FPKIPA
Federal Public Key Infrastructure Policy Authority

Minutes of the 12 November 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2105

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 14 October 2008 FPKIPA Minutes
3. Identity Management (IdM) Initiative Briefing
4. FPKI Certificate Policy Working Group (CPWG) Report
    a. Discuss /Vote on FBCA CP Change Proposal: 2008-05 (Role-Based Certs)
    b. Discuss / Vote on Common Policy Framework CP Change Proposal: 2008-03 (Role-Based Certs)
    c. Discuss / Vote on FBCA CP Change Proposal: 2008-06 (CA validity period)
    d. Review / Vote on USPS FY08 CA/PKI Compliance Audit Certification Letter
    e. Review CPWG Report on VeriSign Operational Parameters Review
    f. Review / Vote on VeriSign WTCA Audit Letter and CPWG Response
    g. Review CPWG Report on Wells Fargo Operational Parameters Review
    h. Discuss / Vote to cross-certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
    i. Re-vote on making SIA extension optional until 2010
5. FPKI Management Authority (FPKI MA) Report
6. Final Meeting Items
    a. Proposed Agenda Items for the next FPKIPA meeting, 9 December 2008
7. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 12/15 (or 80%) where a two-thirds majority 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.fincher@pgs.protiviti.com.

Organization	Name	Telephone
Department of Commerce (NIST)	Proxy to GSA	

Organization	Name	Telephone
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Hagerling, Don	
Department of Justice	Morrison, Scott	
Department of State	Gregory, Steven	
Department of Treasury	Proxy to GSA	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan John	Teleconference
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission (NRC)	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	ABSENT	

OBSERVERS

Organization	Name	Telephone
FPKI MA PM/GSA	Jenkins, Cheryl	Teleconference
IdenTrust	Schambach, Marco	Teleconference
IdenTrust	Wilson, Ben	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
Wells Fargo	Drucker, Peri	Teleconference
Wells Fargo	Gross, Jim	Teleconference
DoD (Legal)	Russell, Shauna	Teleconference
FPKI MA Technical Lead (Contractor, Protiviti Government Services)	Brown, Wendy	
FPKI MA Subject Matter Expert (Contractor, Protiviti Government Services)	Louden, Chris	
FPKIPA Support, Co-Chair CPWG (Protiviti Government Services, Contractor)	McBride, Terry	
Federal PKI and FICC Support (Contractor, FC Business Systems LLC)	Petrick, Brant	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Ms. Judith Spencer, Interim Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2105. Judith Spencer, Interim Chair, called the meeting to order at 9:35 a.m. and conducted introductions of those present in person and via teleconference.

Agenda Item 2

Discussion / Vote on 14 October 2008 FPKIPA Minutes— Terry McBride

The FPKIPA approved the 14 October 2008 FPKIPA minutes by the unanimous count of votes cast (14/14) or 100%.

Approval vote for 14 October 2008 FPKIPA Minutes – red line version			
	Vote (Motion- DHS, 2^{nd-} GPO)		
	Yes	**No**	**Abstain**
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

Agenda Item 3

Identity Management (IdM) Initiative Briefing —Judith Spencer

Judith Spencer gave a brief history of the IdM e-Government initiatives. She pointed out that E-Authentication did not graduate and was put on the parking lot. E-Authentication is not going away, but it is transitioning. OGP will be taking over Governance, Architecture, and the Lab for E-Authentication. The IdM Task Force report and the CIO IDM Committee, which NASA and Justice co-chair, will provide input and direction.

Judith Spencer gave a brief presentation on a PIV-related proposal affecting legacy PKI agencies. The presentation was distributed after the meeting to all those on the FPKIPA listserv (12/10/08). PIV cards are being deployed, she said. It is estimated that 30% [of Federal employees] have them. Legacies have provisions to use the piv-auth OID, but there are concerns about how that works operationally. Technically, the Common Policy is supposed to be the CA that issues the piv-auth OID--not the Bridge. Judith Spencer proposed moving to cross-certify the legacies with the Common Policy CA (not subordinate) for the purposes of PIV. She noted that the current FPKI MA re-design provides us with an excellent timing opportunity. Ms. Spencer went over the benefits and impacts including a shorter PKI validation path and the requirement to issue new cross-certificates. She stated that this is a proposal. It is not set in stone. There would be no need for legacies to map to the Common Policy. The current FBCA mapping is sufficient for the cross-certification at Medium, Medium Hardware or High. There is no foreseeable expectation that legacies would eventually subordinate to the Common Policy. Also, there is no intention to merge the FBCA and Common Policy.

The memo for Implementing HSPD-12 Using Legacy PKI Certificates is attached at the end of these Minutes.

