



Minutes of the 8 June 2010 Meeting
General Services Administration (GSA)
18th and F Streets, NW, CR 5141A
Washington, D.C.
9:35 a.m. – 11:25 a.m.

A. AGENDA

1. Welcome / Introductions
2. Discuss / Vote on 11 May 2010 FPKIPA Minutes
3. NIST (Dr. Ronald Ross) Briefing on Continuous Monitoring and CyberSecurity: "State of Transformation--Next Generation Risk Management for the Federal Government."
4. Discuss / Vote on CertiPath Application for cross certification with the FBCA at PIV-I Hardware
5. Review / Vote on VeriSign Application for cross certification with the FBCA at PIV-I Hardware, PIV-I CardAuth and PIV-I Content Signing
6. FPKI Certificate Policy Working Group (CPWG) Report
 1. USPTO Mapping Report (Basic, Medium and Medium Hardware)
 2. Discuss / Vote to Cross-Certify USPTO at Basic, Medium and Medium Hardware
 3. Discuss / Vote on FBCA CP Change Proposal: 2010-04 (PIV-I UUID)
 4. NIST Identified Technical Issues:
 1. How to Anchor PIV-I OIDs to Common
 2. Letting Legacies use their own Trust Anchor for passing cardAuth from FBCA to Common
 3. Having legacies cross-certify with Common
 5. Real I.D.
7. FPKI Management Authority (FPKI MA) Report
8. Other Agenda Items
 - *ICAM Report*
9. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 12/15 (or 80%) where a two-thirds majority was required. Another member (DoD) joined later, via teleconference, bringing the total to 13/15 or 86.7% of voting members.

FPKIPA Minutes 8 June 2010, FINAL

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	
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	Levine, Susan	Teleconference
Nuclear Regulatory Commission (NRC)	Sulser, David	
SSA	Mitchell, Eric	ABSENT
USPS	Stepongzi, Mark	Teleconference
USPTO	Lindsey, Dan	
Veterans Administration (VA)	Jurasas, Eric	ABSENT

OBSERVERS

Organization	Name	Telephone
Entrust	Hernick, Nicholas	Teleconference
Entrust	Moore, Gary	
GPO IG Audit Office (Ernst & Young)	Iijima, Timothy (T.J.)	
DoE	Breland, Mary Ann	Teleconference
FPKIPA Support	Louden, Chris	Teleconference
EPA (Contractor)	Simonetti, David	Teleconference
FPKI MA and FPKIPA Support (Contractor, Protiviti)	King, Matt	
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoS (Contractor, ManTech)	Froehlich, Charles	
FPKIPA Secretariat (Contractor, Protiviti)	Fincher, Judy	
FPKIPA (Contractor, Protiviti)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	
IdenTrust (vendor)	Schambach, Marco	Teleconference
NIST	Ross, Ronald	Guest Speaker
State of Illinois	Anderson, Mark	
GSA ISSO	Morgan, Bill	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Chair

The FPKIPA met at the GSA Headquarters, 18th and F Streets, NW, Conference Room 5141A, Washington, D.C. Judith Spencer, Chair, called the meeting to order at 9:35 a.m., and conducted introductions of those present in person and via teleconference. We wish to thank Judith Spencer of GSA for hosting this meeting and Dr. Ron Ross of NIST for briefing us on cyber security. Judith Spencer again expressed regrets that her replacement, Deborah Gallagher could not attend because she was on travel.

Agenda Item 2

Discuss / Vote on 11 May 2010 FPKIPA Minutes—Judy Fincher

Ms. Fincher said that all changes had been made to the circulated copy and asked for a vote to approve the minutes. The minutes were approved by 12/15 (80%) where a 50% majority vote was required.

