Federal Public Key Infrastructure Policy Authority (FPKIPA)

Draft Minutes of the 11 December 2007 Meeting

GSA NCR Building, 7th and D Streets, SW, Washington, DC
Conference Room: 5700 (Training Room)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 13 November 2007 FPKIPA Minutes
3. Results of e-vote on the C4CP
4. FPKI Certificate Policy Working Group (CPWG) Report
    a. *Discuss / Vote Common Policy CP Change Proposal: 2007-03*
    b. *Discuss FBCA CP Change Proposal: 2007-0b*
5. FPKI Operational Authority (FPKI OA) Report – Cheryl Jenkins
    a. *Certificate Directory Status*
    b. *Key Rollover Status*
    c. *Interoperability Testing Status*
    d. *Re-Design Status*
6. *Update on* SSPWG Activities
7. Final Meeting Items
8. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 13/15 (or 86.7%), where a two-thirds majority was required. Two members joined the meeting after we met the quorum. This is the first time in many months that all voting members have been represented, either in person, via teleconference or via proxy. A holiday party followed the meeting.

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)	Cooper, David	Teleconference
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	Hagerling, Don	
Department of Justice	Morrison, Scott – and, then, Proxy to HHS	Teleconference
Department of State	McCloy, Mark A.	
Department of the Treasury	Proxy to HHS	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA	Temoshok, David	
NASA	DeYoung, Tice	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	

Organization	Name	Telephone
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Proxy to Commerce (NIST)	

OBSERVERS

Organization	Name	Telephone
FPKI/FICC Support (Contractor-- General Dynamics Information Technology)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Enspier Technologies/Protiviti Government Services)	Fincher, Judy	
SSA (Contractor, Jacob & Sundstrom)	Simonetti, David	Teleconference
IdenTrust	Young, Kenny	
FPKI OA Technical Lead (Contractor— Enspier Technologies/Protiviti Government Services)	Brown, Wendy	
MIT Lincoln Laboratory	Moriaty, Kathleen	Teleconference
FPKI OA/GSA (PM)	Jenkins, Cheryl	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
NRC (Contractor, VeriSign)	Evans, Frazier	
KPMG	Faut, Nathan	
FPKI/FICC/GSA	Spencer, Judith	
Enspier/Protiviti Government Services	King, Matt	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman, Chair

The FPKIPA met at the GSA National Capital Region (NCR) Building, at 7th and D Streets, SW, Washington, DC, Conference Room: 5700. Dr. Peter Alterman, Chair, called the meeting to order at 9:40 a.m. with the attendee roll call. We wish to thank Ms. Cheryl Jenkins of the GSA for hosting this meeting/holiday party.

Agenda Item 2

Discussion / Vote on 13 November 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said that she incorporated all the comments received from Charles Froehlich, Cheryl Jenkins and Brant Petrick and distributed a redline version of the minutes to the FPKIPA five working days prior to the 11 December 2007 FPKIPA meeting. The FPKIPA voted by 66.7% (10/15) to approve the minutes, as amended, where a 50% majority vote was required. Three members abstained, and two were absent for this vote.

Approval vote for 13 November 2007 FPKIPA Minutes			
Voting members	**Vote (Motion –DHS ; 2^{nd} – USPS)**		
	Yes	**No**	**Abstain**
Department of Commerce			√
Department of Defense			√
Department of Health & Human	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury - Proxy to HHS	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	ABSENT FOR THIS VOTE		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT FOR THIS VOTE		
USPS	√		
USPTO (Proxy to Commerce)			√

Agenda Item 3

Results of e-Vote on the C4CP—Judy Fincher
Ms. Fincher said the e-vote passed with an 80% majority vote (12/15) where 66.7% was required. See the results of the e-vote, below.

Results of E-Vote on the C4CP			
Voting members	**e-Vote**		
	Yes	**No**	**Abstain**
Department of Commerce		√	
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT FOR THIS VOTE		
GPO	√		
GSA	√		
NASA			√
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		

Dave Cooper said the C4CA requires an annual audit. Cheryl Jenkins stated that the implementation of the new C4 CP and C4 CPS (and accompanying matrices) will occur at the time the FPKIA re-design is implemented (8 months from now). At the time of the full C&A of the re-designed FPKIA, the C4CP audit will also be updated.

ACTION: Matt King will make sure the posted C4CP matrix matches the posted C4CP.

ACTION: Dave Cooper will schedule a review of the revised C4CP, using an un-redacted version in 2008.

Agenda Item 4

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

1) *Discuss / Vote Common Policy CP Change Proposal: 2007-03 – Judith Spencer, Dave Cooper*

Judith Spencer presented this Change Proposal last month and withdrew it pending the resolution of several issues. This revised Change Proposal, submitted today, and accompanying Memorandum, makes changes to COMMON so that the Federal Legacy PKIs can express Common Policy OIDs in the PIV Auth certificates to meet FIPS 201 requirements.

NOTE: A Legacy PKI refers to any Federal Agency PKI cross-certified with the FBCA, regardless of the level of assurance. It only refers to PKIs owned and operated by a Federal agency.