Agenda Item 4

FPKI Certificate Policy Working Group (CPWG) Report—Charles Froehlich, Terry McBride

a. Discuss /Vote on FBCA CP Change Proposal: 2008-05 (Role-Based Signature Certs)

This change proposal was reviewed. Judy Spencer pointed out that each certificate is issued to an individual, but the name in the certificate is that OF A ROLE (e.g., Secretary of State). The agency and RA can determine which certificate key pair was issued to which individual.

The Change Proposal was approved with 14/15 (93%) voting members approving (75% majority of all voting members needed).

Vote on FBCA CP Change Proposal: 2008-05 (Role-Based Signature Certs)			
	Vote (Motion- DHS, 2^{nd-} DOS)		
	Yes	No	Abstain
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

b. Discuss / Vote on Common Policy Framework CP Change Proposal: 2008-02 (Role-Based Signature Certs)

This Change Proposal is a companion to the FBCA CP Change Proposal: 2008-05 above, It applies to the Common Policy.

The Change Proposal was approved with 14/15 (93%) voting members approving (75% majority of all voting members needed).

Vote on Common Policy Framework CP Change Proposal: 2008-03 (Role-Based Signature Certs)			
	Vote (Motion- DOS, 2nd- DHS)		
	Yes	**No**	**Abstain**
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

c. Discuss / Vote on FBCA CP Change Proposal: 2008-06 (CA validity period)

This Change Proposal was reviewed. It was approved with 14/15 (93%) voting members approving (75% majority of all voting members needed).

Vote on FBCA CP Change Proposal: 2008-06 (CA validity period)			
	Vote (Motion- DHS, 2nd- NRC)		
	Yes	**No**	**Abstain**
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

d. Review / Vote on USPS FY08 CA/PKI Compliance Audit Certification Letter

The CPWG recommendation was discussed. Hearing no objection from any member of the FPKI PA, the audit letter was accepted. There was no need to vote.

e. Review CPWG Report on VeriSign Operational Parameters Review

The CPWG co-chairs indicated that there were a couple of outstanding minor questions for VeriSign. Therefore, the CPWG is not prepared to report on the Operational Parameters Review at this time.

f. Review / Vote on VeriSign WTCA Audit Letter and CPWG Response

Discussion regarding Web Trust for Certification Authorities (WTCA) audit ensued. GSA counsel believes that cross-certifying entities need to go beyond the requirements of WTCA and include the FBCA cookbook requirements when contracting with auditors. Peri Drucker stated that timing is important when considering this issue. She stated that in the case of Wells Fargo the “Cook Book” came out two days before the audit began, so the contract was already issued. Judith Spencer pointed out that VeriSign started their audit before the last cook book change and before this WTCA battle began. Judith Spencer stated that we had always accepted WTCA audits in the past. She pointed out that John Cornell believes this does not mean we should accept them now. Peri Drucker asked what the FPKI PA is going to do with all of the entities that contracted for WTCA audits before the cookbook was issued.

Ben Wilson of IdenTrust said the WTCA is addressing the FPKI PA’s concerns.

Judith Spencer pointed out that VeriSign does this for a living. Moreover, the same facilities have undergone a C&A and have met FISMA requirements for the SSP program. David Sulser indicated that NRC had its own independent review done and can provide work notes and an audit letter to support. The FPKI PA decided to postpone a vote on the audit letter until more information can be provided to the voting members--at which time an e-vote will be called.

g. Review CPWG Report on Wells Fargo Operational Parameters Review

The CPWG report was given. The CPWG found no major issues with the Wells Fargo Operational Parameters Review. However, DoD’s Debbie Mitchell and Shauna Russell raised some concerns.

Ms. Russell pointed out that Wells Fargo does not provide any warranty for transactions not involved with Wells Fargo certificates. Peri Drucker asked why Wells Fargo would warranty somebody else’s certificate? Shauna Russell also pointed out that Wells Fargo assumes no liability--even in gross negligence. Judith Spencer indicated that John Cornell (GSA Counsel) had heard Ms. Russell’s concerns via e-mail and does not agree. He believes that the limitations in liability are not an issue.

Ms. Russell then pointed out that the Wells Fargo CP calls for entities to indemnify Wells Fargo. Judith Spencer pointed out that that issue has been discussed between Wells Fargo and John Cornell and is being dealt with in the MOA. Ms. Russell said that that is not how she would do business. She would make Wells Fargo change the CP.

Finally, Ms. Russell pointed out that Wells Fargo is asking for one-way trust. Wells Fargo will not trust the FBCA. Peri Drucker indicated that that was always understood from the time the application was accepted. Ms. Russell stated that goes against the principles of the Bridge, that it is a sham, and that she was offended.

