



**FEDERAL PKI POLICY AUTHORITY**

**August 13, 2013 MEETING MINUTES**

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

<b>9:30</b>	<b>Welcome, Opening Remarks &amp; Introductions</b>	<b>Deb Gallagher – Chair</b>
<b>9:35</b>	<b>Discussion/Vote: July 2013 FPKIPA Minutes</b>	<b>Matt King</b>
<b>9:45</b>	<b>FPKI Management Authority (FPKIMA) Report</b>	<b>Darlene Gore</b>
<b>10:15</b>	<b>FPKI Certificate Policy Working Group (CPWG) Report</b> <ul style="list-style-type: none"><li><b>1. Discussion/Vote: FPKIMA Clarification Change Proposals (Resulting from Audit)</b></li><li><b>2. DoD Mapping Update</b></li><li><b>3. Mapping Updates</b></li><li><b>4. Other Updates</b></li></ul>	<b>Charles Froehlich</b>
<b>10:50</b>	<b>SHA-1 Transition Status</b>	<b>SHA-1 Affiliates</b>
<b>11:00</b>	<b>FPKIPA Chair Update</b>	<b>Deb Gallagher</b>
<b>11:45</b>	<b>Adjourn Meeting</b>	<b>Deb Gallagher</b>

## A. ATTENDANCE LIST

### a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Bures, Iva	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)	T
Department of Justice (DOJ)	Morrison, Scott	T
Department of State (State)	Newton, Paul	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Orozco, Leo (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	T
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Jackson, Angelina	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	A
Veterans Administration (VA)	Jurasas, Eric	P

**b. Observers**

<b>Organization</b>	<b>Name</b>	<b>T – Telephone P – In Person A – Absent</b>
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA	Ghorbani, Salomeh	P
USPS	Jackson, Angelina	P
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
Treasury	Johnson, Todd	T
DoS (Contractor)	Jung, Jimmy	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
ProTegeus	Shomo, Larry	T
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
STRAC	Webster, Chris	T

## B. MEETING ACTIVITY

### Welcome, Opening Remarks & Introductions, Deb Gallagher

Ms. Deb Gallagher, Chair, called the meeting to order at 9:37 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

### Discuss / Vote on July 9, 2013 FPKIPA Minutes, Matt King

There was a vote to approve the July 9, 2013 FPKIPA minutes. HHS motioned to approve; GSA seconded. The motion was approved unanimously.

Approval Vote for July 9, 2013 FPKIPA Minutes			
Voting members	Vote (HHS Motion; GSA Seconded)		
	Yes	No	Abstain or Absent
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)	√		
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) – Proxy to GSA	√		
Veterans Administration (VA)	√		

## **FPKIMA Report, Darlene Gore**

Ms. Wendy Brown presented the FPKIMA Report. The FPKI Key Rollover is planned for October 11, 2013. Re-key Cross-Certificates and Interim Cross-Certificates will be issued in October and November. The FPKIMA has begun sending Cross-Certification Renewal packages to Affiliates, which will be used to ensure all documentation is in order prior to new cross-certificate issuances.

Two E-Governance certificates were issued and a new cross-certificate was issued from the DoD iRoot CA to the FBCA to add the Device policy OIDs.

The TWG discussed a number of issues including long term validation of Digital Signatures. NARA is now moving to conversion of their records to electronic format. It was suggested that special FPKI Briefings be held to discuss sensitive issues and current incidents. An ad hoc TWG meeting on July 18<sup>th</sup> was held to discuss best practices for implementation of Certificate Authorities, but further discussions are needed in a closed forum to discuss the details. It was also suggested that the FPKIMA should monitor HTTP URLs as well as Directory Chaining. The next TWG will be held on August 27, 2013.



Aug2013 Slides for  
PA Meeting.pdf

---

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

Mr. Charles Froehlich presented the CPWG Report.

### **a. Discussion/Vote: FPKIMA Clarification Change Proposals**

The CPWG has again reviewed and revised the change proposals to the FBCA and FCPCA certificate policies.

