Federal Public Key Infrastructure Policy Authority (FPKIPA)

DRAFT Minutes of the 11 September 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 14 August 2007 FPKIPA Minutes
3. Presentation on Entrust SHA-256 "Shim" Solution
4. Chair's Comments
    1) Medium Hardware Reminder
    2) 3647 RFC Format Reminder
5. Audit Working Group Report
    1) NIST SP 800-53A Memorandum from FPKIPA Chair
    2) ISO 27001 to NIST SP 800-53A Mapping
6. FPKI Certificate Policy Working Group (CPWG) Report
    1) *Discuss/Vote on FBCA CP Change Proposal: 2007-05 (NIST SP 800-78-1)*
    2) *Discuss/Vote to Remove Wells Fargo Provisional Basic Status*
    3) *Discuss Common Policy Change Proposal: 2007-0a: Requiring the inclusion of a subject DN in PIV Authentication Certificates*
7. FPKI Operational Authority (FPKI OA) Report
    1) *Introduction of new OA Team Technical Lead*
    2) *Status of Directory Issues*
    3) *Report on the FBCA TWG Meeting (August 30, 2007)*
        a. *FPKIA Redesign*
        b. *Test Environment Requirements (with cost analysis and SLA/MOA)*
    4) *Federal Common Policy CA Key Rollover*
8. Update on SSPWG Activities
    1) Report on SSP Quarterly Meeting (August 27 2007)
    2) IdenTrust OCD Follow-on
    3) Update on FIPS 201/Common Policy Alignment
9. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 11 voting members of 15, or 73%, where a two-thirds majority vote was required. A 12th member joined at Agenda Item No. 4 (a).

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.fincher@enspier.com.

Organization	Name	Telephone
Department of Commerce (NIST) - ALTERNATE	Cooper, Dave	
Department of Defense --Alternate	O'Brien, Shawn; then Mitchell, Deborah	Teleconference Teleconference
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	ABSENT	

Organization	Name	Telephone
Department of Justice	Morrison, Scott	
Department of State	McCoy, Mark	
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-PROXY TO HHS	Proxy to HHS	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	Robinson, Quentin	Teleconference

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
FPKIPA Support (Contractor --Enspier Technologies/Protiviti Government Services)	King, Matt	
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	
Wells Fargo	Drucker, Peri	Teleconference
NRC (Contractor, VeriSign)	Evans, Frazier	
KPMG	Faut, Nathan	
FPKI OA Support-Technical Lead (Enspier, Contractor)	Brown, Wendy	

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 9:30 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for hosting the meeting.

Agenda Item 2

Discussion / Vote on 14 August 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said that she had incorporated comments received on the 14 August 2007 FPKIPA Minutes and asked the Policy Authority to approve the minutes, as amended. Treasury moved that the minutes as amended be approved, and USPS seconded.

Nine of the 15 voting members voted to approve the minutes, including two abstentions. Four members were absent. This represented 9/15, or 60%, where a simple majority vote (50%) was required. Brant Petrick, FPKIPA Web Master, posted the approved meeting minutes to the FPKIPA website on September 12, 2007.

Approval vote for 14 August 2007 FPKIPA Minutes			
Voting members	**Vote (Motion – Treasury ; 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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	ABSENT FOR THIS VOTE		
GSA	√		
NASA	ABSENT		
Nuclear Regulatory Commission (NRC)-Proxy to HHS	√		
SSA	ABSENT		
USPS	√		
USPTO			√

Agenda Item 3

Presentation on Entrust SHA-256 "Shim" Solution—Dr. Tice DeYoung/Entrust

Dr. DeYoung was absent, as was Entrust. NOTE: This solution has been over-taken by Events (OBE) because of Microsoft's commitment to providing support for SHA-256 in XP and Windows Server 2003.

