



FEDERAL PKI POLICY AUTHORITY

MEETING MINUTES

GSA

**One Constitution Square
1275 First Street, NE,
Conference Room 801
Washington, DC
20 January 2011
9:45 a.m. – 11:47 a.m.**

Agenda

Welcome, Opening Remarks & Introductions

**Deb Gallagher,
Chair**

- 1. Performance and Capacity Planning Briefing
(Giuseppe Cimmino)**

Discuss / Vote on 14 December 2010 FPKIPA Minutes

Matt King

**FPKI Certificate Policy Working Group (CPWG)
Report**

Charles Froehlich

- 1. Discuss/Vote: FBCA CP Change Proposal - PIV-I
Key Management Key Generation**
- 2. Discuss/Vote: Common Policy CP Change
Proposal - OIDs in OCSP Responder Certificates**
- 3. Discuss/Vote: FBCA CP Change Proposal –
Clarification on how CA requirements apply to
other PKI Components (CSS, etc.)**
- 4. Discuss/Vote: FBCA CP Change Proposal –
Protection of Subscriber Attribute Information**
- 5. Discuss/Vote: FBCA CP Change Proposal –
Background Investigation Refresh**

- 6. FPKI SHA-256 FAQ – Status
- 7. FPKI Security Controls Profile of NIST SP 800-53
- Status

FPKI Management Authority (FPKIMA) 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.*
- *Next FPKIPA meeting, 8 February 2011*

Adjourn Meeting

Deb Gallagher

A. ATTENDANCE LIST

Voting Members:

Organization	Name	Present?
Department of Defense	Mitchell, Debbie	T
Department of Energy	Breland, MaryAnn	T
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	Schminky, Jim	P
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	T
GPO	Hannan, John	P
GSA	Gallagher, Deb	P
NASA	Levine, Susan	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
SSA	Mitchell, Eric	T
USPS	Stepongzi, Mark	T
USPTO	Jain, Amit	T
Veterans Administration (VA)	Miller, Jason	P

T – Telephone

P – In Person

A – Absent

Observers:

Organization	Name	Present?
Cipher Solutions (vendor)	Ahuja, Vijay	T
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
NASA	Baldrige, Tim	P
DigiCert	Wilson, Ben	T
GSA, FPKIMA PM	Jenkins, Cheryl	P
FPKIPA (Protiviti)	King, Matt	P
Entrust	Moore, Gary	P
DoE	Olson, Evan	T
GSA (Contractor, Unisys)	Petrick, Brant	P
DHS (Contractor)	Broadnax, Jennifer	P
EPA (Contractor)	Jackmon, Kenya	T
FPKIPA (Protiviti)	Sonnier, Tiffany	P
FPKIPA (Protiviti)	Pinegar, Tim	T
FPKIMA (Protiviti)	Cimmino, Guiseppe	P
	Huza, Chris	T

T – Telephone

P – In Person

A – Absent

B. MEETING ACTIVITY

Agenda Item 1

Welcome, Opening Remarks & Introductions

Deb Gallagher, Chair

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the GSA NOMA building located at One Constitution Square 1275 First Street, NE, Washington, DC. The meeting was called to order at 9:45 A.M EST and those present, both in person and via teleconference introduced themselves.

It was decided that a briefing from the Federal Public Key Infrastructure Management Authority (FPKIMA) on Performance and Capacity Planning (originally scheduled as part of the FPKIMA Report) would be presented first. Mr. Giuseppe Cimmino presented a very informative overview of the drastic improvements to the Federal Trust Infrastructure over the last six months. Mr. Cimmino described the performance trends and how the FPKIMA has planned for significant increases in capacity in the coming months and years. Discussion was held about what type of performance reporting from the FPKIMA might be needed in the future. The FPKIMA welcomes feedback from the community about performance-related plans or issues. It was agreed that the FPKIMA need only report exceptions in terms of repository performance in the future, but should continue to provide information on usage statistics.

Mr. Tim Baldrige asked if it would be useful if agencies provided the FPKIMA with a heads-up if they knew there would be a surge in certificate issuance or usage by the agency. It was agreed that this type of warning would be useful in helping the FPKIMA stay ahead of the required usage.

Agenda Item 2

Discuss / Vote on 14 December 2010 FPKIPA Minutes

Matt King

Mr. King informed the FPKIPA that all changes have been made to the December 14, 2010 FPKIPA minutes. Treasury motioned to approve the minutes, and the motion was seconded by HHS. The minutes were approved by a 16/16 (100%) vote.

Approval Vote for 14 December 2010 FPKIPA Minutes

Voting members	Vote (Motion Treasury ; 2 nd HHS)		
		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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

Agenda Item 3

FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich

1. Discuss/Vote: FBCA CP Change Proposal – PIV-I Key Management Key Generation

Mr. Charles Froehlich explained that the *PIV-I Key Management Key Generation Change Proposal* was introduced by the CPWG at the last moment to help address issues related to PIV-I Testing. This change proposal clarifies the intent and corrects the inaccuracies in the FBCA CP that were causing a delay in testing for some partners who were in the midst of testing or about to be tested. Discussion about the change proposal was held and it was agreed that an E-Vote would be held for this change proposal and the due date would be 27 January 2011. The E-Vote resulted in unanimous approval of the change proposal.

2. Discuss/Vote: Common Policy CP Change Proposal - OIDs in OCSP Responder Certificates

Mr. Charles Froehlich provided an overview of the OIDs in *OCSP Responder Certificates Change Proposal*. There was a question concerning whether or not Mr. Dave Cooper had provided feedback on the change proposal. It was confirmed that Mr. Cooper had no objections to the content. Treasury motioned to approve the change proposal and the motioned was seconded by HHS. The change proposal was approved by a 16/16 (100%) vote.