Approval Vote for 11 May 2010 FPKIPA Minutes			
Voting members	Vote (Motion – Treasury ; 2nd – USPTO)		
	Yes	No	Abstain
Department of Defense	ABSENT		
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		
USPS	√		
USPTO	√		
Veterans Administration	ABSENT		

Agenda Item 3

NIST (Dr. Ronald Ross) Briefing on Continuous Monitoring and CyberSecurity: “State of Transformation--Next Generation Risk Management for the Federal Government.”

Dr. Ronald Ross gave a briefing, based on the PowerPoint slides distributed in advance of the meeting, entitled, “State of Transformation: Next Generation Risk Management for the Federal Government.”

He described how far the IT security community has come since FISMA was enacted seven years ago. Now we are looking at an explosion of IT infrastructure, with an accompanying exponential growth in malware, he said. There is no perfect secure system and the primary goal of IT security is to reduce risk and still operate in the face of an active attack. This is a new concept: operating while under attack. Availability is the greatest threat, he said. We need to limit the time the attacker has to exploit the vulnerability, he said.

“Defense in depth” (guards, guns and gates) and continuous monitoring (people, technology and processes) are basic to transformative IT operations.

Dr. Ross said that DoD, NIST and DNI have created a Unified Information Security Framework to address the C&A process. His briefing contains the depiction of a generalized model. This was driven by the revision of NIST SP 800-37 (Feb. 2010). It created the Risk Management Framework, a six step process integrated across the three communities. The C&A is now focused on life cycle security and calls for an aggressive use of IT security.

He said the NIST Continuous Monitoring guidance is flexible and agile and can be customized for a particular community. In response to a number of questions, he urged the Fed PKI community to develop its own profile. Adapt the NIST SP 800-53 rev. 3 controls to support your mission, he urged. Never degrade the mission, he emphasized. He offered NIST’s assistance in building the technical profile, e.g., the set of controls to be deployed in Federal PKI systems, and said NIST would consult on “political” issues, e.g., how to get approval from OMB, the CIO Council, ISIMC, etc.

Ms. Spencer said she would like to take him up on his offer and tasked the CPWG with forming a special study group to develop such a profile. Anyone wishing to contact Dr. Ross should contact the FPKIPA Secretariat by email or phone.

Agenda Item 4

Review / Vote on CertiPath Application for cross certification with the FBCA at PIV-I Hardware—Judith Spencer, Terry McBride

This item was tabled because we believe there is additional information that needs to be added to the Application. Currently, CertiPath is only requesting cross certification at PIV-I Hardware and we believe they will also need PIV-I cardAuth and PIV-I content signing. They will need to do a “delta” mapping to add the PIV-I OIDs to their existing PKI Bridge under their regular CA.

ACTION: Brant Petrick will contact CertiPath (Steve Howard/Jeff Nigriny) to ask them if they intend to apply also for PIV-I cardAuth and PIV-I content signing.—not just PIV-I Hardware. (DONE)

Ms. Spencer said that John Cornell modified language in the PIV-I MOA template for Bridges, which she would distribute to the CPWG.

Agenda Item 5

Review / Vote on VeriSign Application for cross certification with the FBCA at PIV-I Hardware, PIV-I CardAuth and PIV-I Content Signing—Judith Spencer

The FPKIPA accepted the VeriSign cross certification request for PIV-I Hardware, PIV-I CardAuth and PIV-I Content Signing and sent it forward to the CPWG to be mapped. In addition to the mapping, we will need to do an operational parameters review and white space mapping.

Debbie Mitchell had an issue with the diagram in the application. She asked: How will relying parties deal with MedHW CBP being under the same root as PIV-I? Ms. Spencer said that DoD would have to read the OIDs.

When and if Symantec acquires VeriSign, we will have to revisit the whole cross certification. Symantec has made an offer to VeriSign and the sale is currently in the review cycle. Once the sale is final, we will need to make sure it is US-owned and that trusted roles are occupied by U.S. citizens.

The vote to accept the VeriSign application passed, with 13/15 (or 86.7%) where a 75% majority vote was required.

