



FEDERAL PKI POLICY AUTHORITY

MEETING MINUTES

**14 December 2010
USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC**

9:35 a.m. – 10:55 a.m.

Welcome, Opening Remarks & Introductions	Judy Spencer Chair
Installation of new FPKIPA Chair	Judy Spencer/ Deb Gallagher
Discuss / Vote on 9 November 2010 FPKIPA Minutes	Matt King
SHA-256 Transition Update	Matt King
FPKI Certificate Policy Working Group (CPWG) Report	Charles Froehlich
1. Discuss: Common Policy CP Change Proposal - OIDs in OCSP Responder Certificates	
2. Discuss/Vote: Common & FBCA Policy CP Change Proposals – Key Rollover Clarification	
3. Mapping Reports – DigiCert, Entrust PIV-I, Verizon	

- Business PIV-I**
4. **Discuss/Vote Recommendation to Approve VeriSign at PIV-I**
 5. **Discuss/Vote Recommendation to Approve CertiPath at PIV-I**
 6. **Discuss/Vote Recommendation to Approve Verizon Business at PIV-I**
 7. **Notice of Change Proposals in January 2011**
 8. **Report from FPKI Security Profile WG – Profiles Status**

FPKI Management Authority (FPKI MA) Report

Cheryl Jenkins

Other Agenda Items

Deb Gallagher

- *ICAM Update—Deb Gallagher*
- *If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.*

Adjourn Meeting

Deb Gallagher

A. ATTENDANCE LIST

Voting Members:

Organization	Name	Present?
Department of Defense	Mitchell, Debbie	T
Department of Energy	Breland, MaryAnn	P
Department of Health & Human Services	Slusher, Toby	P
Department of Homeland Security	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice	Morrison, Scott	P
Department of State	Frahm, Jarrod M.	P
Department of Treasury	Gallagher, Deb (Proxy)	P
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	T
GPO	Hannan, John	P

Organization	Name	Present?
GSA	Spencer, Judith / Gallagher, Deb	P
NASA	Levine, Susan	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
SSA		A
USPS	Stepongzi, Mark	P
USPTO		A
Veterans Administration (VA)	Jurasas, Eric	T

T – Telephone

P – In Person

A – Absent

Observers:

Organization	Name	Present?
Cipher Solutions (vendor)	Ahuja, Vijay	T
Illinois	Anderson, Mark	T
DEA	Briggs, Sharrod	T
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
CertiPath	Howard, Steve	P
Ernst & Young	Iijima, Timothy	T
GSA, FPKI MA PM	Jenkins, Cheryl	P
FPKIPA (Protiviti)	King, Matt	P
FPKIPA (Protiviti)	Louden, Chris	P
Entrust	Moore, Gary	P
SSA (Contractor)	Myers, Matt	T
DoE	Olson, Evan	P
GSA (Contractor, Unisys)	Petrick, Brant	P
CertiPath	Nigriny, Jeff	P
VeriSign	Piazzola, Nick	T
SAFE BioPharma	Cullen, Cindy	T
FPKIPA (Protiviti)	Sonya, Tiffany	P

T – Telephone

P – In Person

A – Absent

B. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks, Introductions

Judy Spencer, Chair

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza SW, Conf. Rm. 4841, Washington, DC. Judith Spencer, Chair, called the meeting to order at 9:35 A.M EST and introduced those present, both in person and via teleconference. All voting representatives attended the start of the meeting with the exception of USPTO and SSA.

Agenda Item 2

Installation of new FPKIPA Chair

Judy Spencer

Ms. Spencer reminded everyone that the FPKIPA agreed that GSA would be the chair, so no action is needed to transfer the Chair to Ms. Deb Gallagher. The charter will need to be revised if the FPKIPA wants GSA to remain as the permanent Chair (without requiring future voting).

Agenda Item 3

Discuss / Vote on 9 November 2010 FPKIPA Minutes

Matt King

Mr. King informed the FPKIPA that all changes have been made to the circulated November 9, 2010 FPKIPA minutes. DOE motioned to approve the minutes and the motion was seconded by USPS.