> By adding language pertaining to naming conventions and off-line root CAs, the main obstacles to compliance with the Common Policy by Federal Legacy PKI agencies have been removed. This should enable the Federal Legacy PKI agencies to express Common Policy OIDs in the PIV Authentication Certificates, as is required to meet the requirements of FIPS 201…. (From “Memorandum for Federal Agency Legacy PKIs”)

Tice DeYoung pointed out a discrepancy between the Change Proposal and the accompanying Memorandum. FIPS 201 requires both HTTP and LDAP, whereas the Change Proposal (section 2.1) refers to the use of “either LDAP or HTTP.” It should say “and” to be compliant with FIPS 201, (Section 5.4.5.1).

The authors of the Change Proposal agreed with this observation and struck section 2.1 from the Change Proposal because the section should be about directories, not certificates.

The FPKIPA voted to approve the Common Policy CP Change Proposal: 2007-03, as revised during the meeting, by a majority vote of 14/15, or 93.4%, as shown below.

Approval vote on Common Policy Change Proposal: 2007-03			
Voting members	**Vote (Motion –NRC ; 2nd – GPO)**		
	Yes	**No**	**Abstain**
Department of Commerce	√		
Department of Defense		√	
Department of Health & Human	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury - Proxy to HHS	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO (Proxy to Commerce)	√		

DoD said they would vote to approve the change with the provision that they could have a longer CRL publishing time (24 hours) and next update time (7days). As a legacy PKI, DoD can still not meet the requirements of the Common Policy CP even as presently modified, Ms. Mitchell said. The FPKIPA Chair interpreted these remarks as a “no” vote, and Ms. Mitchell confirmed the “no” vote.

2) *Discuss FBCA CP Change Proposal: 2007-0b – Judith Spencer*

This Change Proposal addresses the “disconnect” between COMMON and the FBCA CP by imposing requirements for the value that is placed in the nextUpdate field in a CRL. The current FBCA CP is silent on the value of nextUpdate, but imposes a CRL issuance frequency requirement (less than 24 hours). This Change Proposal proposes adding a nextUpdate field to the FBCA CP that is the same as that in Common, e.g., the nextUpdate time in the CRL may be no later than 48 hours after issuance time.

Dr. Peter Alterman asked for feedback on this proposal from all cross-certified members – not just the voting members.

Discussion ensued about the possible disruptive impact of this change on PKI operations. Don Hagerling said this change had the risk of shutting everybody down, e.g., an internal denial of service attack. Debbie Mitchell said that DoD cannot support less than a seven (7) day interval due to the length of time required to push to the whole organization. DoD feels this could be an operational risk, she said unless Microsoft changes the way the nextUpdate field is treated to produce a warning “not to proceed,” we cannot support this Change proposal, she said.

Don Hagerling urged the cross-certified members to learn from DoD's experience in pushing out CRLs and stated that our priority should be the availability of essential service and management of risk.

Judith Spencer said the real limitation is imposed by the Common Access Card's limited container and the fact that DoD has not implemented OCSP worldwide.

DoD strongly disagreed with this statement. Ms. Mitchell said that DoD has over 30 Certificate Status Servers implemented in over six locations worldwide. Today, she said, DoD would not be able to support a CRL issuance frequency of less than 24 hours and a nextUpdate field in the CRL or no later than 48 hours. DoD, she said, would not be able to come into compliance with the proposed policy change.

Dr. Alterman said the issue is the period of the nextUpdate field. This is a contentious issue that should be discussed further in the CPWG and by the FPKIPA cross-certified members, he said

ACTION: Judy Fincher is to send out a memo to all FBCA cross-certified members asking them to respond by a specified time to the following questions: 1) Are you already using a nextUpdate field? 2) What is it? 3) What is a reasonable nextUpdate field value?

ACTION: Judy Fincher is to schedule a Key Recovery Policy drafting session in January 2008. We need to convert the draft KRP to RFC 3647 format. Participants will be Dr. Peter Alterman, Judith Spencer, and Dave Cooper.

Agenda Item No. 5

FPKI Operational Authority (FPKI OA) Report —Cheryl Jenkins, Wendy Brown

1. Certificate Directory Status

   Wendy Brown reported on the directory status and said that a living report was issued on Directory status: "Directory Status and Plan of Action for FBCA Cross-Certified Affiliates." The majority of errors are missing SIA's, she said. Certificate issues will be addressed as new cross certificates are issued after the FBCA Key Rollover.

   ACTION: Judith Fincher will distribute the "Directory Status and Plan of Action for FBCA Cross-Certified Affiliates" to the FPKIPA listserv.

2. Key Rollover Status

   The key rollover of the FBCA to 2048-bit key size is due before December 31, 2007. The FPKI OA is on schedule for this rollover. The new FBCA certificate will be a six-year certificate to match policy (not 10 year). Once the FPKI OA has the new key, we will issue new cross-certificates to all cross-certified members. Please notify your technical staff of these events.

Cheryl Jenkins reported that the E-Gov CA will be rolled over (re-keyed) before the end of January 2008 and will be issued as a 6 year certificate to match policy (not 5-year).