Agenda Item 4

Chair's Comments—Dr. Peter Alterman

1. **Medium Hardware Reminder**
   Dr. Alterman reminded the FPKIPA that members cross-certified at Medium need to satisfy the HSPD-12 requirement by October 27, 2007. Members may either upgrade to Medium Hardware or use the services of an SSP, he said. Thus far, only two agencies (DoD and Treasury) have cross-certified at Medium Hardware. Sixteen months ago, he said, the FPKIPA agreed that agencies could upgrade by making operational changes and by making minor policy changes by October 27, 2007.

   The CPWG is assisting in the migration of agencies to Medium Hardware by mapping the four "delta" tables only, e.g., the tables in Medium Hardware not found in the Medium Policy. Judith Spencer reminded the FPKIPA that ACES Federal credentials are supposed to be sunset soon.

   ACTION: Dr. Alterman will contact each cross-certified member (who has not upgraded yet) to find out their strategy and whether or not they will be able to meet the October 27, 2007 deadline.

   We do not plan to revoke your cross-certificates, he said, but be aware that if you do not comply with this requirement, you will not be able to issue HSPD-12 credentials.

2. **3647 RFC Format Reminder**

   Dr. Alterman reminded the FPKIPA that they should convert their CPs from RFC 2527 format to RFC 3647 format by December 31, 2007. So far, we have mapped DoD at 3647, but need an assertion letter to that effect. Both DoS and the State of Illinois have provided assertion letters, already.

   ACTION: DoD will send an email asserting that the DoD CP is in RFC 3647 format. (Done)

Agenda Item 5

Audit Working Group Report —Dr. Peter Alterman

1. **NIST SP 800-53A Memorandum from FPKIPA Chair**
   Dr. Alterman said he sent the memo to all Agency CIOs last week, with a hyperlink to the 800-53 –to- FBCA & Common CPs mapping table. The memo deals with the "Reuse of PKI Compliance Audit Results in Federal IT Systems Security Reviews and Certification and Accreditation Reviews." The mapping tables show how many of the 800-53A security controls the two FPKI policies meet, and flags those that are not met.

   ACTION: Judith Spencer will send the NIST SP 800-53A memo to Sr. Agency Information Security Officers this week. (Done)

ACTION: Dr. Peter Alterman will send the NIST SP 800-53A memo to the FPKIPA listserv. (Done)

2. ISO 27001 to NIST SP 800-53A Mapping

Dr. Alterman said that Richard Wilsher of the Zygma Partnership, LLA, and ISO expert is working on the mapping between 800-53A and ISO 27001 (ISMS management requirement). Mr. Wilsher is working in cooperation with the NIST FISMA implementation team headed by Ron Ross. Auditors from the Austin School of Business are also working on this project. This is the kind of activity that helps us all, he said.

Dr. Alterman said he had been asked--but had declined--to conduct a mapping of NIST SP 800-53A and the Health Insurance Portability and Accountability Act (HIPAA) because there was no funding.

Agenda Item 6

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

1) *Discuss/Vote on FBCA CP Change Proposal: 2007-05 (NIST SP 800-78-1)*
The FPKIPA agreed to conduct an e-vote (Motion by GSA, seconded by GPO) on this important topic, since it is impossible to obtain a 75% majority if more than two members are absent—even if all agencies vote "yes." This gives everyone an opportunity to vote, Dr. Alterman said.

2) *Discuss/Vote to Remove Wells Fargo Provisional Basic Status*
The Wells Fargo Provisional Basic cross-certification expires the end of September and required a 75% vote by the FPKIPA to remove the provisional status. Peri Drucker (Wells Fargo) said in the meeting that the ARCOT version currently in use by Wells Fargo customers is not the same version NIST validated. Consequently, the FPKIPA could not vote to remove the Wells Fargo Provisional Basic status at this meeting.

The FPKIPA agreed to conduct an e-vote the last week of September (by COB September 28) or as soon as Wells Fargo upgrades to the ARCOT HSM recently validated by NIST. Peri Drucker promised to notify the FPKI PA as soon as Wells Fargo has updated the HSM.

