



Minutes of the November 9, 2010 Meeting

USPS Headquarters

475 L'Enfant Plaza, SW, Conf Room 4841, Washington DC 20001

09:35 am – 12:25 p.m.

A. AGENDA

1. Welcome / Introductions
2. Discuss / Vote on 12 October FPKIPA Minutes
3. SHA-256 Transition
 - SHA-256 Transition Plan Update
 - Discuss/Vote: FBCA & Common CP Change Proposals Legacy Use of SHA-1
 - SHA-256 Working Sessions-Status
4. FPKI Certificate Policy Working Group (CPWG) Report
 - Discuss: Common Policy CP Change Proposal OIDs in OCSP Responder Certificates
 - Discuss/Vote: Common & FBCA Policy CP Change Proposals - Key Rollover Clarification
 - Mapping Reports - DigiCert, Entrust PIV-I, Verizon Business PIV-I
 - Report From FPKI Security Profile WG - Status
5. FPKI Management Authority (FPKI MA) Report
6. Other Agenda Items
 - *ICAM Update*
 - *Next FPKIPA meeting, 14 December 2010*
7. Adjourn Meeting

B. ATTENDANCE LIST

Voting Members:

Organization	Name	Telephone
Department of Defense	Mitchell, Debbie	Teleconference
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	Schminky, Jim	P
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	P
GSA	Spencer, Judith	P
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission (NRC)	Sulser, David	P
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	P
USPTO		Absent
Veterans Administration (VA)	Jurasas, Eric	Teleconference

Observers:

Organization	Name	Telephone
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
Illinois	Anderson, Mark	Teleconference
DEA	Briggs, Sharrod	Teleconference
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
FPKIPA (Protiviti)	Cimmino, Giuseppe	P
NIST	Cooper, Dave	P
FPKIPA (Protiviti)	Cruz, Lamontria	P

Organization	Name	Telephone
DoD (Contractor, Booz Allen)	Franks, Larry	Teleconference
DoS (Contractor, ManTech)	Froehlich, Charles	P
DHS	Garcia, Gladys	Teleconference
Entrust	Henick, Nick	Teleconference
CertiPath	Howard, Steve	Teleconference
Ernst & Young	Iijima, Timothy	Teleconference
GSA, FPKI MA PM	Jenkins, Cheryl	Teleconference
DoS (Contractor)	Jung, Jimmy	Teleconference
FPKIPA (Protiviti)	King, Matt	P
MSO (Contractor, Noblis)	Lins, Andrew	Teleconference
FPKIPA (Protiviti)	Louden, Chris	P
	Miller, Jason	Teleconference
Entrust	Moore, Gary	P
SSA (Contractor)	Myers, Matt	Teleconference
DoD (Contractor, Booz Allen)	Nielsen, Rebecca	Teleconference
DoE	Olson, Evan	P
GSA (Contractor, Unisys)	Petrick, Brant	P
EPA (Contractor)	Simonetti, Dave	Teleconference
DigiCert	Wilson, Ben	Teleconference
GSA, OGP	Gallagher, Deb	P
DHS (Contractor)	Shomo, Larry	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions

Judith Spencer

The 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. 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

NASA. NASA joined the meeting by phone after the vote for the approval of the FPKIPA October meeting minutes.

Agenda Item 2
Discuss / Vote on 12 October 2010 FPKIPA Minutes
Matt King

Mr. King informed the Policy Authority that all changes have been made to the circulated October 12, 2010 FPKIPA minutes. The minutes were approved by a 14/14 (100.0%) vote, where a 50% majority vote was required.

Approval Vote for 12 October 2010 FPKIPA Minutes			
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 – ABSENT			
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Agenda Item 3
SHA-256 Transition
Judith Spencer

a. SHA-256 Transition Plan Update:

Ms. Judy Spencer provided an overview of the SHA-256 Transition Plan. This plan was developed at the 25 October FPKI SHA-256 Workshop. The details of the plan were then captured in a memo that was distributed to the FPKIPA and stakeholders and sent to OMB. Key components of the plan involve:

- a) Continuing to operate the current FPKI Federal Bridge Certificate Authority (FBCA) and Common Policy CAs through March 31, 2011 in order to ease the transition to SHA-256
- b) Establishing a parallel SHA-1 infrastructure (SHA-1 Federal Root CA (FRCA)) within the FPKI to be operational during the transition period that will issue SHA-1 cross-certificates under differentiated Object Identifiers (OID) and
- c) Altering the FPKI Certificate Policies to allow the use of SHA-1 to sign revocation information for certificates issued before 12/31/2010, to define the SHA-1 differentiated OIDs, and to allow SHA-1 for signing revocation information for SHA-1 certificates until 12/31/2013

Change proposals were also drafted and circulated to the FPKIPA for a vote at today's meeting. Approval of the change proposals will allow implementation of the Transition Plan and provide three years for the FPKI Community to fully transition from SHA-1 to SHA-256. If the change proposals are not approved, there is no relief from the NIST requirement to transition to SHA-256 by 1/1/2011.

b. Discuss/Vote: FBCA & Common CP Change Proposals Legacy Use of SHA-1

The FBCA & Common CP Change Proposals Legacy Use of SHA-1 were discussed.

