



**Minutes of the 13 July 2010 Meeting
USPS Headquarters
475 L'Enfant Plaza, SW, Conference Room 4841
Washington, DC
9:35 a.m. – 11:49 a.m.**

A. AGENDA

1. Welcome / Introductions
2. Welcome to Deborah (Deb) Gallagher, GSA/OGP
3. Discuss / Vote on 8 June 2010 FPKIPA Minutes
4. PKI Operation Risk Realized and Mitigation Going Forward
5. Discuss / Vote on CertiPath PIV-I Application
6. Discuss / Vote on DigiCert Cross Certification Application
7. Discuss / Vote on HEBCA Cross Certification Application
8. FPKI Certificate Policy Working Group (CPWG) Report
 1. Report from SHA 256 WG
 2. Report from FPKI Security Profile WG
9. FPKI Management Authority (FPKI MA) Report
10. Other Agenda Items
 - *ICAM Update—Judith Spencer*
 - *If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.*
 - *Proposed Agenda Items for next FPKIPA meeting, 10 August 2010*
11. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 14/15 (or 93.35%) where a two-thirds majority was required¹.

¹ Contact information was redacted in the published FPKIPA minutes at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members 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 Matthew.King@pgs.protiviti.com

Organization	Name	Telephone
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Garcia, Gladys	Teleconference
Department of Justice	Morrison, Scott	
Department of State	Frahm, Jarrod M.	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Morris, Justin	Teleconference
Nuclear Regulatory Commission (NRC)	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Lindsey, Dan	ABSENT
Veterans Administration (VA)	Jurasas, Eric	Teleconference

OBSERVERS

Organization	Name	Telephone
Entrust	Hernick, Nicholas	Teleconference
Entrust	Moore, Gary	Teleconference
DoE	Breland, Mary Ann	Teleconference
FPKI MA and FPKIPA Support and Acting Secretariat (Contractor, Protiviti)	King, Matt	
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoS (Contractor, ManTech)	Froehlich, Charles	
FPKIPA (Contractor, Protiviti)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	
CertiPath	Nigriny, Jeff	
State of Illinois	Anderson, Mark	Teleconference
DigiCert	Wilson, Ben	
HEBCA	Rea, Scott	
DigiCert	Rowley, Jeremy	Teleconference
Ernst & Young	Iijima, Timothy?	Teleconference
DoE	Olson, Evan	
CertiPath	Smith, Sergio	
DigiCert	Lavigne, Thierry	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions – Judith Spencer, Chair

The FPKIPA met at the USPS Headquarters, 475 L'Enfant Plaza, SW, Conference Room 4841, Washington D.C. Judith Spencer, Chair, called the meeting to order at 9:35 A.M. and introduced those present in person and via teleconference.

Agenda Item 2

**Welcome to Deborah (Deb) Gallagher, GSA/OGP
Judy Spencer**

Deborah Gallagher could not attend, but Judith Spencer pointed out we had welcomed her at a previous meeting. Ms. Spencer said this would not be a recurring item on the agenda.

Agenda Item 3

**Discuss / Vote on 8 June 2010 FPKIPA Minutes
Matt King**

Mr. King said that all changes had been made to the circulated June 8, 2010 FPKIPA minutes, and asked for a vote to approve the minutes. The minutes were approved by 13/13 (100%) where a 50% majority vote was required.

Approval Vote for 8 June 2010 FPKIPA Minutes			
Voting members	Vote (Motion – Treasury; 2nd – USPS)		
	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	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		
Veterans Administration			√

Agenda Item 4

**PKI Operation Risk Realized and Mitigation Going Forward
Jeff Nigriny, CertiPath**

Mr. Nigriny presented a briefing on the risk to current operational PKIs, and described a recent attack on a PKI environment that resulted in a CA compromise. In addition, Mr. Nigriny suggested improvements to the audit process, which may help mitigate these threats. Ms. Spencer suggested that the information in the briefing be considered as input into the Security Profile Working Group.