Discussion ensued regarding the points above until Don Hagerling (DHS) moved that the PA move to the next agenda item so that a vote could proceed on cross-certifying Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP (item h below). He said that a point had been reached where no new information was being heard.

h. Discuss / Vote to cross-certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP

The discussion from above and Don Hagerling's motion (see item g above) moved the PA to this agenda item. Acceptance of Wells Fargo for cross-certification was approved with 13/14 (92%) votes cast (75% majority of all votes cast needed).

Vote to cross-certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP			
	Vote (Motion- NRC, 2nd- DHS)		
	Yes	**No**	**Abstain**
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense		√	
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

i. Re-vote on making SIA extension optional until 2010

The vote on making SIA extension optional until 2010 passed with 14/15 (93%) voting members approving.

Re-vote on making SIA extension optional until 2010			
	Vote (Motion- DHS, 2nd- NRC)		
	Yes	**No**	**Abstain**
Department of Commerce PROXY to GSA/J. Spencer	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury PROXY to GSA/J. Spencer	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

Agenda Item 5

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins, Wendy Brown, Chris Louden

Chris Louden presented the near-term strategy for stabilizing the MA repositories and touched briefly on mid and long-term strategies. Mr. Louden showed a graph of the types of traffic and the increase in traffic. Traffic has increased over 50% since June. The MA will be enabling load balancing in the near-term to deal with increased traffic. In addition, the MA will consider adding different directories behind the load balancer. The mid and long terms call for more repositories geographically dispersed and multiple hot sites.

The presentation was distributed after the meeting to all those on the listserv (12/10/08).

Agenda Item 6

Final Meeting Items

1) Proposed Agenda Items for the next FPKIPA meeting, 9 December 2008
    a. None discussed

Agenda Item 7

Adjourn Meeting

Ms. Spencer adjourned the meeting at 11:47 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
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
329	Cheryl Jenkins and Dr. Peter Alterman will reach out to Wells Fargo to determine what should be in the Directory and what the next steps are.	Cheryl Jenkins, Dr. Peter Alterman	11 March 2008	21 March 2008	Open
331	Dr. Alterman will draft language for the FBCA policy change procedure to do some “reality testing” and distribute it to the FPKIPA.	Dr. Peter Alterman	8 April 2008	13 May 2008	Open
366	Debbie Mitchell will share the finalized DoD Test Plan; the FPKIPA will then review it and decide what pieces they can and cannot do. Then Cheryl Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Cheryl Jenkins	13 May 2008	10 June 2008	Open
371	Dr. Alterman will inform Verizon Business Systems (VBS) that their application was approved and will ask for the ETA for the Policy.	Dr. Peter Alterman	8 July 2008	15 July 2008	Open
372	The CPWG will talk with VeriSign and Verizon Business to see how they would delimit boundaries and guarantee that certs will only go to government.	CPWG	9 Sept. 2008	14 Oct. 2008	Open
373	Deborah Gallagher will check with DHS to verify the FRAC requirement.	Deborah Gallagher	9 Sept. 2008	14 Oct. 2008	Open

No.	Action Statement	POC	Start Date	Target Date	Status
374	PGS (Terry McBride) will draft the LOA for Ms. Spencer's signature to issue a cert to DoS at Basic, Medium, Medium Hardware and High.	Terry McBride	14 October 2008	12 Nov. 2008	Open
375	The FPKIPA Chair will take the enduring proxy and meeting schedule issues under advisement and will notify non-attendees that they risk losing their voting privileges if they persist in unexplained absences and do not designate a proxy when they cannot attend.	Judith Spencer	14 October 2008	12 November 2008	Open

FPKIPA

Federal Public Key Infastructure Policy Authority

MEMORANDUM FOR FEDERAL AGENCY LEGACY PKIs

SUBJECT: Implementing HSPD-12 using Legacy PKI certificates

[DATE: 10/7/07]

Section 5.4.4 of FIPS 201 states: “Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)”
In order to facilitate Federal Legacy PKI compliance with this requirement, the Common Policy has been modified to include provisions that exclusively pertain to the Federal Legacy PKIs. 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 (additional certificates for signing and key management can continue to only assert agency OIDs). However, those agencies planning to take advantage of this new language must ensure that they implement their certificates in a manner consistent with other provisions in the Common Policy. A Federal Legacy PKI will be deemed to be issuing PIV Authentication certificates in conformance with the Common Policy if it issues those certificates in accordance with the requirements of a certificate policy that has been mapped to the FBCA CP at the Medium Hardware or High assurance level and in accordance with the following additional provisions that affect certificate issuance:

- Identity proofing requirements (FIPS 201 Section 2)

- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.

- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)

- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP)* Program [SSP-PROF] (FIPS 201 Section 5.4.2.1).

- Requirement not to post PIV Authentication certificates to a public directory. (FIPS 201 Section 5.4.5.1)

- Requirement to make directory information available via LDAP and HTTP. (FIPS 201 Section 5.4.5.1

Peter Alterman, Ph.D.
Chair