Federal Public Key Infrastructure Policy Authority (FPKIPA)

Draft Minutes of the 12 February 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316 (Inside 2P310)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 8 January 2008 FPKIPA Minutes
3. Results of E-vote on 11 December 2007 FPKIPA Minutes
4. Discuss/Vote on University of Texas Cross-Certification Application
5. FPKI Certificate Policy Working Group (CPWG) Report
    a. *Review CPWG Mapping Recommendation for USPS at Medium Hardware*
    b. *Review CPWG Mapping Recommendation for GPO at Medium Hardware*
    c. *Review SAFE Bridge Interoperability Test Report*
    d. *Review CPWG Recommendation to approve SAFE Mapping at Medium CBP and Medium Hardware CBP*
    e. *Review CPWG Recommendation to Approve USPS Audit Report*
    f. *Discuss/Vote on FBCA CP Change Proposal: 2008-01 (Alignment of Cryptographic Algorithm Requirements with NIST Special Publication 800-57)*
6. *Discuss/Vote on SAFE Bridge Cross-Certification at Medium CBP and Medium Hardware CBP*
7. *Discuss/Vote on cross-certification of GPO at Medium Hardware*
8. *Discuss/Vote on cross-certification of USPS at Medium Hardware*
9. FPKI Operational Authority (FPKI OA) Report
    1. Certificate Directory and Cross-Certification Status
    2. Key Rollover Status
    3. Re-design Status
10. *Update on SSP and* SSPWG Activities
11. Final Meeting Items
    a. Other Topics:
        1. NASA Migration to new CA (Under SSP)
        2. Qualified CP (QCP) Mapping
12. 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. This included three proxies (USPTO, Treasury and NRC). Another member joined the meeting after the quorum was established.

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	
Department of Defense	O'Brien, Shawn	
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	Hagerling, Don	
Department of Justice	Morrison, Scott	
Department of State	Gregory, Steven E.	
Department of Treasury	Proxy to HHS	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Absent	
GSA	Temoshok, David	
NASA	DeYoung, Tice	
Nuclear Regulatory Commission- NRC	Proxy to HHS	
SSA	Elspas, Greg	
USPS	Stepongzi, Mark	
USPTO	Proxy to Commerce	

OBSERVERS

Organization	Name	Telephone
DoD	Hymes, Morris	
FICC/ GSA	Spencer, Judith	
GSA	Jenkins, Cheryl	
E-Auth PMO	Frazier-McElveen, Myisha	Teleconference
USPS (Contractor – USPS CA Operations)	Walter, Mike	Teleconference
CertiPath	Takanti, Vijay	Teleconference
SAFE	Shields-Urling, Molly	Teleconference
SAFE	Cullen, Cindy	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
University of Texas	Goldsmith, Clair	Teleconference
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant	Teleconference
FPKIPA Secretariat (Contractor -- Enspier Technologies/Protiviti Government Services)	Fincher, Judy	Teleconference
FPKIPA (Contractor—Enspier Technologies/Protiviti Government Services)	King, Matt	Teleconference
IdenTrust (vendor)	Young, Kenny	Teleconference
FPKI OA Technical Lead (Contractor—Enspier Technologies/Protiviti Government Services)	Brown, Wendy	
DoD (Attorney)	Russell, Shauna	
eValid8	Dilley, Brian	
Department of the Army	Brown, Cindy	
MIT Lincoln Laboratory IT Security, ICS	Malabon, Mikiala	Teleconference
KPMG	Nazario, Noel	
DoS (Contractor, ManTech)	Froehlich, Charles	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman, Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2P316 (inside 2P310). Dr. Peter Alterman, Chair, called the meeting to order at 9:40 a.m. The voting included three proxies: USPTO to Commerce, Treasury to HHS, and NRC to HHS.

Agenda Item 2

Discussion / Vote on 8 January 2008 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all comments received and distributed a redline version of the minutes to the FPKIPA five working days prior to the 12 February 2008 FPKIPA meeting.

The FPKIPA voted by 10/15, or 66.7%, to approve the minutes, where a 50% majority was required.