Approval Vote to accept the VeriSign Application for cross certification with the FBCA at PIV-I Hardware, PIV-I CardAuth and PIV-I Content Signing			
Voting members	Vote (Motion – GPO ; 2nd –NRC)		
	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	ABSENT		
USPS	√		
USPTO	√		
Veterans Administration	ABSENT		

Agenda Item 6

FPKI Certificate Policy Working Group (CPWG) Report— Terry McBride, Co-Chair

1) USPTO Mapping Report (Basic, Medium and Medium Hardware)

Terry McBride said the CPWG has successfully completed the USPTO mapping and is recommending the USPTO Mapping Report to the FPKIPA for approval. No vote is required because the mapping was not contentious.

2) Discuss / Vote to Cross-Certify USPTO at Basic, Medium and Medium Hardware

The FPKIPA voted to cross-certify USPTO at Basic, Medium and Medium Hardware (RFC 3647 format) with an 86.7% majority vote when 75% was required.

USPTO also plans to ask permission to use PIV Authentication and Card Authentication for pass through. Currently their CP stipulates 24 Hour CRLs (Section 4.9.7) when FIPS 201 requires 18 Hour CRLs.

ACTION: 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. (DONE)

Approval Vote to Cross Certify USPTO (3647 RFC Format) at Basic, Medium and Medium Hardware			
Voting members	Vote (Motion – Justice ; 2nd –State)		
	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	ABSENT		
USPS	√		
USPTO			√
Veterans Administration	ABSENT		

3) Discuss / Vote on FBCA CP Change Proposal: 2010-04 (PIV-I UUID)

The purpose of this change is to clarify the encoding in PIV-I cardAuth certificates. The vote to approve the change proposal for PIV-I UUID passed with (13/15) 86.7% where a 75% majority is required.

Vote to approve FBCA CP Change Proposal: 2010-04 (PIV-I UUID)			
Voting members	Vote (Motion – GPO ; 2nd –NRC)		
	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	ABSENT		
USPS	√		
USPTO	√		
Veterans Administration	ABSENT		

4) NIST Identified Technical Issues

Mr. McBride also listed three technical issues that NIST has brought to our attention. The CPWG is currently addressing these three issues.

- a. How to Anchor PIV-I OIDs to Common
- b. Letting Legacies use their own Trust Anchor for passing cardAuth from FBCA to Common
- c. Having legacies cross-certify with Common

5) Real I.D.

Real I.D. is an issue the CPWG is also exploring. We are currently waiting for a briefing from DHS to guide our thinking about allowing the states to use Real I.D. as if it were a federal ID for purposes of identity proofing.

Agenda Item 7

FPKI Management Authority (FPKI MA) Report--Wendy Brown (for Cheryl Jenkins)

- **Infrastructure Management**
- Repository traffic has increased 29% per month in the past 6 months. The FPKI MA is looking to load balance between our two production sites to improve throughput and this should be in place by the end of June. In addition the FPKI MA is planning for the three additional repository only sites to be

added in the near future. Ms. Jenkins is looking at additional repository sites in Texas and a production site in Denver, CO. It is difficult for the FPKI MA to determine the maximum required throughput based on the growth seen over the last year.

Detailed repository usage statistics can be found on the Repository Dashboard which was distributed to the listserv this morning.

Ms. Brown said the IV&V was completed on 4 June 2010 and reported that the system met all the operational requirements.

Agenda Item 8

Other Agenda Items—Judith Spencer

ICAM Report

Ms. Spencer said that work on the ICAM Roadmap is starting up again. She anticipates that the FPKIPA will be asked to provide input going forward.

Agenda Item 9

Adjourn Meeting

GPO (John Hannan) made the motion to adjourn and Ms. Spencer adjourned the meeting at 11:25 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

FPKIPA Minutes 8 June 2010, FINAL

No.	Action Statement	POC	Start Date	Target Date	Status
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
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

FPKIPA Minutes 8 June 2010, FINAL

No.	Action Statement	POC	Start Date	Target Date	Status
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