



FEDERAL PKI POLICY AUTHORITY

September 13, 2011 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:35 a.m. – 10:55 a.m.**

09:30	Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
09:50	Discuss / Vote on August 9, 2011 FPKIPA Minutes	Matt King
10:00	FPKI Certificate Policy Working Group (CPWG) Report <ul style="list-style-type: none">• Review of ORC Status• Review of DigiCert Status• Review/Vote on LDAP Change Proposals (FBCA and FCPF)• Review/Vote on Device Certificate Change Proposals (FBCA and FCPF)• Presentation of draft FPKIPA Charter and By-Laws• Discussion on FISMA Matrix vis-à-vis FPKI Security Controls Profiles• Discussion on CA/Browser Forum Extended Validation Certificate proposal	Charles Froehlich
10:30	FPKI Management Authority (FPKI MA) Report	Darlene Gore
11:00	Position Paper-Microsoft Timestamp Requirements	Matt Kotraba
11:30	Other Agenda Items <ul style="list-style-type: none">○ <i>ICAM Update—Deb Gallagher</i>○ <i>If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.</i>○ <i>Next FPKIPA meeting, October 18, 2011</i>	Deb Gallagher
12:00	Adjourn Meeting	Deb Gallagher

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DoD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Frahm, Jarrod M.	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	A
Veterans Administration (VA)	Jurasas, Eric	T

b. Observers

Organization	Name	T – Telephone P – In Person
CipherSolutions	Ahuja, Vijay	T
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA, FPKIMA PM	Gore, Darlene	P
USPTO (Contractor)	Jain, Amit	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
State (Contractor)	Jung, Jimmy	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Kotraba, Matt	T
US Access (Contractor)	Lins, Andrew	T
GSA (Contractor, Unisys)	Petrick, Brant	T
FPKIPA (Contractor, Protiviti)	Povenmire, Elizabeth	P
eValid8	Schminky, Jim	P
eValid8	Brian Dilley	P
DHS (Contractor)	Schomo, Larry	T
FPKIPA (Contractor, Protiviti)	Sonnier, Tiffany	P

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher, Chair

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza, SW CR4841 Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:35 a.m. EST, and those present, both in person and via teleconference introduced themselves.

Ms. Gallagher made a number of announcements in her opening remarks.

- The ICAMSC is meeting tomorrow (Wednesday, September 14) from 10 a.m. -12 p.m. EST at main Justice. Please let them know you're coming – Mr. Paul Fitzgerald is the main POC.
- The ISIMC is also meeting tomorrow from 1-3 p.m. EST – Ms. Gallagher will be briefing an update of FPKIPA activities.
- Mr. Man Lau is now working for Ms. Gallagher in the IDM division.
- With the recent earthquake and DigiNotar compromise, we realized we may not have sufficient incident response procedures. So an effort will begin to evaluate these procedures, and volunteers are needed to support this effort. Anyone who is interested in supporting this effort should contact Mr. Jeff Jarboe of the FPKIMA. Mr. Matt King will send out a request to the FPKIPA Mail List asking for volunteers.

Ms. Gallagher notes that the CPWG continues work on the Crits and Methods document and the Bylaws and Charter document, and participation by all agencies is encouraged. As part of the Charter review, we discovered that we're overdue for the FPKIPA Chair election. We should have voted and elected in July 2011. A vote will be held in November 2011 and the options will be to elect (or re-elect) a new Chair or vote to assign GSA as the Permanent Chair.

Ms. Gallagher also mentioned that the “/s/” convention was discussed since there is a desire to remove the option from the Charter and encourage digital signatures for Electronic Votes. Ms. Gallagher asked if all of the voting members can sign a document or an email with a digital signature, and asked them to let her know if they cannot digitally sign emails or documents. Mr. David Sulser mentioned that members should consider whether they can sign email at the desktop vs. on a mobile device.

ACTIONS:

1. Mr. King will send announcement to the group asking for volunteers to develop incident response procedures.
2. All FPKIPA members shall submit their nomination for a new FPKIPA Chair to Ms. Gallagher and Mr. King by October 31, 2011.

Discuss / Vote on August 9, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the August 9, 2011 FPKIPA minutes. HHS motioned to approve; NRC seconded. The motion was approved unanimously.

Approval Vote for August 9, 2011 FPKIPA Minutes			
Voting members	Vote (HHS Motion; NRC Second)		
	Yes	No	Abstain
Department of Defense (DoD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury) - ABSENT			
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO) - ABSENT			
Veterans Administration (VA)	√		

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

Review of ORC Status-

Following the last FPKIPA meeting and resolution of the one outstanding item regarding the ORC audit, an e-vote was conducted to approve ORC for cross certification at Medium, Medium Hardware, and PIV-I. This vote passed (16/16—100%).

Review of DigiCert Status

An e-vote was conducted to approve DigiCert for cross certification at Rudimentary, Basic, Medium CBP, Medium Hardware CBP, Medium, and Medium Hardware. This vote passed (14/16—87.5%; SSA & VA abstained). DigiCert originally applied for cross certification at PIV-I, but decided to move forward without PIV-I at present. Following completion of their PIV-I testing, DigiCert will request that they be approved as a PIV-I provider.