Approval vote for 8 January FPKIPA Minutes – red line version			
Voting members	**Vote (Motion- NASA ; 2nd- USPS)**		
	Yes	**No**	**Abstain**
Department of Commerce			√
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	Not Present for this Vote—joined later		
Department of Justice	√		
Department of State	√		
Department of the Treasury (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	Not present for this vote—joined later		
GPO	Absent		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	√		
USPS	√		
USPTO (Proxy to Commerce)			√

Agenda Item 3

Results of E-vote on 11 December 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher conducted the e-vote on the 11 December 2008 FPKIPA Minutes. Once the e-vote quorum was established (12/15, or 80%), the e-vote was 11/12 in favor, or 91.6% where a 50% majority was required.

Results of e-vote on 11 December 2008 FPKIPA Minutes			
Voting members	**Vote (Quorum was 12/15 or 80% where a 2/3 majority was required)**		
	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	Did Not Vote		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	Did Not Vote		
USPS	√		
USPTO	Did Not Vote		

Agenda Item 4

Discuss/Vote on University of Texas Cross-Certification Application—Dr. Peter Alterman

The FPKIPA discussed the merits of allowing an individual university system to cross-certify, as opposed to the Higher Education Bridge (HEBCA) or EDUCAUSE. Dr. Alterman explained that 1) most of higher education is SAML-based, not PKI, 2) consequently, there is no driving force behind HEBCA and there is no funding, 3) there is a pressing business need, e.g., HHS needs to award electronic bio-medical research grants and there are 6 bio-medical research centers in the University of Texas (UTx) system. We are not going to use grants.gov, he said.

UTx is the largest university running PKI. The others are the University of Wisconsin, the University of California, and Dartmouth, Dr. Alterman said.

Dave Cooper suggested the CPWG workload would grow to unmanageable size if organizations were allowed to participate at the C4 Level of Assurance (LOA).

Dr. Alterman said there were only 16 mapping tables in the C4 matrix and that the workload for C4-related mapping would be “trivial.”

Judith Spencer said that the Liberty Alliance Identification Framework is designed to create a larger trust federation that we can plug into and short-circuit our mapping efforts in the future. David Temoshok elaborated on this growing community of interest. C4 will become a path for communities of interest where we don't want to be the sole authority over that group, e.g., like the Common Policy. We want to work with the Liberty Alliance so that an acceptable LOA can be maintained within that community.

Dr. Alterman said that as the institution of a higher education bridge becomes more realistic (through Liberty Alliance), the other universities will most likely emulate.

Judith Spencer said that the FBCA and C4 are increasingly outward looking and want to establish trust relationships with the larger community.

Cheryl Jenkins inquired about the timeframe for completion of the mapping and initiation of the NIH system. Dr. Alterman said that the goal is the end of April 2008 for the mapping and cross-certification. This dovetails with the NIH pre-production pilot that will start up the end of April 2008.

Judith Spencer said that the revised Criteria and Methodology document requires a vote by the FPKIPA on all new applicants for cross-certification, to ensure there is a compelling business interest for the government and to control CPWG resources.

The CPWG then voted 12 to 15 (80%) in favor of the UTx application where a 75% majority vote was required. Two members voted, "No."

Approval vote for University of Texas Cross-Certification Application (at C4)			
Voting members	**Vote (Motion – NASA ; 2nd –State)**		
	Yes	**No**	**Abstain**
Department of Commerce		√	
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	v		
Department of the Treasury (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	Absent		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	√		
USPS	√		
USPTO (Proxy to Commerce)		√	

Agenda Item 5

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

a. Review CPWG Mapping Recommendation for USPS at Medium Hardware
The CPWG successfully mapped the USPS at Medium Hardware. The USPS modified their existing policy since the USPS has not yet issued any digital certificates, and all certificates (certs) will be issued at Medium Hardware.
Note: The revised Criteria and Methodology no longer requires the FPKIPA to approve the CPWG mapping report.

b. Review CPWG Mapping Recommendation for GPO at Medium Hardware
The CPWG successfully mapped the GPO at Medium Hardware. In this case, the GPO added a new policy OID--so there are now two OIDs.

