



Minutes of the 6 April 2010 Meeting
USPS, 475 L'Enfant Plaza, SW, Washington, DC.
CR 2P316 (inside CR 2P310)
9:40 a.m. – 11:50 a.m.

A. AGENDA

- 1. Welcome / Introductions**
- 2. Discuss/Vote on 9 March 2010 FPKIPA Minutes**
- 3. Documenting the Use of PKI at DoS**
- 4. Discuss/Vote on Triennial Compliance Audit Requirements**
- 5. FPKI Certificate Policy Working Group (CPWG) Report**
 - *NIST SP 800-53 Rev 3 Review by CPWG*
 - *Change of E-Auth Level of FBCA*
 - *Dartmouth Request*
 - *PIV-I Change Proposal*
- 6. FPKI Management Authority (FPKI MA) Report**
 - *Architecture Re-Design Update*
 - *The Target Architecture*
 - *Feds Only Meeting*
 - *FPKIA Usage Statistics*
 - *Annual Compliance Audit*
 - *FPKI TAG Recommendations Paper: Path Development and Validation (PD-Val)*
- 7. Other Agenda Items**
 - *ICAM Report*
 - *SAFE-BioPharma Pilot*
- 8. Adjourn Meeting**

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 14/15 (or 93.3%) 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 were 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 Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Miller, Tanyette	Teleconference
Department of Justice	Morrison, Scott	
Department of State	Gregory, Steve	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Absent	
Nuclear Regulatory Commission (NRC)	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Lindsey, Dan	Teleconference
Veterans Administration (VA)	Jurasas, Eric	Teleconference

OBSERVERS

Organization	Name	Telephone
Treasury PKI PMO	Bracy, Gayle	Teleconference
FPKI MA/PM	Jenkins, Cheryl	
State of Illinois	Anderson, Mark	Teleconference
Entrust (vendor)	Moore, Gary	
IdenTrust (Vendor)	Schambach, Marco	Teleconference
FPKI MA and FPKIPA Support (Contractor, PGS)	King, Matt	
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoS (Contractor, ManTech)	Froehlich, Charles	
FPKIPA Secretariat (Contractor, PGS)	Fincher, Judy	
FPKIPA (Contractor, PGS)	McBride, Terry	Teleconference
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
DOE (Contractor, M Squared Strategies, Inc.)	Olson, Evan	
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
EPA (Contractor, Jacob & Sundstrom)	Simonetti, David	Teleconference
SSA (Contractor, Jacob & Sundstrom)	Jackmon, Kenya	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Chair

The FPKIPA met at the USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC, CR 2P316 (inside CR 2P310). Judith Spencer, Chair, called the meeting to order at 9:40 a.m., and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of USPS for hosting this meeting.

Agenda Item 2

Discuss/Vote on 9 March 2010 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she received comments on the 9 March 2010 FPKIPA minutes too late to verify the ICAM section with Ms. Spencer. Once that is done, Ms. Spencer could call for an e-vote or the FPKIPA could vote on them at the 11 May 2010 meeting. Consequently, the FPKIPA did not vote.

Agenda Item 3

Documenting the Use of PKI at the DoS —Steve Gregory

Steve Gregory gave a presentation on PKI usage at the DoS. His report was compiled from directory logs, using a tool the DoS developed for that purpose. He reported that the use of PKI for the week ending 3/02/2010 averaged 12,855 requests per day, with a total of 89,986 during the week. Additionally, the Department's PKI supported 22,500 instances of information sharing with external partners during the same time period.

This information was gathered by tracking daily requests for validation of a PKI certificate used on the OpenNet or validation of a PKI used to transmit data to external entities.

This reflected PKI usage on OpenNet and included the number of OpenNet PKI Certificate Revocation List Requests (Web CRL Requests per day and the number of LDAP CRL requests per day). Similarly, the tool collected data on Certificate Revocation Lists Requests by external PKI users. He noted that the DoS OCSP Responder is in C&A now and will be deployed in several months.

He offered to provide the script (code) to other Federal agencies and Treasury accepted. The DoS desktop client is under development and is probably eighteen months away, he said.

Judy Spencer said that policy requiring PKI usage data is coming soon.