Approval Vote for Common Policy CP Change Proposal – OIDs in OSCP Responder Certificates			
Voting members	Vote (Motion Treasury; 2 nd HHS)		
	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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

3. Discuss/Vote: FBCA CP Change Proposal – Clarification on how CA requirements apply to other PKI Components (CSS, etc.)

Mr. Charles Froehlich explained that CPWG discussion of this change proposal uncovered more issues that require additional discussion in future CPWG meetings. It was decided that the CPWG needed to look at the broader impacts of this policy change. Therefore a vote on this change proposal will be deferred to a future FPKIPA meeting.

4. Discuss/Vote: FBCA CP Change Proposal – Protection of Subscriber Attribute Information

Mr. Charles Froehlich provided an overview of the *Protection of Subscriber Attribute Information Change Proposal*. Mr. Froehlich explained that this change proposal was created as a result of concerns identified by CertiPath. Treasury motioned to accept the CP, and it was seconded by NRC. The change proposal was approved by a 16/16 (100%) vote.

Approval Vote for FBCA CP Change Proposal –Protection of Subscriber Attribute Information			
Voting members	Vote (Motion Treasury; 2nd NRC)		
	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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

5. Discuss/Vote: FBCA CP Change Proposal – Background Investigation Refresh

Mr. Charles Froehlich provided an overview of the *Background Investigation Refresh Change Proposal*. Mr. Froehlich explained that this change proposal was created as a result of concerns identified by CertiPath. Treasury motioned to accept the CP and it was seconded by VA. The change proposal was approved by a 16/16 (100%) vote.

Approval Vote for FBCA CP Change Proposal – Background Investigation Refresh			
Voting members	Vote (Motion Treasury ; 2nd VA)		
	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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

6. FPKI SHA-256 FAQ – Status

The FPKI SHA-256 FAQ is complete and was posted to the FPKIPA website after final edits were applied.

7. FPKI Security Controls Profile of NIST SP 800-53 - Status

The FPKI Security Controls Profile of NIST SP 800-53 is undergoing format changes and should be ready for publication within the FPKI Community in the coming weeks. Ms. Deb Gallagher will be coordinating with OMB to establish a mechanism for enforcing compliance with the profile.

There was a request to ask Ron Ross if NIST SP 800-53 could mention the FPKI Security Profile since the Profile will be published as a separate document.

ACTION: Matt King will add an agenda item to a future CPWG meeting related to processes for enforcing compliance with change proposals approved by the FPKIPA.

Agenda Item 4
FPKI Management Authority (FPKIMA) Report
Cheryl Jenkins

In support of the SHA-2 Transition Project, thirty certificates were issued in December 2010, and seven additional certificates need to be issued.

As part of the SHA-2 Transition Plan and in accordance with FPKI policies, all SHA-1 certificates had to be issued by December 31, 2011. The FPKIMA was directed by the FPKIPA to issue SHA-1 cross-certificates from the legacy Common CA to the SHA-1 Federal Root CA (FRCA) and to the new Common CA and decommission the legacy Common CA. The FPKIMA encountered a technical problem that required a patch from the vendor to complete the assignment. However, the resolution was completed after December 31, 2011, which required the FPKIPA to approve the issuance of SHA-1 certificates after the due date. In addition to the technical problem encountered, entities requested the SHA-1 certificates from the legacy Common CA remain available for continued interoperability. It was agreed that the FPKIPA would vote to allow the FPKIMA to “issue cross-certificates from the Legacy Common CA to the New Common CA and SHA-1 FRCA and decommission the Legacy Common CA (including destruction of private keys) without revoking these certificates (that will expire by December 31, 2013). A long term CRL will also be issued, when the Legacy Common Policy CA is decommissioned.”

Treasury motioned to approve FPKIMA’s request and the motion was seconded by VA. The request was approved by a 15/16 (94%) vote.

Approval Vote for Issuance of Cross Certificate to New Common and SHA-1 FRCA from Old Common and the Decommission of Old Common without Revocation			
Voting members	Vote (Motion Treasury ; 2nd VA)		
	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	√		
Drug Enforcement Administration (DEA CSOS)	√		

GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA (ABSENT for this vote)			
USPS	√		
USPTO	√		
Veterans Administration	√		

The accreditation letter granting the FPKIMA Authorization To Operate (ATO) the new Trust Infrastructure was verbally approved in December 2010, and it is expected that the signed letter will be provided imminently.

Agenda Item 5

Other Agenda Items

ICAM Update—Deb Gallagher

Ms. Gallagher explained that the issue of Federal issuers of PIV-I Cards will be raised to the ICAM Architecture Working Group (AWG) and the Federal Interoperability Working Group (FIWG).

ACTION: Mr. Toby Slusher agreed to send the HHS briefing on *Federal Issuers of PIV-I Cards* to the FPKIPA List.

The next FPKIPA meeting will be February 8, 2011 at USPS.

Agenda Item 6

Adjourn Meeting

The meeting was adjourned at 11:47 PM 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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 paper.		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.		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 approve Verizon Business at PIV-I	Matt King	14 December 2010	18 January 2011	Open
409	Matt King will add an agenda item to a future CPWG meeting related to processes for enforcing compliance with change proposals approved by the FPKIPA.	Matt King	20 January 2011	28 February 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
410	Mr. Toby Slusher agreed to send the HHS briefing on the Federal Issuers of PIV-I Cards to the FPKIPA List	Matt King	20 January 2011	28 February 2011	Open