Approval Vote for 9 November 2010 FPKIPA Minutes			
Voting members	Vote (Motion DOE ; 2 nd USPS)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA - ABSENT			
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Agenda Item 4

SHA-256 Transition Update Matt King

The SHA-256 transition is in progress. The FPKI MA has implemented some of the components of the planned solution. Working sessions will continue in January 2011 to maintain communication within the community. Use of the SHA-256 Working Group mail list (ICAM-SHA256@LISTSERV.GSA.GOV) is encouraged to exchange information and lessons learned.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich

Discuss: Common Policy CP Change Proposal - OIDs in OCSP Responder Certificates

The Common Policy CP Change Proposal, *OIDs in OCSP Responder Certificates*, was discussed. An overview of the background of this change proposal was provided and it was explained that DoD initiated this change because FCPF CP does not explicitly require that certificates issued to OCSP responders assert all the policy OIDs for which the responder provides responses. Since a responder acts as a surrogate to a Certification Authority (CA), the responder should be issued a certificate that includes all the policies that the CA can assert for which the Responder is authoritative. No further discussion was held, and it was agreed that a vote on this change proposal would be held in January 2011.

Discuss/Vote: Common & FBCA Policy CP Change Proposals – Key Rollover Clarification

The Common & FBCA Policy CP Change Proposals, *Key Rollover Clarification*, were discussed briefly and a vote was called. Both change proposals were approved by a 14/16 majority (87.5%).

Approval Vote for Common Policy CP Change Proposal – Key Rollover Clarification			
Voting members	Vote (Motion HHS ; 2 nd State)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		

Department of the Treasury (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA-ABSENT			
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Approval Vote for FBCA CP Change Proposal – Key Rollover Clarification			
Voting members	Vote (Motion HHS ; 2nd State)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA-ABSENT			
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Mapping Reports – DigiCert, Entrust PIV-I, Verizon Business PIV-I

It was reported that DigiCert passed the mapping process but still needs to provide additional information, and that the CPWG will work with them to move forward. DigiCert still needs to do interoperability testing as well as PIV-I card testing.

Entrust and Verizon Business have completed the PIV-I mapping process, but still need to do PIV-I card interoperability testing.

Discuss/Vote Recommendation to Approve VeriSign at PIV-I

VeriSign completed all steps to add PIV-I. The CPWG recommended that they be approved for PIV-I. Discussion was held as to whether additional testing is required if different Card Management Systems are used. It was agreed that the CPWG would discuss this issue.

ACTION: CPWG to discuss what changes require retesting of a PIV-I Issuer (e.g., Is retesting required if new CMS is used or other major changes are implemented?).

An issue was raised about the number of contactless card failures observed during testing (i.e. high failure rates of the contactless interface using the card authentication key). It was suggested that this issue be raised at the ICAM level and with card vendors.

The change proposal was approved by a 14/16 majority (87.5%).

Approval Vote for the Approval of VeriSign at PIV-I			
Voting members	Vote (Motion NRC ; 2 nd USPS)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		

SSA-ABSENT			
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Discuss/Vote Recommendation to Approve CertiPath at PIV-I

CertiPath completed all steps to add PIV-I. The CPWG recommended that CertiPath be approved for PIV-I. It was noted that this is an approval for a bridge, and that test cards will be tested the first time a new issuer comes to CertiPath (the FPKI Lab will be invited to observe). The PIV-I Test Plan will be published this week on IDManagement.gov. It was noted that the test plan is a living document that will be improved over time.

The change proposal was approved by a 14/16 majority (87.5%).

Approval Vote for the Approval of CertiPath at PIV-I			
Voting members	Vote (Motion NRC ; 2nd USPS)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA-ABSENT			
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Discuss/Vote Recommendation to Approve Verizon Business at PIV-I

Verizon Business has completed all mapping steps, but PIV-I card interoperability testing is still in progress. It was agreed that an email vote will be held upon successful completion of testing.

ACTION: Once Verizon Business PIV-I testing is complete, an email vote will be held to approve Verizon Business at PIV-I.

Audit Reports

It was reported that the FPKI MA Day Zero Audit Report was completed and all suggested changes to the CPS were implemented. It was noted that the audit of the existing FPKI MA infrastructure was still in progress; therefore no report of compliance could be made.

It was also reported that GPO has successfully completed their annual audit.

Notice of Change Proposals in January 2011

It was noted that new change proposals would be presented to the FPKIPA in January 2011 as a result of the CertiPath reverse mapping. The changes will relate to the following:

- a. Clarification on how CA requirements apply to other PKI Components (e.g., RAs);
- b. Data Protection; and
- c. Trusted Role Background Check Refresh.

It was noted that CertiPath is hoping for resolution of these change proposals in time for their February 10, 2011 meeting. It was also noted that USIS, the main provider of commercial background checks, is exiting the market. USIS is the only background check provider and it's unclear who else will offer this service. Therefore, CertiPath may need assistance in identifying other commercial vendors who perform background checks.