Agenda Item 4

Discuss/Vote on Triennial Compliance Audit Requirements—Judith Spencer, Jim Schminky

Triennial Audit Requirements

Jim Schminky (Treasury), chair of the Audit Working Group that developed the proposed Triennial Compliance Audit methodology, led the discussion of the two Triennial Audit Change Proposals (FBCA CP Change Proposal: 2010-02 and FCPFCA Change Proposal: 2010-04) needed to implement the recommendations of the Audit Requirements document.

Judith Spencer said that there is a growing momentum for continuous monitoring of IT systems, including the Federal Public Key Infrastructure. She reported that Ron Ross of NIST at the CNSS conference in late March addressed the relationship between FISMA

requirements for continuous monitoring, as found in NIST SP 800-37 (C&A) and NIST SP 800-53 Rev 3 (IT security controls), and NIST Draft SP 800-128 (configuration management). She expressed a hope that the proposed Triennial Compliance Audit methodology would complement FISMA and urged the FPKIPA to adopt it.

Steve Gregory said that budget cycle considerations drove the Department of State view of the Triennial audit. We already submitted our budget request for next year. He said that DoS could not accept the proposed new methodology unless the Implementation Date changes to “two years” and would vote “No” on the proposed changes.

Mr. Schminky agreed. It depends on where you are in your budget cycle, since the budgeting process is out two years, he said.

The FPKIPA agreed with the change in Implementation Date. The FBCA CP Change Proposal now reads:

“This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Bridge CA Certificate Policy. Currently cross-certified entities have two years from the date of approval to effect this change.”

Another change in both Change Proposals is the removal of “delta” audits and management assertion language (sections 8.1 and 8.4).

The FPKIPA then voted on each Change Proposal, in turn. Each Change Proposal passed with the unanimous vote of members present, or 14/15 (or 93.3%) of voting members. NASA was absent for this meeting.

Approval Vote for Common Policy CP Change Proposal Number: 2010-04			
Voting members	Vote (Motion –NRC ; 2nd – DoS)		
	Yes	No	Abstain
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)	×		
GPO	×		
GSA	×		
NASA	Absent		
Nuclear Regulatory Commission (NRC)	×		
SSA	×		
USPS	×		
USPTO	×		
Veterans Administration	×		

Approval Vote for FBCA Certificate Policy Change Proposal Number: 2010-02			
Voting members	Vote (Motion – Treasury ; 2nd – USPS)		
	Yes	No	Abstain
Department of Defense	×		
Department of Health & Human	×		
Department of Homeland Security	×		
Department of Justice	×		
Department of State	×		
Department of the Treasury	×		
Drug Enforcement Administration (DEA CSOS)	×		
GPO	×		
GSA	×		
NASA	Absent		
Nuclear Regulatory Commission	×		
SSA	×		
USPS	×		
USPTO	×		
Veterans Administration	×		

Alignment with the C&A Process

Cheryl Jenkins said that the C&A should marry with the CA audit. She mentioned the research conducted by the CPWG in 2006 that found that a “significant subset: of SP 800-53 maps back to the FBCA CP:

“The FPKI Policy Authority, in consultation with NIST, has reviewed the security requirements imposed by the FBCA CP and compared them to the security controls defined in SP 800-53. Based on this review, the FPKIPA has determined that a successful compliance audit by a cross-certified PKI or an SSP CA verifies that a significant subset of the SP 800-53 security controls are in place....” [Memo to Agency Chief Information Officers and Senior Agency Information Security Officers, Aug. 31, 2007]

She said the FPKI MA had compiled a table that she uses to define the audit parameters. We look at each control from two perspectives, she said. Ms. Jenkins offered to share the mapping table with the FPKIPA.

Mr. Schminky said with this new Triennial Audit approach we are falling into a continuous monitoring pattern where everything gets looked at in a three year cycle. He reminded the FPKIPA members that Federal agencies would not be required to adopt the new Triennial methodology, nor would the external cross-certified entities. They could still opt to do a full annual audit.

This new approach is a shift away from a one-time look at everything to a model of continuous monitoring. (For background on the proposed new audit methodology, refer to the 12 January 2010 FPKIPA Minutes, published on the FPKIPA web site, and the draft 9 March 2010 Minutes which were sent to the FPKIPA listserv).

The FPKIPA also discussed making compliance audit letters public, e.g., posted on the web, for the Relying Parties to read. The FPKIPA agreed to send this to the CPWG for discussion and a recommendation.

Ron Ross of NIST will be invited to participate in the 11 May 2010 FPKIPA meeting to address the continuous monitoring issue and potential alignment of the Triennial Audit process with the C&A process.