ACTION: The Secretariat will conduct an e-vote by COB September 28, or as soon as Wells Fargo upgrades to the ARCOT HSM recently validated by NIST, to remove the Provisional Basic Status of the existing Wells Fargo Cross-Certificate.

3) *Discuss Common Policy Change Proposal: 2007-0a: Requiring the inclusion of a subject DN in PIV Authentication Certificates*

The purpose of this Change Proposal is to enable us to map PIVAuth to the FBCA CP. For Common, the subject DN is optional in the PIVAuth Cert;

whereas, the FBCA says it is mandatory for Basic and above. The solution is to make the subject DN mandatory in the PIVAuth cert.

Judith Spencer briefed the SSPs about this change and requested them to let her know by September 14 (COB) if there is any adverse impact on them.

ACTION: Judy Fincher will conduct an e-vote on Common Policy Change Proposal: 2007-oa (or 2007-02) on September 21, 2007, provided that Judith Spencer confirms there is no adverse effect on the SSPs.

Debbie Mitchell submitted a Change Proposal to the CPWG (Dave Cooper and Judith Spencer) and requested a review. Dave Cooper and Judith Spencer have drafted a comprehensive Change Proposal for the Common Policy, to align it with FIPS 201, incorporating most but not all of DoD's concerns. (DoD can still not meet the Common Policy as currently revised).

Agenda Item No. 7

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

1) *Introduction of new OA Team Technical Lead (Tim Pinegar)*
Tim Pinegar, FPKI OA Project Manager (contractor), introduced the newest member of his team, Wendy Brown, who will be the OA team technical lead. She will spearhead efforts to fix the X.500 Directory, which has been experiencing outages.

2) *Status of Directory Issues (Cheryl Jenkins, Tim Pinegar)*
Ms. Jenkins said she suspects that a memory leak is causing the directory problem. The push rate of the CRLs may also be a factor, she said. It is not an Isode software problem, she said. She noted that the OA is trying to resolve on-going technical problems and still have not been able to work with Treasury, State of Illinois, DHS and NASA.

3) *Report on the FBCA TWG Meeting (August 30, 2007)*
   a. *FPKIA Redesign (Tim Pinegar*)
   Feedback from the FBCA TWG after the briefing on the new FPKI Architecture on August 30, 2007, has been positive. It indicates we are heading in the right direction, he said. He said that the plan is to sunset the X.500 directory by the end of 2008 calendar year. The 99.9% directory availability requirement has been changed to 95.5% and the workforce requirements have also changed. Ms. Jenkins said she expects to rollout the new FPKIA in March 2008. The primary and backup sites will be working at commercial level. We will phase in the third site later, she said.

   b. *Test Environment Requirements (with cost analysis and SLA/MOA) (Cheryl Jenkins, Tim Pinegar)*

We are looking for each cross-certified entity – not just Federal agencies – to set up a test environment by December 31, 2008, Mr. Pinegar said. The SLA will become a MOA, Ms. Jenkins said.

Ms. Jenkins asked for feedback at the Program level as to whether this is doable. We provided cost estimates, assuming a rate of $120/hour for set up and maintenance. The next step is for each cross-certified entity to look at the requirements and determine what it will cost that agency.

Jim Schminky objected to the notion that the test environment should be kept up at all times and advocated scheduling testing events, instead.

Both Judith Spencer and Dr. Alterman spoke to the need to provide a secure, solid solution for making PKI work on the Federal Government Identity Card. PKI is about to become the central security piece of the Federal Government Identity Card, according to Ms. Spencer. We need to be a commercial grade provider, utilizing the Bridge, and we need to be able to accept certificates from other agencies. We need to "beg, borrow, and steal" to make this test environment work. Judith Spencer is preparing a high-level briefing on the need for a test environment at GSA. Jim Schminky urged her to emphasize OMB M-06-16 (encryption and two-factor authentication) in her justification, as well as the VA PII loss (secure archiving).

