding meeting of a new initiative with Liberty Alliance, the Identity Assurance Expert Group (IAEG). You do not have to be a member of the Liberty Alliance to participate, she said.

This IAEG replaces the defunct E-Authentication Partnership (EAP), an initiative of the GSA OGP and E-Authentication PMO. The EAP attempted to develop an accreditation schema for individuals to develop certification practices, but it did not fulfill its promise, she said.

Status of the FPKIPA Memo to OMB

Scott Morrison asked about the status of the FPKIPA Memo to NIST/OMB regarding the requirement in FIPS 201 that legacy PKI agencies have to express the Common Policy OIDs by January 1, 2008.

Judith Spencer said that there was an agreement in principal with NIST about the desirability of this change to the FIPS 201.

Dr. Alterman said that Bill McGregor had said this was a “done deal” a couple of months ago.

ACTION: Judith Spencer will update the FPKIPA on the status of the FIPS 201 modification to remove the requirement for agency legacy PKIs asserting the Common Policy OIDs by January 1, 2008.

ACTION: Debbie Mitchell volunteered to draft a memo for OMB signature that Mary Dixon will present at the next ESC.

NASA Issue

Drs. DeYoung and Alterman engaged in a discussion about NASA complying with the FBCA requirement that the CA have policy mapping in the cross-certificate.

ACTION: Dr. Peter Alterman will send an e-mail memo to NASA stating that if NASA doesn't comply by the end of September 2007 with the FBCA requirement that the NASA CA have policy mapping in the cross-certificate, he would revoke the FBCA cross-certificate with NASA.

Agenda Item 9

Adjourn Meeting

The meeting adjourned at 11:50 AM. The next FPKIPA meeting is scheduled for 11 September 2007 (9:30 AM – 11:30 a.m. at the USPS Headquarters, 475 L’Enfant Plaza, SW, Washington, DC.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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

No.	Action Statement	POC	Start Date	Target Date	Status
212	Ms. Cheryl Jenkins is to develop an Approach to Application Testing for PD-Val.	Cheryl Jenkins	14 March 2006	8 Aug. 2006	Open
234	The SSP re-write committee headed by Dr. Peter Alterman will create a new section 4 of the Crits and Methods (C&M) document for SSPs. This will bleed into the FPKIPA Charter and By-Laws. Dr. Alterman said the C&M re-write will be analogous to what we did with ACES, i.e., we ask for their bona fides: memo of application, 800-79 compliance statement, and audit summary.	Peter Alterman, Rebecca Nielsen et al	11 July 2006	31 Jan. 2007	Open
237	Dr. Alterman and Steve Duncan will talk about how the migration of FPKI agencies to Medium Hardware will affect the ACES agencies.	Peter Alterman, Steve Duncan	8 August 2006	12 Sept. 2006	Open
246	Dr. Alterman will write a White Paper on why we want to cross-certify with SAFE, the pharmaceutical bridge.	Peter Alterman	12 Sept. 2006	10 Oct. 2006	Open
253	Dr. Alterman and/or the CPWG 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
281	Tim Polk will send his presentation on SHA-256 to the listserv.	Tim Polk	13 March 2007	5 April 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
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
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
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
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
309	Dr. Tice DeYoung will make a presentation at the next FPKIPA on the Entrust "shim" solution), September 11, 2007.	Tice De Young	14 Aug. 2007	11 Sept. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
310	Brant Petrick (Web Master) will post the revised, final version of the FBCA CP Change Proposal: 2007-04 to the FPKIPA website.	Brant Petrick	14 Aug. 2007	17 Aug. 2007	Closed
311	Debbie Mitchell volunteered to draft a memo for OMB signature that Mary Dixon will present at the next ESC.	Debbie Mitchell	14 Aug. 2007	11 Sept. 2007	Open
312	Dr. Peter Alterman will send an e-mail memo to NASA stating that if NASA doesn't comply by the end of September 2007 with the FBCA requirement that the NASA CA have policy mapping in the cross-certificate, he would revoke the FBCA cross-certificate with NASA.	Dr. Alterman	14 Aug. 2007	11 Sept. 2007	Open