3. Interoperability Testing Status

   The FPKI OA has been preoccupied with the FBCA key rollover and as such did not have time to work with SAFE on interoperability testing.

4. Re-design Status

   The FPKI OA hopes to get the third party reviewers on board for the IV&V by early January 2008. Ms. Jenkins stated that work is underway on the annotated Implementation Plan.

   ACTION: Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA. NOTE: At this juncture, we are not asking for comments; this is for information only.

   David Temoshok asked that the FPKI OA brief the FPKIPA once the re-design plan has been validated (based on the IV&V review)—probably in the February/March timeframe.

   Ms. Jenkins reported that the data center must be relocated by June 2008 to a new government-owned primary site within 99 miles or less of the District of Columbia. She and Judith Spencer are currently looking for a new site. Dr. Alterman urged them to consider the data center at NIH. Ms. Jenkins will make her decision once the Implementation Plan is finalized.

Agenda Item No. 6

Update on SSPWG Activities— Judith Spencer

December 6, 2007 SSP Quarterly Meeting

Ms. Spencer said that she met on December 6 with the SSP vendors to discuss, 1) ways the SSP Program could help with FRAC, TWIC, etc., 2) and to report on the status of the SSP audit methodologies evaluation. Richard Wilsher, an independent third party expert, is in town this week meeting with Entrust and VeriSign, she said, to document their audit methodologies. Tom Lockwood (DHS) addressed the SSP vendors on the PIV-like programs underway in the public sector.

Agenda Item No. 7

Final Meeting Items

a) Dr. Tice DeYoung reported that 85% of the NASA employees had moved to the new CA.
b) The next FPKIPA meeting will be held on January 8, 2008, from 9:30 a.m. – noon at the GSA National Capital Region Building at 7th and D Streets, SW, Washington, DC, in room 5700 (accessed via Room 5060)
c) The updated Executive Summary Sheet was distributed to the FPKIPA listserv prior to the 11 December 2007 FPKIPA meeting.

Agenda Item No. 8

Adjourn Meeting

The meeting adjourned at 10:55 a.m., followed by a potluck holiday party.

CURRENT ACTION ITEMS

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, 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
314	Judy Fincher will contact Phil Welsh, the SAFE Technical POC, to see if any issues had arisen in SAFE's "reverse mode" testing.	Judy Fincher	9 Oct. 2007	19 Oct. 2007	Open
315	Cheryl Jenkins will generate the SAFE Interoperability Test Report once it is determined that all remaining issues have been resolved.	Cheryl Jenkins	9 Oct. 2007	19 Oct. 2007	Open
314	Dr. Alterman and Larry Shomo (DHS Contractor, Cygnacom) will talk offline next week to discuss DHS's plans for their PKI.	Dr. Alterman, Larry Shomo	9 Oct. 2007	19 Oct. 2007	Open
315	Dr. Alterman and John Cornell will incorporate language into the FPKIPA audit Cook Book." This language was provided by Noel Nazario of KPMG and says that if customers set up the terms of their Web Trust audits appropriately, the Web Trust audit would satisfy all our requirements.	Dr. Alterman, John Cornell	9 Oct. 2007	13 Nov. 2007	Open
316	Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.	??	13 Nov. 2007	26 Nov. 2007	Open
320	An ad hoc working group comprised of Dr.Tice DeYoung, Jim Schminky, Judith Spencer, Dr. Peter Alterman, the "right" NIST person, and a representative from the Department of State (Charles Froehlich?) is empowered to review the DoD Issues Paper and make a recommendation to the FPKIPA.	Dr. Alterman, et al.	13 Nov. 2007	3 Dec. 2007	Open
321	Dr. Alterman will develop and distribute a questionnaire for the FPKIPA cross-certified members about the status of their test environments.	Dr. Alterman	13 Nov. 2007	20 Nov. 2007	Open
322	Matt King will make sure the posted C4 CPA matrices match the posted C4CP.	Matt King	11 Dec. 2007	15 Jan. 2008	Open
323	Dave Cooper will schedule a review of the revised C4CP, using an un-redacted version in 2008.	Dave Cooper	11 Dec. 2007	2008	Open

No.	Action Statement	POC	Start Date	Target Date	Status
324	Judy Fincher is to send out a memo to all FBCA cross-certified members asking them to respond by a specified time to the following questions: 1) Are you already using a nextUpdate field? 2) What is it? 3) What is a reasonable nextUpdate field value?	Judy Fincher, FBCA cross-certified members	11 Dec. 2007	21 Dec. 2007	Open
325	Judy Fincher is to schedule a Key Recovery Policy drafting session in January 2008. We need to convert the draft KRP to 3647 format. Participants will be Dr. Peter Alterman, Judith Spencer, and Dave Cooper.	Judy Fincher	11 Dec. 2007	31 Dec. 2007	Open
326	Judith Fincher will distribute the "Directory Status and Plan of Action for FBCA Cross-Certified Affiliates" to the FPKIPA listserv.	Judy Fincher	11 Dec. 2007	12 Dec. 2007	Done
327	Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA.	Cheryl Jenkins	11 Dec. 2007	January 2008	Open