c. Review SAFE Bridge Interoperability Test Report
Wendy Brown said the FPKI OA had distributed this report and that there were no problems with the interoperability testing.

d. Review CPWG Recommendation to approve SAFE Mapping at Medium CBP and Medium Hardware CBP
The SAFE Bridge has been successfully mapped by the CPWG and there are no remaining mapping issues from the due diligence review (Business Operations) or from the technical review (the Operational Parameters review).

e. Review CPWG Recommendation to Approve USPS Audit Report
Both the CPWG and John Cornell (the GSA Attorney for FPKI) reviewed the USPS Audit Report and found it acceptable.

f. Discuss/Vote on FBCA CP Change Proposal: 2008-01 (Alignment of Cryptographic Algorithm Requirements with NIST Special Publication 800-57)

DoD drafted (with assistance from the CPWG and NIST) FBCA CP Change Proposal: 2008-01 that would allow Entity CAs that have certificates with 1024-bit RSA to continue to be cross-certified with the FBCA until 12/31/2010 regardless of when the 1024-bit certificates expire. NIST (Tim Polk) is willing to assert that this does not violate SP 800-57 since Federal relying parties would not make use of the 1024-bit keys after 2010.

Morris Hymes (DoD) joined the FPKIPA to present the Change Proposal and explain the reasons that compelled it.

DoD is fully using PKI and has up to 6.7 million users, he said. Operational complexities compel the DoD to advance more slowly than agencies who have not deployed PKI widely in their environments.

DoD is looking at operations as a significant issue, and we want to improve the strength of the algorithms. We must be cautious in moving to SHA 256 and Elliptical Curve technology, and must test them to ensure interoperability.

There is limited value to having an agency that can only talk to itself. We want to be interoperable with federal and non-federal partners, he said.

Scott Morrison reported that the FBI is still issuing 1024-bit certs and that this policy would benefit them, as well as the DoD.

The FPKIPA then voted by 14/15 or 93.3% of eligible voters, to approve FBCA CP Change Proposal: 2008-01, where a 75% majority vote was required.

Approval vote on FBCA CP Change Proposal: 2008-01 (alignment with 800-57)			
Voting members	**Vote (Motion – NASA ; 2nd – DHS)**		
	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 (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	Absent		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	√		
USPS	√		
USPTO (Proxy to Commerce)	√		

Agenda Item 6

Discuss/Vote on SAFE Bridge Cross-Certification at Medium CBP and Medium Hardware CBP—Dr. Peter Alterman

There was no discussion on this issue and the FPKIPA approved the cross-certification of the SAFE Bridge by 13/15 or 86.9 %, where a 75% majority vote was required.

Vote to Approve SAFE Bridge Cross-Certification at Medium CBP and Medium Hardware CBP			
Voting members	**Vote (Motion – DHS ; 2nd –State)**		
	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 (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	Absent		
GSA	√		
NASA			√
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	√		
USPS	√		
USPTO (Proxy to Commerce)	√		

Agenda Item 7

Discuss/Vote on cross-certification of GPO at Medium Hardware—Dr. Peter Alterman

There was no discussion of this item and the FPKIPA voted by 14/14 or 100% of eligible voters, to approve the cross-certification of GPO at Medium Hardware, where a 75% majority was required.

Approval Vote on the Cross-Certification of GPO at Medium Hardware			
Voting members	**Vote (Motion – DHS ; 2nd – NASA)**		
	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/Recused		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	v		
USPS	√		
USPTO (Proxy to Commerce)	√		

Agenda Item 8

Discuss/Vote on Cross-certification of USPS at Medium Hardware—Dr. Peter Alterman

There was no discussion on this item and the FPKIPA voted to approve cross-certification of USPS at Medium Hardware by 13/14, or 92.9% of eligible voters, where a 75% majority vote was required.