Agencies/organizations must decide whether they need the parallel SHA-1 path and inform the FPKIPA. Issuance of SHA-1 certificates after 12/31/2010 must be done from a SHA-1 CA that does not issue SHA-2 certificates and has not issued PIV certificates.

It was recommended that organizations trust SHA-1 Medium Hardware certificates as they would trust SHA-2 Medium Hardware certificates unless a SHA-1 collision is found in the wild. If a collision is found in the wild, the FPKI SHA-1 FRCA will be shut down and cross-certificates revoked.

It was noted that there is no relief from NIST SP 800-78 or FIPS 201 regarding the transition to SHA-256, so SHA-2 credentials must be on PIV cards to remain compliant. It is possible to put a SHA-1 certificate on a PIV card as an optional certificate.

While issuance of SHA-1 certificates after 12/31/2010 will result in non-compliance with FIPS 201 and NIST SP 800-78, OMB has been informed that products are still lagging in their support for SHA-256, so transition time is needed. If an agency does not transition to SHA-256 by 1/1/2011, it is likely that OMB will require reporting on the issues, status, and progress toward the full transition to SHA-256.

Concerns were raised about the ability to setup a new SHA-1 CA in time for the transition.

It was noted that SSPs are required to remain in compliance with HSPD-12 (FIPS 201, NIST SP 800-78) even if their customers are not. The change allowing legacy use of SHA-1 in the Common Policy is in place because the SSPs need to be in compliance with the Common Policy. With this approach, they will need to modify their CPS. It was noted that complying with the Common Policy doesn't "fix" the SSP problem of complying with FIPS 201 and NIST SP 800-78.

A smart card with a id-fpki-SHA1-cardAuth certificate issued after 12/31/2010 is not a compliant HSPD-12 card, even if it contains all the other PIV compliant contents.

OMB asked the FPKIPA to write a SHA-256 FAQ.

ACTION: Matt King will write a SHA-256 FAQ and distribute it on or about 1 December for discussion by the CPWG.

The SHA-1 Federal Root CA will issue certificates signed with SHA-1 to FBCA Affiliates or SSPs who request certificates signed with SHA-1.

There are 4 scenarios for FBCA cross-certified CAs currently issuing SHA-1 certificates:

- If a CA currently issues SHA-1 certificates and continues to do so after 12/31/2010, the certificates will be recognized as being signed by a deprecated OID (and cross-certified with the SHA1 FRCA)
- If a CA issues certificates signed with SHA-1 before 1/1/2011 and SHA-256 after 12/31/2010, a new SHA-1 CA will need to be setup if the organization wishes to continue issuing SHA-1 certificates (and cross-certify their new SHA-1 CA with the SHA-1 FRCA).
- A CA can simply stop issuing SHA-1 certificates after 12/31/2010 and retain their current policy mappings. However, the current cross-certificate with the FBCA will be revoked when the FBCA shuts down by 3/31/2011. Therefore, if their users require a pure SHA-1 environment, they will need to cross-certify with the SHA-1 FRCA.
- A CA can simply stop issuing SHA-1 certificates after 12/31/2010 and retain their current policy mappings and receive a new cross-certificate from the new SHA-2 FBCA.

There are 2 scenarios for SSP CAs currently issuing SHA-1 certificates:

- If a CA issues certificates signed with SHA-1 before 1/1/2011 and SHA-256 after 12/31/2010 it will receive a new cross-certificate from the new SHA-2 Common Policy CA. A new SHA-1 CA (with a cross-certificate from the SHA-1 FRCA) will need to be setup if the SSP needs to continue issuing SHA-1 certificates for some or all of their customers.
- A CA can simply stop issuing SHA-1 certificates after 12/31/2010 and remain a compliant SSP CA. However, it will need a new cross-certificate either from the new SHA-2 Common Policy CA or the SHA-1 FRCA, depending on whether their users require a pure SHA1 environment.

Changes to the Common Policy CA Change Proposal circulated prior to the meeting were made as follows to clarify that CAs cannot issue SHA-1 and SHA-2 end-entity certificates out of the same CA after 12/31/2010:

Common Change Proposal:

Section 6.1.5:

RSA signatures on ~~CA~~certificates that are issued after December 31, 2010 and before January 1, 2014, to CAs that issued certificates prior to December 31, 2010 may be generated using SHA-1 provided that CA issues no additional end entity certificates. ~~However, these CAs shall only issue additional subscriber certificates using SHA-1 if those certificates assert id-fpki SHA1 policies.~~

A vote was called for both the change proposals and the results are below:

The Common CP Change Proposal Legacy Use of SHA-1 was approved by a 12/16 (75.0% vote, where a 75% majority of voting members (12/16) was required.

