



FEDERAL PKI POLICY AUTHORITY

May 14, 2013 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 p.m. EST**

9:30	Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
9:35	Discussion/Vote: April 2013 FPKIPA Minutes	Matt King
9:45	FPKI Management Authority (FPKIMA) Report	Darlene Gore
10:15	FPKI Certificate Policy Working Group (CPWG) Report 1. Reference CP 2. Mapping Updates 3. Other Updates	Charles Froehlich
10:45	SHA-1 Transition Status	SHA-1 Affiliates
11:00	FPKIPA Chair Update	Deb Gallagher
11:45	Adjourn Meeting	Deb Gallagher

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	O'Brien, Shawn	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	T
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Newton, Paul	T
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	A
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	A
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
IdenTrust	Cox, Jerry	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA	Ghorbani, Salomeh	P
FPKIMA	Gore, Darlene	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
Treasury	Johnson, Todd	T
State	Jung, Jimmy	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Louden, Chris	P
Entrust	Schoen, Isadore	T
DHA (Contractor)	Shomo, Larry	T
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
SAFE	Wilson, Gary	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

Ms. Deb Gallagher, Chair, called the meeting to order at 9:33 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on April 9, 2013 FPKIPA Minutes, Matt King

The vote to approve the April 9, 2013 FPKIPA minutes was postponed until the June meeting.

FPKIMA Report, Darlene Gore

Ms. Gore noted that responses to the FPKIMA RFP were due on May 13, 2013. The technical evaluation is expected to begin on May 22, 2013. The FPKI Compliance Audit was completed and the report and letter were received. Eight discrepancies were found and a POA&M was submitted. The TWG evaluated a number of issues including long term validation of digital signatures, PD-Val testing process updates, Microsoft patches, and information from the CA/B Forum EV Code Signing Working Group. The Ascertia Path Discovery and Validation (PDVal) product was tested. The TWG reviewed and discussed the report. The FPKIPA agreed that the methodology was sound and no “product approval vote” was needed, so the approved products can be listed on IDManagement.gov once they pass testing.

The next two TWG meetings will be on June 25, 2013 and August 27, 2013.



May2013 Slides for
PA Meeting-final.pdf

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

Mr. Charles Froehlich presented the CPWG Report.

a. Reference CP

A majority of attendees had not reviewed/re-reviewed the Reference CP (NISTIR 7924). Therefore, only the additional comments were reviewed. NISTIR 7924, the NIST comment form, and the previous redline version of CPWG comments were sent out to the full CPWG with comments due by May 16, 2013 to allow two CPWG meetings for discussion and resolution prior to the June 9, 2013 response date.

b. Mapping Updates

- a. DoD ECA: Continued CPWG review. Additional requirements for clarification were returned to DoD. Resolution should be achieved at the 21 May CPWG meeting
- b. USPS: Reviewed the “white space” mapping specifically centered on issuing PIV-I certificates to non-USPS personnel; USPS will make updates to clarify these points.
- c. IdenTrust: Reviewed and resolved the remaining policy mapping issues. Testing is expected to begin in June.

c. Other Updates

- a. The Cross Certification Mapping Tiger Team presented a revised methodology using an MS-Excel spreadsheet format, vice the MS-Word format. DoS volunteered to add this new format to their existing cross certification baseline update package that will be submitted this week, along with analysis and comments back to the Tiger Team.
- b. The CPWG received a briefing from the “Office of the National Coordinator for Health IT” on the DIRECT Project dealing with the secure direct exchange of health information between health care providers over the Internet using SMTP and S/MIME based on PKI credentials.
 - 1. A number of Federal agencies have an interest in using DIRECT for exchange of Electronic Medical Records (EMR), but operate under stringent privacy and security policies
 - 2. Gaps between Federal requirements and current implementations exist stemming from the use of “Dual-Use” certificates, which are only allowed for “legacy systems” and the resulting lack of technical non-repudiation for Federal agencies. DIRECT was not yet specified when the term “legacy” was introduced in the FPKI Certificate Policies, therefore non-federal PKI issuers cross-certified with the FBCA CP opposed issuing Dual-Use certificates to DIRECT participants; however, the initial implementation of DIRECT required Dual-Use certificates.
 - 3. NIST will “tolerate” Dual-Use certificates for legacy systems as long as there is a path forward; FBCA permits Dual-Use certificates. ONC is requesting that DIRECT be considered a “legacy system” until the end of 2015. ONC has indicated they already have a plan in place to eliminate the requirement for Dual-Use certificates for federal participants that will end by then.

The CPWG concluded that a vote at the FPKIPA might indicate long-term approval for Dual-Use certificates and recommends that ONC coordinate a memorandum with the FPKIPA Chair to indicate that the FPKIPA has no objections to the use of Dual-Use certificates until the end of 2015.

Further discussion was held about ONC's use of the DIRECT protocol. There are still a number questions about their plans and approach. It was explained that the content transported over the DIRECT protocol in the ONC implementation is signed by a separate certificate. The dual use certificates are used only during the transport of the content. Ms. Gallagher stated that more information will be needed before the FPKIPA takes a position on this issue. Ms. Debbie Bucci will send information to Ms. Gallagher regarding the ONC approach (including a rollout plan) and request a statement of the FPKIPA's formal position when appropriate.

The PKI FISMA Metrics for 2014 is still under discussion, but requires the participation of all interested parties at a single meeting; therefore, CPWG members are requested to participate in this discussion at the next meeting

SHA-1 Transition Status, SHA-1 Affiliates

SAFE indicated they are still on schedule to transition to SHA-2 in September 2013.

FPKIPA Chair Update, Deb Gallagher

Ms. Gallagher presented the FPKIPA Chair Report. Upcoming meetings and events include:

Meeting	Date
CNSS Meeting	April 10, 2013
Mobile Technical Exchange Meeting	May 23 & June 6, 2013
CPWG	May 21 & June 6, 2013
TWG	June 25, 2013

Ms. Gallagher stated that the PIV-I for Non-US citizens approach met an impasse in the ICAMSC meeting. Therefore, a meeting will be held (including DoD) to resolve the outstanding issues and ensure that additional changes to PIV-I requirements are not needed.

Ms. Gallagher noted that the FCCX contract has not been awarded, but they expect FCCX to be awarded in the next two months and hope for a fully operational system to be established by September 2013. Several external organizations have expressed interest in using FCCX services.

Currently there is a lot of activity in NSTIC. Most notably, they are evaluating about 4 use cases involving PIV-I in the Identity Ecosystem Steering Group (IDESG). The next two meetings for this group will be in July at MIT and in October at NIST.

The next FPKIPA meeting is June 11, 2013. The meeting will be at USPS.



FPKIPA Chair
Report_14MAY13_fin

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 11:17 a.m. EST.

FPKIPA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
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	12-Jul-11	13-Sep-11	Closed
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSS	Wendy Brown	8-May-12	30-Jul-12	Open
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Closed
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open