Review/Vote on LDAP Change Proposals (FBCA and FCPF)

The CPWG review of the FPKIMA LDAP Change Proposals to the FBCA and FCPF CPs is still ongoing. At issue was the maintenance of LDAP support until there is certainty that LDAP is no longer required by FBCA and FCPF cross certified and subordinate entities. At the last FPKIPA meeting it was determined that there was a need to (a) confirm LDAP certificate expiration; (b) prepare a “white list” of access points; (c) evaluate the impact on PKI end-users and infrastructure; and, (d) that the FPKIMA would develop a roadmap for LDAP phase out upon final approval. It was also requested that DoD report back on Lessons Learned from their migration away from LDAP. All of these items are still pending. In addition, the FCPF LDAP Change Proposal will first require amendment of FIPS 201, comments for which have already been submitted to NIST and will be discussed with NIST at the 20 September or 6 October CPWG meeting. Ms. Debbie Mitchell mentioned DoD could provide lessons learned from their LDAP transition.

ACTION:

1. Ms. Mitchell will provide DoD Lessons Learned from the LDAP transition by Oct 6, 2011.

Review/Vote on Device Certificate Change Proposals (FBCA and FCPF)

The CPWG has completed its review of the DoD and DHS Device Certificate change proposals to the FBCA and FCPF CPs. These change proposals accomplish two things: (1) expand the meaning of “Device” to include both hardware devices and software applications; and (2) distinguish between certificates housed on tokens and those housed in software. The change proposals have been revised to maintain comparability between the two CPs, but neither mandates the use of certificates OIDs to identify those distinctions except as required by the Relying Party. As such, the CPWG recommends that the FPKIPA vote on their acceptance.

The CPWG agreed at the last meeting that Ms. Hansen would work with DoD to finalize the FBCA change proposal to add just enough language to allow people to assert to Common Policy. The change proposal was sent out Friday afternoon, using most of the

language from Common for Bridge. The Bridge change proposal number is 2011-05 and Common is 2011-02. Ms. Gallagher proposed the vote be held to approve both change proposals at the same time due to similar content. No objections to this approach were raised. HHS moved to approve the change proposals, DoJ seconded. The change proposals were approved unanimously.

Approval Vote for Device Certificate Change Proposals (FBCA and FCPF)			
Voting members	Vote (HHS Motion; DoJ 2nd)		
	Yes	No	Abstain
Department of Defense (DoD)	√		
Department of Energy (DOE) – ABSENT			
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury) - ABSENT			
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO) - ABSENT			
Veterans Administration (VA)	√		

Presentation of draft FPKIPA Charter and By-Laws

The CPWG has nearly completed review of the CPWG charter and bylaws. They will be finalized at the Sept 20 CPWG meeting, and will be distributed for review and vote prior to the October 11th FPKIPA meeting. Two issues of particular note: (1) use of /s/ signing, and (2) identifying an authoritative source for mandated funding to support the activities of the FPKIPA and the Chair. These issues will be resolved at the September

20th CPWG meeting. The question was raised about who should officially approve the charter. Ms. Gallagher stated that research still needs to be done to find out.

It was noted again that an election for a new FPKIPA Chair will be held in November 2011, and nominations are being accepted. Please send your nominations to Ms. Gallagher and Mr. King.

Discussion on FISMA Matrix vis-à-vis FPKI Security Controls Profiles

The last remaining item to have the Federal PKI Security Controls Profiles for NISTSP 800-53 and NIST SP 800-53A specified as the governing federal standard is to have these profiles recognized and mandated in the annual FISMA Metrics. Mr. Charles Froehlich reported that he, Mr. King, and Ms. Gallagher held conversations with DHS, and have forwarded questions to them along with supplementary information about each question to guide respondents in answering the appropriate question(s). The questions are specifically keyed to (a) entities cross certified with either the FBCA or FCPCA; (b) SSPs subordinate to the FCPCA; or (c) customers of an SSP that are responsible for some portion of the FISMA infrastructure boundary, such as RA functions. The FISMA Metrics Team asked that questions provide a measurable result (e.g., what percentage of controls is satisfied?). More detailed questions appear in quarterly Metrics.

Discussion on CA/Browser Forum Extended Validation Certificate Proposal

Following the last FPKIPA meeting, the Chair circulated the CA/Browser Forum Extended Validation Certificate proposal. The CAB intends to have this document incorporated into the required federal IT standards. However, it has been noted by some who have reviewed the document that there are issues with the proposal – aspects that are contrary to established FPKI standards and policies. The CPWG will review the document at the earliest opportunity, and FPKIPA members are strongly encouraged to review the document and participate in the CPWG discussion. It was decided that the document needs a thorough review so the Federal Government can make a decision on how to leverage the stated requirements because it has proprietary solutions and there are certain requirements that simply cannot be accommodated. This item will potentially be discussed at the Sept 20 CPWG Meeting, and if not, it may be pushed to the Oct 6 CPWG meeting.