Agenda Item 5
Discuss / Vote on CertiPath PIV-I Application
Judith Spencer

The FPKIPA accepted the CertiPath cross certification application for PIV-I. The vote to accept the CertiPath application passed, with 14/15 (or 93.35%) where a 75% majority vote was required.

Approval Vote for PIV-I Cross Certification Application from CertiPath			
Voting members	Vote (Motion – NRC; 2nd – Treasury)		
	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	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		
Veterans Administration	√		

Agenda Item 6
Discuss / Vote on DigiCert Cross Certification Application
Judith Spencer

Ms. Spencer asked Mr. Wilson to provide background. Mr. Wilson stated that he and others at DigiCert had been involved with PKI since the late 90's with ACES and various other programs. Currently, DigiCert is a CA mainly focused on SSL certificates. DigiCert is one of the largest SSL certificate providers, currently supporting projects in the Government and commercial sectors.

DigiCert seeks to cross certify their Assured ID CA to support a federated ID credential. It would be a commercial solution. It would support first responders, for example. DigiCert would first cross certify at the various Levels of Assurance requested, including PIV-I. DigiCert does not plan to provide PIV-I card management services, but would partner with others who have those services, while DigiCert provides the PKI certificates. DigiCert recognizes that as the cross-certified partner, they would be responsible for ensuring their partners meet FBCA requirements.

When asked who is the Federal government customer justifying their need for cross-certification, Mr. Wilson stated that it was a “chicken and egg” situation. DigiCert currently has customers for SSL certificates that may be interested in additional certificates if they are cross-certified with the FBCA. There are customers that don't want to stand up their own CA, and DigiCert could provide the commercial service to offer those credentials. Mr. Rea noted that as these credentials become more available State and local government organizations will decide to use them.

Mr. Froehlich asked if they would be providing cross-certified certificates to other providers (e.g., a bank) that would provide PIV-I credentials to their customers. Ms. Spencer stated that there is a new market for these types of credentials with National Strategy for Trusted Identities in Cyberspace, and the wider the market, the better it is.

Mr. Hannan asked how we certify that DigiCert's partners are doing the right thing. There was discussion about how much the Day Zero audit would cover for operations.

Mr. Froehlich pointed out that DigiCert's application shows just PIV-I, but should include all three PIV-I OIDs. It was agreed the FBCA application template needs to be updated to clearly identify that when one requests PIV-I, it means they are asking for all three related OIDs.

Mr. Wilson was asked why DigiCert is requesting both C4CA and FBCA cross certification. The answer is that they want to be diverse. The FPKI has different CAs for the FBCA and the C4CA, and DigiCert just has one CA that will handle all policy levels. This means DigiCert would still need two cross-certificates. There was some concern with being able to clearly identify that an agency wished to trust only some of the policies under DigiCert's one CA. Ms. Spencer stated that the problem already exists, and relying party applications should be looking at the policy OIDs, not just the Trust Anchors.

Mr. Froehlich asked if the DigiCert CA is the same as the HEBCA CA. Mr. Rea responded, No. DigiCert is running a CA for HEBCA similar to the way Verizon Business operates the Safe BioPharma Bridge CA and VeriSign operates the CertiPath Bridge CA.

Ms. Mitchell voiced a concern about the FBCA being cross-certified with a DigiCert CA that has both C4CA and FBCA Mapping, as that presents a problem for relying party applications that implement direct trust. Ms. Spencer suggested that one still has to evaluate the assurance levels. However, this may result in some circular issues with certificate path validation. These types of technical issues should be addressed during the mapping process rather than during the discussion on whether or not to accept an application for cross certification.

Mr. Sulser asked how DigiCert would perform the Day Zero audit if the other PIV-I parts aren't there yet. Mr. Schminky replied we have done it in the past. Ms. Spencer noted that these are valid questions in the next stage.