Agenda Item 5

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

1. NIST SP 800-53 Rev 3 Review by CPWG—Charles Froehlich

The CPWG led by Mickey Tevelow (PGS) is in the process of updating the mapping of NIST SP 800-53 to the FBCA CP, now that rev 3 has been approved. He has identified a number of new requirements, that the CPWG is examining. We expect to report on that initiative at the 8 June 2010 FPKIPA.

2. Change of FBCA FIPS Category—Terry McBride

Mr. McBride said the FPKI MA is transitioning from a FIPS 199 risk category of “Moderate” to one of “High.” This will affect the NIST 800-53 mapping, since that document has different security controls for the two different categories.

3. Dartmouth Request—Judith Spencer

Scott Rea of Dartmouth, Chair of the Higher Education Bridge CA, has developed a policy mapping tool and wishes to populate it with CPs from the FPKI community. Mr. Rea has asked that the FPKI cross-certified members publish their CPs. Several already do: The State of Illinois, USPS, and Treasury. Ms. Spencer asked that cross-certified members give their URL’s to Brant Petrick.

4. PIV-I Change Proposal—Terry McBride, Judith Spencer

Terry McBride said that the PIV-Interoperable Tiger Team (PIVITT) had developed a change proposal and corresponding marked up 3647 format FBCA CP for the issuance by Non-Federal Issuers of smart cards that would interoperate with Federal LACs and PACs systems. PIVITT is comprised of ICAM member agencies and contractors, and is chaired by Chris Loudon of PGS. Mr. Loudon turned over the PIV-I Change Proposal to the CPWG, who is in the process of reviewing the marked up document.

Ms. Spencer said she rejected the creation of three new Levels of Assurance. PIV-I applies to all Medium and Medium HW policies, she said. Mr. McBride said the edits made by the CPWG were on 1) Identity proofing, 2) affiliated organization, 3) card management system, 4) changes to the cert profile and OSCP Responder, 5) Definition of PIV-I Card, 6) CMS appendix.

Debbie Mitchell asked that the minutes of the 1 April 2010 CPWG be published by COB Friday, so the DoD would have a chance to review them before the DoD PKI Conference in Minneapolis next week. At that time, Ms. Spencer and other FPKI cross-certified members will meet with the DoD PKI PMO to discuss the PIVITT document. Ms. Mitchell also requested that the minutes reflect the rationale for the edits made by the CPWG. The CPWG will resume the edit of the PIVITT document at their April 20, 2010 meeting.

Ms. Spencer said she would send out the revised PIVITT document and a copy of the joint memo being prepared by Russ Housley, Chair of the IETF and Chair of the CertiPath PMA, and Chris Loudon for NIST (Tim Polk) on the issue of content signing. (See the 1 April 2010 CPWG Minutes for more detail on this controversial topic.)

The FPKIPA was not prepared to sign off on the current version of the PIVITT document until there had been more discussion. It will go back to the CPWG for action.

Agenda Item 6

FPKI Management Authority (FPKI MA) Report-Cheryl Jenkins

1) Architecture Re-Design Update

Ms. Jenkins said that the OMB gave the FPKI MA seven key activities to complete by 9/30/2010, which could be capsulated in three big buckets: Deploy new architecture across six sites, accredit the new architecture in accordance with FISMA, and move the current architecture to better facilities. We are on schedule or ahead of schedule for these activities. In fact, we moved the current architecture one month ahead of schedule to better facilities and as such, have achieved a 43% improvement in providing repository response time. However, as traffic continues to grow, the FPKI MA will have to roll-out new solutions to maintain this improved response time. For instance, in the month of March, the repository had 80 million hits. The FPKI MA will deploy a global load balancing solution between the production sites to help manage the traffic load.

2) The Target Architecture

The deployment of the new FPKIA will not affect any Federal PKI customers. The FPKI MA has decided to develop and distribute for comment a transition plan to include a schedule for when each customer will move to the new architecture beginning on 9/30/2010.

3) Feds only Meeting

Included in the transition plan, will be the final plans to move legacy federal customers from the FBCA to the COMMON. There will be a "Feds" only meeting to discuss this topic prior to distributing the plan.

4) PKI Usage Statistics

Ms Jenkins said the FPKI MA registered 80 M repository searches in March 2010 and are tracking both Directory and HTTP usage. Judith Fincher distributed the FPKI MA “dashboard” just after the FPKIPA meeting.