The changes to the FBCA CP included (1) clarifying the circumstances for certificate modification; (2) clarifying the roles and responsibilities of trusted roles to preserve separation of duties; and, (3) clarifying multi-person access requirements

The changes to the FCPCA CP included (1) clarifying the roles and responsibilities of trusted roles to preserve separation of duties {this change maintains comparability with the FBCA CP}; and, (2) clarifying the types of events recorded in system and PKI application audit logs and how long those logs must be retained on site  
Both change proposals are submitted to the FPKIPA for discussion and vote.

There was a vote to approve the FPKIMA Clarification Change Proposals resulting from the recent FPKI Audit. HHS motioned to approve; VA seconded. The motion was approved unanimously.

<b>Approval Vote for FPKIMA Clarification Change Proposals</b>			
<b>Voting members</b>	<b>Vote (HHS Motion; VA Seconded)</b>		
	<b>Yes</b>	<b>No</b>	<b>Abstain or Absent</b>
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ) – Proxy to GSA	√		
Department of State (State) – Proxy to GSA	√		
Department of the Treasury (Treasury)	√		
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)	√		
Veterans Administration (VA)	√		

**b. DoD Mapping Update**

There is a vote required to accept/ reject two DoD iRoot policy discrepancies. DoD does not validate email addresses which is a policy violation. In addition, they will not transition from SHA-1 by the deadline. Ms. Spencer pointed out that, if the FRCA is shut down, this becomes a non-issue because the iRoot CA will no longer be cross-certified. Ms. Gallagher pointed out that the email issue may not be a security issue. Rather it is an assurance issue. DoD indicated that they are unable to validate the

email addresses due to multiple addresses and decentralized mail servers. Therefore, the FPKIPA needs to decide whether including email addresses that are not validated in certificates is a risk.

Both the DoD iRoot and DoD ECA CPs have completed basic policy mapping and are now in “white space” mapping; technical testing is also complete, but testing of end entity certificates and repository configuration is on hold until end entity certificates are issued

### **c. Mapping Updates**

Policy mapping for USPS is pending their feedback on one key point—the implementation of PIV-I credentialing

Policy mapping has begun for Certipath, and initial comments and questions have been returned for their response.

Policy mapping for Symantec, DoS, and STRAC will follow.

Policy mapping for Illinois and USPTO may require expedited handling due to the need to issue new cross certificates.

Other policy mappings are expected from Treasury, and from those other agencies that have not submitted to update their baseline mapping and revised MOAs.

### **d. Other Updates**

A list of issues (changes) to the FBCA CP has been compiled and circulated to the CPWG. We are discussing doing a major review of both the FBCA and FCPCA CPs during the next year rather than addressing each issue separately, or as a single massive change proposal.

### **SHA-1 Transition Status, SHA-1 Affiliates**

All Affiliates are asked to provide status on their SHA-1 Transition Plans if they have not already transitioned to SHA-2.

## **FPKIPA Chair Update, Deb Gallagher**

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

<b>Meeting</b>	<b>Date</b>
CNSS SSWG	Aug. 13, 2013
CPWG	August 20 & September 5, 2013
FAS Industry Day	August 26, 2013
TWG	August 27, 2013
ICAMSC	August 28, 2013
IAB	August 28, 2013
NSTIC / PM ISE conference	October 24, 2013
TSCP Symposium	November 14 & 15

Ms. Gallagher sent a request for feedback on the impact of decommissioning the FRCA. Only 2-3 responses were received. The decommissioning is still undecided, but the decision has been elevated to OMB and NIST for review.

Several discussions were held on the topic of PIV-I for Non-US citizens, but no information or specific use cases were received from FAA. Therefore, this type of issuance will be addressed on a case-by-case basis when specific use cases are brought to the attention of the FPKIPA. Ms. Gallagher suggested that the people with the use case (FAA, airlines, or others) bring use cases to the FPKIPA so specific problems can be solved.

Ms. Gallagher provided an update on FCCX and noted that the PMO has been established in GSA's Office of Citizen Services. It is hoped that a pilot will be operational in the next 30-60 days.

The NSTIC PMI-ISE conference will be held on October 24, 2013. The NSISS initiative is still working to get FICAM across all fabrics.

The next FPKIPA meeting is September 10, 2013. The meeting will be at USPS.



FPKIPA Chair  
Report\_13AUG13.ppt

**Adjourn Meeting**

Ms. Gallagher adjourned the meeting at 11:34 a.m. EST.

## FPKIPA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
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
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