Mr. Hannan asked if the FPKIPA can approve an application for cross certification without a Federal sponsor. Ms. Spencer said the *Crits and Methods* recommends a Federal Sponsor, but that is an old requirement and is outdated since the Federal Identity management landscape has changed – we have a much wider need for interoperability. The suggestion was made that FPKIPA be the sponsor, if the application for cross certification was accepted.

A suggestion was made to update the application for cross certification to specify a Federal sponsor was not required if there was a clear indication that the application for cross certification was still in the interest of the Federal government.

The FPKIPA accepted the DigiCert cross certification request. The vote to accept the DigiCert application passed, with 12/15 (or 80%) where a 75% majority vote was required.

Approval Vote for PIV-I Cross Certification Application from DigiCert			
<i>Please check all that apply.</i>			
x C4CA			
x FBCA Medium Commercial Best Practices			
x FBCA Rudimentary			
x FBCA Medium Hardware			
x FBCA Basic			
x FBCA Medium Hardware Commercial Best Practices			
x FBCA Medium			
x PIV-I			
Voting members	Vote (Motion – USPS; 2 nd – Treasury)		
	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	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		
Veterans Administration	√		

Agenda Item 7

Discuss / Vote on HEBCA Cross Certification Application

Judith Spencer

Ms. Spencer introduced the HEBCA application for cross certification with the statement that HEBCA has been collaborating with the FPKIPA from the beginning, and that they are now ready to go live. Mr. Rea said there are universities ready to cross certify, and that VA and DoEd as well as other agencies that do research with academia would benefit from the relationship.

HEBCA has decided that the best approach for them was to partner with a commercial CA. They have chosen DigiCert to be that commercial partner. The new HEBCA root has been created and is live. A number of schools are waiting to begin issuing credentials. HEBCA expects upcoming projects with SAFE, and they may cross certify directly with the SAFE BioPharma Bridge as well.

Ms. Brown asked whether there will be issues with path validation if HEBCA cross certifies with bridges that are already cross certified with the FBCA. Mr. Rea stated that we'll need to look at this issue. However, the recommendation is for Bridges to form a mesh so that members of a bridge can use path length constraints to limit transitive trust. Ms. Spencer explained that it might be necessary for HEBCA to have a separate, stand-alone CA for C4CA operations.

The FPKIPA accepted the HEBCA cross certification request. The vote to accept the HEBCA application passed, with 13/15 (or 86.67%) where a 75% majority vote was required.

Approval Vote for Cross-Certification Application from HEBCA			
Desired Federal PKI Cross Certification Level(s)			
<i>Please check all that apply.</i>			
X C4CA			
X FBCA Medium Commercial Best Practices			
X FBCA Rudimentary			
X FBCA Medium Hardware			
X FBCA Basic			
X FBCA Medium Hardware Commercial Best Practices			
X FBCA Medium			
X PIV-I			
Voting members	Vote (Motion – GPO; 2nd – NRC)		
	Yes	No	Abstain
Department of Defense	√		
Department of Health & Human	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		

Approval Vote for Cross-Certification Application from HEBCA			
Desired Federal PKI Cross Certification Level(s)			
<i>Please check all that apply.</i>			
X C4CA			
X FBCA Medium Commercial Best Practices			
X FBCA Rudimentary			
X FBCA Medium Hardware			
X FBCA Basic			
X FBCA Medium Hardware Commercial Best Practices			
X FBCA Medium			
X PIV-I			
Voting members	Vote (Motion – GPO; 2 nd – NRC)		
	Yes	No	Abstain
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission	√		
SSA	ABSENT		
USPS	√		
USPTO	ABSENT		
Veterans Administration	√		

Agenda Item 8

FPKI Certificate Policy Working Group (CPWG) Report Charles Froehlich, Co-Chair

Charles Froehlich presented the CPWG report.