Approval Vote for the Common CP Change Proposal Legacy Use of SHA-1			
Voting members	Vote (Motion HHS ; 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	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)		√	
SSA	√		
USPS	√		
USPTO – ABSENT			
Veterans Administration	√		

Changes to the FBCA CP Change Proposal circulated prior to the meeting were made as follows to clarify that CAs cannot issue SHA-1 and SHA-2 end-entity certificates out of the same CA after 12/31/2010:

FBCA Change Proposal:

Section 1.0:

CAs that issue SHA-1 end entity certificates after December 31, 2010 may not also issue SHA-256 certificates

Section 6.1.5:

For Medium assurance, signatures on certificates and CRLs asserting certificate policy OIDs that identify the use of SHA-1 ~~shall~~ may be generated using SHA-1 until December 31, 2013. CAs that issue end entity certificates generated using, at a minimum, SHA 224 after December 31, 2010 must not issue end entity certificates signed with SHA 1.

~~RSA signatures on cross-certificates that are issued before January 1, 2014 to CAs that issued certificates prior to December 31, 2010 may be generated using SHA 1. However, these CAs shall only issue additional end-entity certificates using SHA 1 if certificates issued after December 31, 2010 assert certificate policy OIDs that identify the use of SHA-1. Additionally, Certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013.~~

The FBCA CP Change Proposal Legacy Use of SHA-1 was approved by a 13/16 (81.3% vote, where a 75% majority of voting members (12/16) was required.

Approval Vote for the FBCA CP Change Proposal Legacy Use of SHA-1			
Voting members	Vote (Motion HHS ; 2 nd DOE)		
	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 – ABSENT			
Veterans Administration	√		

ACTION: Dave Cooper will provide the SHA-1 OIDs for inclusion in the approved SHA-1 Change Proposals

ACTION: Cheryl Jenkins will provide guidance on how to transition to the new SHA-256 FPKI

c. SHA-256 Working Sessions-Status:

This agenda item was not discussed due to the lengthy SHA-1 Change Proposal discussion.

**Agenda Item 4
FPKI Certificate Policy Working Group (CPWG) Report**

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

The Common Policy CP Change Proposal OIDs in OCSP Responder Certificates was not discussed due to the lengthy SHA-1 Change Proposal discussion. It was agreed that this change proposal would be discussed at the December FPKIPA meeting.

b. Discuss / Vote: Common & FBCA Policy CP Change Proposals- Key Rollover Clarification

The Common & FBCA CP Change Proposals for Key Rollover Clarification were not discussed due to the lengthy SHA-1 Change Proposal discussion. It was agreed that these change proposals would be discussed at the December FPKIPA meeting.

c. Mapping Reports - DigiCert, Entrust PIV-I, Verizon Business PIV-I

The Mapping Reports for DigiCert, Entrust PIV-I and Verizon Business PIV-I were not discussed due to the lengthy SHA-1 Change Proposal discussion. It was agreed that these items would be discussed at the December FPKIPA meeting.

d. Report From FPKI Security Profile WG - Status

The FPKI Security Profile WG Report was not discussed due to the lengthy SHA-1 Change Proposal discussion. It was agreed that these change proposals would be discussed at the December FPKIPA meeting.

**Agenda Item 5
FPKI Management Authority (FPKI MA) Report**

This agenda item was not discussed due to the lengthy SHA-1 Change Proposal discussion.

Agenda Item 6
Other Agenda Items

a. ICAM Update

This agenda item was not discussed due to the lengthy SHA-1 Change Proposal discussion.

b. Next FPKIPA meeting- 14 December 2010

Agenda Item 7
Adjourn Meeting
Judith Spencer

Ms. Spencer adjourned the meeting at 12:25 PM.

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.	Judith Spencer	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.	Judith Spencer	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.	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	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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-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	Open
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	Judith Spencer	10-Aug-2010	14-Sep-2010	Open
398	Wendy Brown will send an email notifying interested parties that she will accept and respond to requests for test CA certs with either SHA-1 or SHA-256 for testing	Wendy Brown	10-Aug-2010	14-Sep-2010	Open
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- Nov-2010	1- Dec-2010	Open

No.	Action Statement	POC	Start Date	Target Date	Status
405	Dave Cooper will provide the SHA-1 OIDs for inclusion in the approved SHA-1 Change Proposals	Dave Cooper	9- Nov- 2010	19- Nov- 2010	Closed
406	Cheryl Jenkins will provide guidance on how to transition to the new SHA-256 FPKI	Cheryl Jenkins	9- Nov- 2010	1- Dec- 2010	Open