5) Annual Compliance Audit

Ms. Jenkins said the FPKI MA retrospective compliance audit would start in June 2010, and that the Day Zero Compliance Audit Letter and C&A Letter would be issued by 9/30/2010.

6) FPKI TAG Recommendations Paper: Path Development and Validation (PD-Val)

Ms. Jenkins said the FPKI MA Technical Advisory Group (TAG) published a recommendations paper: “Managing and Resolving Certification Path Development and Validation Issues in the FPKI.” The paper identified several concerns in the existing infrastructure dealing with:

“The quality of contents asserted in certificates that are used in this environment. Specifically, incorrect and inconsistent certificate content present certification path development and validation issues for relying parties that need to rely on these certificates. Furthermore, agencies are discovering that certification path development and validation during signature verification and authentication is time-consuming, which presents operational burden to the end users.” [TAG, February 2010]

The TAG recommended that the FPKI MA provide the PA with processes for the agencies to address these problems and maintain a trusted infrastructure with the FPKI Architecture. [This paper was distributed to the FPKIPA listserv just prior to the meeting, and there was insufficient time for the members to review and further discussion was postponed.]

Ms. Jenkins said that a PD-Val Working Group will be re-convened to develop guidance and processes that will track issues and provide a wide-spread of communication regarding this topic. However, she also said that due to the requirements involved with establishing the new architecture by 9/30/2010, it could be several months after 9/30/2010 before this occurred.

Agenda Item 7

Other Agenda Items—Judith Spencer

1- ICAM Report

Ms. Spencer said guidance will be provided soon for everyone to implement ICAM. We can do Trusted Internet Connection by using an agency interface or by standing up your own. But, we will need relief because of Blue Coat.

2- SAFE-BioPharma Pilot

Ms. Spencer reported on a “collaboration mode” pilot being conducted at SAFE-BioPharma between clinicians and the National Cancer Institute (NCI). SAFE has developed a new tool for workflow management to track digital signature authentication (instead of relying on a paper routing slip).

Agenda Item 8

Adjourn Meeting

USPS made a motion to adjourn and Treasury seconded it. Ms. Spencer adjourned the meeting at 11:50 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
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
378	Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.	Cheryl Jenkins	9 June 2009	14 July 2009	Open
379	Cheryl Jenkins will provide a milestone and timeline sheet for the redesign effort. This will be provided as a dashboard on a monthly basis to the FPKIPA.	Cheryl Jenkins	9 June 2009	14 July 2009 and monthly afterwards	Open
381	Judith Spencer will check with NIST for additional guidance on device certificates.	Judith Spencer	9 June 2009	18 June 2009	Open

FPKIPA Minutes 6 April 2010

No.	Action Statement	POC	Start Date	Target Date	Status
382	Judith Spencer will talk with Bill Macgregor at NIST about guidance for Key Management history.	Judith Spencer	9 June 2009	18 June 2009	Closed
382	Judy Spencer will send the Discussion Paper: "SSL Inspection and Mutual TLS Issue" to ICAMSC with today's date as an information paper, not a recommendation from the FPKIPA.	Judith Spencer	10 Nov. 2009	16 Nov. 2009	Open
383	The Secretariat will add a reference to the Discussion Paper: "SSL Inspection and Mutual TLS Issue," in the FY2010 Accomplishments paper.	Judith Spencer	10 Nov. 2009	Oct. 2010	Open
384	Wendy Brown is to draft an email memo for the ICAMSC re the Mozilla root store request and send to Brant Petrick for distribution to the ICAMSC.	Wendy Brown	10 Nov. 2009	16 Nov. 2009	Open
385	We need to write a Change Proposal, adding a <i>cardAuth</i> policy to FBCA. FBCA will require a UUID, as opposed to being optional.	Judith Spencer	10 Nov. 2009	30 Nov. 2009	Closed
386	Jim Schminky will provide the MA with a report of availability from a customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.	Jim Schminky	10 Nov. 2009	30 Nov. 2009	Open
388	Cheryl Jenkins will reach out to Marianne Swanson (and Ron Ross) of NIST to determine what their audit standards strategy is vis-à-vis aligning the FBCA and NIST SP 800-53 with ISO standards.	Cheryl Jenkins	9 March 2010	13 April 2010	Open