Cheryl Jenkins urged FPKIPA cross-certified members to do a cost analysis, based on the minimal set of Test Environment Requirements (TER). She asserted that agencies would spend more time and money continually breaking down and standing up their test environments, than by maintaining a dedicated test environment. Jim Schminky disagreed. He advocated putting out a test schedule that we know in advance.

Charles Froehlich said that the DoS test environment is for internal use only, for the testing of HSPD-12 and PKI. Moreover, the test environment is changing daily, as testing requirements change; and there is no directory, he said.

Either Ms. Jenkins or her staff will brief the FPKIA at the November 13, 2007 FPKIPA meeting, and that approval of the Test Environment Requirements (TER) is required. We need to hear alternative proposals, also, she said.

ACTION: Judy Fincher will put a presentation on Test Environment Requirements on the agenda for the 13 November 2007 FPKIPA meeting. (Done)

4) *Federal Common Policy CA Key Rollover*
Dave Cooper explained that the SSPs need key rollover and that he had sent them a plan, which the OA then simplified. He will examine it this week to make sure the technical approach is in line with the policies. He plans to send the revised plan to the SSPs this week so that Common Policy CA key rollover can be done next week. This will include the Common Policy DN, he said.

Dave Cooper then suggested that the Common Policy Common Name be changed to read: "US Federal Common Policy Root CA."

The FPKIPA voted 12/15 or 80% to approve the name change, where a 75% majority was required.

Approval vote to change the Common Policy Common Name to "US Federal Common Policy Root CA"			
Voting members	**Vote (Motion – Treasury ; 2nd – DoS)**		
	Yes	**No**	**Abstain**
Department of Commerce	√		
Department of Defense	√		
Department of Health & Human	√		
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 – Proxy to HHS	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

.

Agenda Item 8

Update on SSPWG Activities—Judith Spencer

1. **Report on SSP Quarterly Meeting (August 27, 2007)**
Ms. Spencer reported on her meeting with the SSPs. The first half of the meeting was a learning experience for both GSA and the vendors. GSA led the vendors through the C&A process. The GSA is trying to put in place "unique" entities that will provide services to the Federal Government. GSA wants to designate an SSP as a government-owned system. In that case, FISMA would apply. Ms. Spencer contends that a SSP touches the Federal Government, but the Federal Government does not own it. Jim Schminky said the IG and GAO will resist this interpretation and that we need to lobby Congress to make this happen.

2. **IdenTrust OCD Follow-on**
There were some issues and IdenTrust has responded. Ms. Spencer will schedule an SSPWG meeting the third week in October (when she returns from vacation.)

3. Update on FIPS 201/Common Policy Alignment

Ms. Spencer said that OMB will try to provide relief to legacy PKIs in FIPS-201, which it is trying to publish before the end of this calendar year. OMB will not issue interim guidance. Legacy PKIs will be out of compliance with FIPS 201, so it is necessary to revise the Common Policy. She and Dave Cooper are drafting the Change Proposal and will present it to the CPWG at the 18 September 2007 meeting. Two of the changes involve 1) specifying 18-hour CRLs, to align with FIPS 201, 2) run off-line CAs with 30-day CRLs. Both OMB and NIST will support these changes and will review it before it goes out.

Agenda Item 9

Adjourn Meeting

The meeting adjourned at 11:30 AM. The next FPKIPA meeting is scheduled for 9 October 2007 (9:30 a.m. – 11:30 a.m.) at the USPS Headquarters, 475 L'Enfant Plaza, SW, Room 2P316 (inside 2P310) 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	Nov. 15 2007	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
259	Debbie Mitchell will forward policy statements to the FPKI PA for review when available.	Debbie Mitchell	12 Dec. 2006	9 Jan. 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
313	Dr. Alterman will contact each cross-certified member (who has not upgraded yet) to find out their strategy and whether or not they will be able to meet the October 27, 2007 deadline	Dr. Alterman	11 Sept. 2007	9 Oct. 2007	Open