Approval vote for cross-certification of USPS at Medium Hardware			
Voting members	**Vote (Motion – DHS ; 2nd – NASA)**		
	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 (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	Absent		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (Proxy to HHS)	√		
SSA	√		
USPS	Recused		
USPTO (Proxy to Commerce)	√		

Agenda Item 9

FPKI Operational Authority (FPKI OA) Report

1. Certificate Directory and Cross-Certification Status

The FPKI OA distributed the statistical report for December that identifies a number of issues with current certificates. The OA is trying to address all of these issues when we issue the new cross certificates, following the FBCA key rollover. The FPKI OA sent out the requests for new certificates to all cross-certified entities, but have not been receiving the signed certificates back. The FPKI OA will issue new certs once they receive the cross certificate from the partner.

The FPKI OA issued new certificates to DEA CSOS, DoD ECA, DoD Interoperability Root and MIT Lincoln Laboratory. The OA is working with MIT to resolve some interoperability issues, e.g., chaining to their directory.

As a result of today's vote to approve the FBCA CP Change Proposal: 2008-01, the OA will issue new cross certificates to DoD ECA and DoD IRoot. The OA will issue cross certificates that expire on 12/31/2010 to CAs who are issuing end entity certificates with 1024-bit RSA keys that expire after that date.

2. Key Rollover Status

The FBCA rollover occurred on 12/31/07, and new EGCAs were established on February 1, 2008.

3. Re-design Status

The FPKI OA has to vacate the primary FPKIA site by 30 June 2008 and are asking for feedback on where the new site should be located. Cheryl Jenkins and Judith Spencer are planning to tour a facility in the Willow Woods complex, but no decision has been made.

The contract for an IV&V review of the re-design documents was delayed due to changes in the contracting office at GSA, but should be awarded soon. The FPKI OA is making progress on the Implementation Plan and more details should be available by the March FPKIPA meeting. Ms. Jenkins said it is a good plan to get the new architecture up and running. We are moving forward and will do what can be funded this year, she said.

Agenda Item 10

Update on SSP and SSPWG Activities—Judith Spencer

Ms. Spencer is planning to hold another SSPWG meeting soon. She said that the independent study of C&A-like assessments performed by the SSPs is due this week.

She also described activities run by the states that make use of PIV-card like capabilities, such as ACIS, FRAC and TWIC. Since the States cannot use SSPs (which are certified for use by Federal Government agencies only), several SSPs will come in with commercial clones at Medium Hardware for cross-certification with the FBCA. Their policies will be clones of the Common Policy and must be mapped, she said.

Agenda Item 11

Final Meeting Items

a. Other Topics:

1. NASA Migration to new CA (Under SSP)
   Tice DeYoung reported that 92% of NASA PKI users are now on the new SSP-provided system. NASA plans to shut down their legacy CA by 31 March 2008 and will ask that their certs be revoked. NASA intends to provide official notice on 29 February 2008 to comply with the 30-day notification rule.

2. Qualified CP Mapping
   Dave Cooper wanted to know why Enspier/Protiviti Government Services is mapping the European Qualified CP (QCP). Judith Spencer and Dr. Peter Alterman provided some background on previous attempts to perform this mapping. Back in 2002-2003, Judith Spencer performed a mapping of the QCP, which is, in effect, a technical standard, not a policy. At that time the GSA issued a letter to the EU stating, "we were in harmony" with them and that the likelihood was good that the FBCA would cross-certify with any PKI using QCP as its basis for writing their CP.

   About 1 ½ years ago, Dr. Alterman and Ms. Spencer went to Italy to attend the European Signature Initiative (ESI) conference and she presented an expanded mapping to the ESI at that time. The ESI wanted the FBCA CP to be changed to require FIPS 140-Level 3 plus adding verbiage about user rights.

   We agreed we would come closer together if there was a business case. Now with the cross-certification of SAFE and CertiPath, we may have a business case because we now have European PKIs within the Federation.

   Dr. Alterman asked Enspier/Protiviti Government Services to perform a preliminary mapping with the understanding it was a "back burner" type activity and that it would come to the CPWG only when we have a business case.

   In the meantime, the Department of State mapping is the priority.

Agenda Item 12

Adjourn Meeting

Dr. Alterman adjourned the meeting at 11:15 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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

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
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
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