Report from FPKI Security Profile WG – Profiles Status

It was reported that FPKI Security Profile content has been finalized. NIST provided comments and suggestions for a revision of the document format so as to align with the FedRamp program's Cloud Profile. Since the FPKI profile will also be moved over to the FedRamp program, these format changes will be beneficial. Work is still needed to get the FPKI Profile into the FedRamp program and to obtain OMB approval to enforce the use of the FPKI Profile.

Agenda Item 6

FPKI Management Authority (FPKI MA) Report

Cheryl Jenkins

Ms. Cheryl Jenkins reported on FPKI MA accomplishments. The new trust infrastructure is up and running and the ATO Letter is expected to be finalized on December 14, 2010. All E-Gov customers have been transitioned in preparation for SHA-256 and the old EGCA's will be decommissioned by December 31, 2010. Ms. Jenkins noted that 18 certificates have been issued in support of the SHA-256 transition and up to 12 more would be issued by the

end of the year. Directory performance has drastically improved over the last 3-4 months. Responses are now returned in less than ½ second. A briefing on these improvements will be presented in the near future.

Agenda Item 7

Other Agenda Items

ICAM Update—Deb Gallagher

Ms. Gallagher noted that the ICAMSC is working on the second phase of the FICAM Roadmap Guidance and that she would send this to anyone who requests it. Ms. Gallagher offered congratulations to Ms. Jenkins and the FPKI MA team on setting up the new FPKI SHA-2 CAs and the SHA-1 Federal Root CA infrastructure. She also offered congratulations to VeriSign and CertiPath for being approved at PIV-I and their contributions to interoperability testing of PIV-I cards.

At the end of the meeting, Ms. Gallagher and all the FPKIPA members thanked Ms. Spencer for her leadership and contributions to the Federal PKI community (aka Identity Federation) over the last decade, and presented her with a letter of appreciation.

There was some discussion of moving the January 11 FPKIPA meeting to January 18 to be closer to Ms. Spencer’s retirement party on January 19 – more details will follow.

Agenda Item 8

Adjourn Meeting

Ms Gallagher asked for a motion to adjourn (HHS/USPS) the meeting at 10:55 AM EST.

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

No.	Action Statement	POC	Start Date	Target Date	Status
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-Jun-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.		14-Oct-2008	12-Nov-2008	Open
378	Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.	Cheryl Jenkins	9-Jun-2009	14-Jul-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-Jun-2009	14 July 2009 and monthly afterwards	Ongoing
381	Judith Spencer will check with NIST for additional guidance on device certificates.		9-Jun-2009	18-Jun-2009	Open
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.		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		10 Nov. 2009	Oct. 2010	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	paper.				
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.		10 Nov. 2009	30 Nov. 2009	Obsolete by PIV-I
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	Obsolete
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-Mar-2010	13-Apr-2010	Open
393	Patricia Kless will discuss USPTO's desire to Move to Common with Dan Lindsey and respond to the FPKIPA	Dan Lindsey	10-Aug-2010	14-Sep-2010	Closed – by default they stayed with FBCA since they did not request a move
394	DOE will indicate their desire about whether to cross certify with the FBCA or Common	Mary Ann Breland	10-Aug-2010	14-Sep-2010	Open
396	Ms. Spencer agreed to send additional clarification about requirements surrounding SHA-256 that appear in NIST SP 800-78, 800-131, and other related Special Publications		10-Aug-2010	14-Sep-2010	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
398	Wendy Brown will send an email notifying interested parties that she will accept and respond to requests for test CA certificates with either SHA-1 or SHA-256 for testing	Wendy Brown	10-Aug-2010	14-Sep-2010	Ongoing
401	Cheryl Jenkins will draft SOP for the PA regarding how to enforce corrections for problems in the FPKI repositories and then forward a draft to CPWG	Cheryl Jenkins	14-Sep-2010	12-Oct-2010	Open
403	CPWG will draft a memo about Trusted Internet Connection (TIC) and PKIs	CPWG	14-Sep-2010	12-Oct-2010	Open
404	Matt King will write a SHA-256 FAQ and distribute it on or about 1 December	Matt King	9 November 2010	1 December 2010	Closed
406	Cheryl Jenkins will provide guidance on how to transition to the new SHA-256 FPKI	Cheryl Jenkins	9 November 2010	1 December 2010	Closed
407	CPWG to discuss what changes require retesting of a PIV-I Issuer (e.g., Is retesting required if new CMS is used or other major changes are implemented?).	Matt King	14 December 2010	18 January 2011	Open
408	Once Verizon Business PIV-I testing is complete, an email vote will be held to	Matt King	14 December 2010	18 January 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	approve Verizon Business at PIV-I				