- There is now a SHA-256 WG, which has developed a draft SHA-256 guidance memo. Ms. Spencer and Tim Polk are working to edit the SHA-256 memo. Ms. Spencer provided some highlights of the content:
 - A warning that if anyone is running XP with an earlier version than SP3, things will break and there are some issues with email.
 - The approach to the memo is to link to technical detail, rather than include it.
 - Beginning July 15, 2010, Microsoft will no longer support XP SP2 and earlier OS versions.
 - Brant Petrick sent an email to the CPWG members and the FPKIPA members to authenticate to a secure web site containing SHA-256 test results provided by Treasury, EPA, USPTO, and SSA
- FPKI Security Profile WG
 - A second working group has been formed to develop a FPKI security profile that is standard for all Federal agencies.

- The next meeting is on July 15, 2010 at GSA, 18th and F St, Conference room 5141B starting at 10:00 a.m.

Agenda Item 9
FPKI Management Authority (FPKI MA) Report
Wendy Brown (for Cheryl Jenkins)

Ms. Jenkins and other FPKI MA members went to Dallas and Denver to look at possible data centers for one of the full operational sites and for Repository-only sites. The FPKI MA is currently evaluating the sites and should have something to announce soon (i.e., whether any of the sites are acceptable).

A message about using DNS to access the FPKI Repositories and load balancing was sent to the FPKI community this week. Ms. Spencer suggested that this information should also be posted on the FPKIPA web site.

Ms. Brown has requested that agencies and cross-certified organizations provide her with an email list of operations staff who should receive communications such as the aforementioned DNS announcement. The FPKI MA wants to be sure that it is reaching all the necessary customers.

Ms. Jenkins expects to award the Auditor contract by the end of the week.

The FPKI MA continues to see growth in the usage of the FPKI Repositories. There were over 100 million searches in June. There were over 60 million Directory searches and over 40 million HTTP requests. Usage of both protocols is increasing, but there is a higher rate of increase in HTTP traffic.

The FPKI MA issued a new cross-certificate to USPTO after their approval for Medium Hardware and the PIV pass-through policies. The USPTO CA that was cross-certified has already moved to use SHA-256.

Agenda Item 10
Other Agenda Items
Judith Spencer

ICAM Update

Tomorrow is the monthly ISIMC. Ms. Spencer will be briefing the FPKI Redesign to the committee, and plans to mention the SHA-256 issue. Ms. Spencer will also mention the load balancing information.

The Roadmap Implementation Guidance work is underway again. The first phase is expected to be complete in the September/October 2010 timeframe. If the Deloitte team asks for input, please assist them.

Yesterday, NIST held a workday for Federal employees only to discuss revision of FIPS 201. NIST needs Commerce approval to open the document for review, and the group yesterday agreed it needs revision. There are places in FIPS 201 today that have since been eclipsed by other NIST Special Publications or standards, so some discussion was held about raising the level of FIPS 201 and referencing these other documents instead of repeating the details.

**Agenda Item 11
Adjourn Meeting**

USPS (Mr. Stepongzi) made the motion to adjourn, and Ms. Spencer adjourned the meeting at 11:49 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	Ongoing

FPKIPA Minutes 13 July 2010, Final

No.	Action Statement	POC	Start Date	Target Date	Status
381	Judith Spencer will check with NIST for additional guidance on device certificates.	Judith Spencer	9 June 2009	18 June 2009	Open
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	Open
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
390	Brant Petrick will contact CertiPath (Steve Howard/Jeff Nigriny) to ask them if they intended to apply also for PIV-I cardAuth and PIV-I content signing.	Brant Petrick	8 June 2010	15 June 2010	Closed
391	Brant Petrick will send the letter to Dan Lindsey at USPTO regarding the requirements a Legacy Federal PKI must meet to issue PIV related certificates.	Brant Petrick	8 June 2010	15 June 2010	Closed