FPKI Management Authority (FPKIMA) Report, Darlene Gore

Ms. Brown noted that there isn't much change in the trust store status other than Opera. It has been verified that Chrome Browser does not use a trust store. The FPKIMA is still researching Chrome OS. After looking at Chrome and Chrome OS, the FPKIMA is now looking at Mobile trust stores. The FPKIMA is asking for feedback from the FPKIPA as to whether the FPKIMA is researching the right devices currently. Ms. Gallagher suggested including more tablets than just iPad. Ms. Brown asked FPKIPA members to

please send information about higher-priority devices. The FPKIMA is looking to identify the OS and hardware itself. Ms. Darlene Gore noted that one problem has been lack of point of contacts, so that the issues can be discussed. It would be helpful if any agency has contacts. Ms. Gallagher went to a USDA mobile devices conference. She mentioned that the main position in this conference was that mobile devices are “wide open” when it comes to security. Blackberry is the most secure because they do encryption. Some of the others mobile devices have applications that are not verified or validated. If you connect to your network with such devices, you are exposing your network. DoD noted that there are efforts currently underway for security evaluation of mobile devices. Ms. Mitchell suggested the FPKIPA might need to make a request to a customer advocate to get the correct information about these efforts. Ms. Gallagher also mentioned that a number of agencies are treating mobile devices and treating them as a service so certain security requirements do not apply.

SHA2 Decommission

The SHA2 decommission has been officially completed. Ms. Brown asked FPKIPA members to provide any information on changes in traffic (e.g., it was noted that there was an increase in usage in August when August is usually a slow month for the Federal Government). The FPKIMA would like to know about any impact if you experience any downtime. There was a short (less than 3 hours on a weekend) period of time when only an expired CRL was available due to a data center outage, but the FPKIMA does not expect this caused issues for anyone in the FPKI Community. Ms. Gallagher praised the FPKIMA team for the excellent performance statistics.

Position Paper-Microsoft Timestamp Requirements

All comments have been resolved. The FPKIMA was seeking FPKIPA approval before sending the paper to Microsoft. Ms. Gallagher recommended that the paper be sent forward and all were in agreement.

Other Items

CITE guidelines are published on the idmanagment.gov website. The FPKIMA encourages all members to participate in CITE.

The next TWG Meeting is September 15, 2011 at PGS (Alexandria VA). Discussion topics include: Microsoft path validation issues and federal guidance on how to manage PKI trust stores. Mr. Chris Loudon noted that the process for resolving the Microsoft path validation is a breakthrough because this is a potential viable process for getting issues fixed. If there are other problems with Microsoft products, a similar resolution process can be followed.

Other Agenda Items, Deb Gallagher

NIST SP 800-63-1 is expected in the near future; it is currently going through comment review at NIST.

Federal ICAM is working closely with NSTIC to make sure that our trust framework provider process is available to everyone. A memo will come out soon saying that all web services should accept not only PIV and PIV-I, but also 3rd party approved providers. NIH already has iTrust – Ms. Gallagher can provide more information if interested.

Mr. Lau is looking at the approved products listing for FIPS-201 certification, and is reviewing the process – looking for interoperability testing.

The next ICAMSC meeting is September 14, 2011.

The next IAB meeting is September 28, 2011.

The next FPKIPA meeting is October 18, 2011.

Adjourn Meeting

Ms. Gallagher adjourned the FPKIPA meeting at 10:55 a.m. EST.

FPKIPA Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
433	Matt King will place a deadline for C4CA responses for the first August CPWG for all agencies to provide their position on the necessity of the C4CA	Matt King	July 12, 2011	August 8 2011	Closed
434	Ms. Brown will send the MA report to the PA after changing the TWG date.	Wendy Brown	July 12, 2011	July 19, 2011	Closed
435	Ms Cheryl Jenkins will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011	Cheryl Jenkins	July 12, 2011	September 15, 2011	Open
436	Ms. Gallagher will send an email with the request for a statement of need for removing the non-revocable certificates to the voting PA members .	Deb Gallagher	July 12, 2011	August 9, 2011	Open
437	Mr. Matt King will send the EGTTS briefing to the group	Matt King	July 12, 2011	August 9, 2011	Closed
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	July 12, 2011	September 13, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
439	Ms. Wendy Brown and Mr. Matt King work to establish a fed-only email list.	Matt King / Wendy Brown	August 9, 2011	September 13, 2011	Open
442	Mr. King will send ORC PIV-I testing documentation and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
443	Mr. King will send DigiCert audit letter and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
446	The Timestamp Server White Paper will be added to the CPWG and FPKIPA agendas.	FPKIMA	August 9, 2011	September 13, 2011	Closed
449	All FPKIPA members shall submit their nomination for a new FPKIPA Chair to Ms. Gallagher and Mr. King by October 31, 2011	All Voting Members	September 13, 2011	October 31, 2011	Open
450	Ms. Mitchell will provide DoD Lessons Learned from the LDAP transition by Oct 6, 2011.	Debbie Mitchell	September 13, 2011	October 6, 2011	Open