



**FEDERAL PKI POLICY AUTHORITY**

**March 12, 2013 MEETING MINUTES**

**GSA NOMA**

**1275 1st St. NE, Conference Room 803**

**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: February 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. Vote: Digital Signature Change Proposal</b></li><li><b>2. Mapping Updates (including mapping tiger team)</b></li><li><b>3. Vote: VeriSign NFI Medium HW cross-certification approval</b></li><li><b>4. Vote Results: Exostar Cross-Certification</b></li><li><b>5. Other Updates</b></li></ul>	<b>Charles Froehlich</b>
<b>10:45</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)	Mitchell, Debbie	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)	Rice, Barry (Proxy to GSA)	A
Department of Treasury (Treasury)	Wood, Dan	P
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)	Stepongzi, Mark (Proxy to GSA)	A
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	A
Veterans Administration (VA)	Miller, Jason (Proxy for Eric Jurasas)	T

**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
Department of Defense (DOD)	Bures, Iva	T
IdenTrust	Cox, Jerry	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA	Ghorbani, Salomeh	P
Treasury	Johnson, Todd	T
State (Contractor)	Jung, Jimmy	P
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Louden, Chris	T
Exostar	Schoonmaker, Jon	P
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 9:32 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

### Discuss / Vote on February 12, 2013 FPKIPA Minutes, Matt King

There was a vote to approve the February 12, 2013 FPKIPA minutes. Treasury motioned to approve; GSA seconded. The motion was approved unanimously.

Approval Vote for February 12, 2013 FPKIPA Minutes			
Voting members	Vote (Treasury 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) – 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)			Absent
United States Postal Service (USPS) – Proxy to GSA	√		
United States Patent & Trademark Office (USPTO)			Absent
Veterans Administration (VA)	√		

## **FPKIMA Report, Wendy Brown**

Ms. Wendy Brown noted that there was no formal report for the FPKIMA. The Identrust certificate was reissued to address a name constraints issue. The next TWG meeting will be on April 23, 2013. Topics will include Electronic Record Retention and long term validation of digital signatures.

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

Mr. Charles Froehlich presented the CPWG Report.

### **a. Vote: Digital Signature Change Proposal**

The CPWG received no additional comments regarding inclusion of the Practice Note regarding promoting the use of digital signatures for PKI-related actions. It was determined that there is an ongoing need for discussion regarding the long-term validation of digital signatures, and for recommendations to NARA regarding the publication of updated guidance

There was a vote to approve the Digital Signature Change Proposal. Treasury motioned to approve; Justice seconded. The motion was approved unanimously.

<b>Approval Vote for February 12, 2013 FPKIPA Minutes</b>			
<b>Voting members</b>	<b>Vote (Treasury Motion; Justice 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)	√		
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)			Absent
United States Postal Service (USPS) – Proxy to GSA	√		
United States Patent & Trademark Office (USPTO)			Absent
Veterans Administration (VA)	√		

**b. Mapping Updates (including Mapping Tiger Team)**

The mapping Tiger Team continued to meet and identified additional improvements in mapping processes that are simple, yet reduce the review time for the CPWG significantly. The team continues to work to resolve other issues including:

- Challenges of the current mapping
- Duplication of mapped requirements
- Clarifying the “Care abouts”
- Reviewing overall mapping
- Policy language clarification – a long term issue

**c. Vote: VeriSign NFI Medium Devices HW cross-certification approval**

VeriSign requested the addition of the NFI OID at Medium Devices Hardware; given that all other Medium Devices HW requirements were met, this review found no issues with the VeriSign application and CP mapping

There was a vote to approve VeriSign NFI PKI at Medium Hardware. Treasury motioned to approve; GSA seconded. The motion was approved unanimously.

<b>Approval Vote for VeriSign NFI Medium Devices Hardware</b>			
<b>Voting members</b>	<b>Vote (Treasury Motion; GSA 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)	√		

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)			Absent
United States Postal Service (USPS) – Proxy to GSA	√		
United States Patent & Trademark Office (USPTO)			Absent
Veterans Administration (VA)	√		

**d. Vote: Exostar Cross-Certification**

ExoStar cross certification was approved via electronic vote

There was a vote to approve the cross-certification of Exostar. Treasury motioned to approve; GSA seconded. The motion was approved unanimously.

<b>Approval Vote for Exostar Cross-Certification</b>			
<b>Voting members</b>	<b>Vote (Treasury Motion; GSA 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)	√		
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)			Absent
United States Postal Service (USPS) – Proxy to GSA	√		
United States Patent & Trademark Office (USPTO)			Absent
Veterans Administration (VA)	√		

#### **e. Other Updates**

##### **INCITS ID Proofing Document**

The CPWG reviewed and provided comments to ISO/IEC JTC 1/SC 27 N11746 ISO/IEC WD1 29003 -- Information technology – Security techniques – Identity Proofing; recommended changes included: (1) clarification of the technology and uses of biometrics; (2) recommendations on how to consider portions of the overall human life cycle (e.g., military, medical status, etc.); and, (3) recommendations on procedural requirements and techniques

##### **SP 800-53 Rev4 Comments**

Reviewed and provided comments to NIST SP 800-53 Rev 4 Final Public Draft reiterating and expanding on references to the Federal PKI Security Controls Profiles to SP 800-53/53A.

##### **NIST/NSA Reference CP Discussion**

Reviewed and provided general comments regarding the initial NIST/NSA draft on developing a “Reference CP.” Comments were very general given that it was unclear if the “Reference CP” was to be a guideline on how to write a CP, a “fill-in-the-blanks” type exemplar, or a “Master CP” that all PKI entities, including the FPKIPA, would have to follow. Although the “Reference CP” was modeled after the FCPCA CP but had expanded security controls requirements (e.g., Section 6), the CPWG concluded that it required significant reworking before it could be considered again, and then only after clarification of its purpose. The CPWG is reaching out to NIST to request a briefing at a CPWG meeting in April.

### **Derived Credentials Discussion**

Began review and comment to the NIST Change Proposal to the FCPCA CP to implement Derived PKI Credentials; unfortunately, despite a few minor editorial points, the CPWG was unable to make much progress due to the fact that SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, has not been released for initial public comment. It is difficult to consider modifying either of the CPs without a firm basis for the requirement.

### **PKI FISMA Metrics**

At Treasury's request, discussion of the PKI FISMA Metrics for 2014 was held, but the CPWG did not have a copy of the metrics available, so there was little progress on the discussion and no movement to develop new, revised, or additional FISMA Metrics questions for submission.

### **Current Mapping Follow on Activities (DoD ECA, USPS, Identrust) Profile reviews, operational parameters, etc.**

Responses have been received regarding the DoD ECA, USPS and Identrust policy mappings. White Space mapping, certificate profile and operational parameters reviews are in progress, and PIV-I testing for Identrust is expected to begin within the next month. Baseline CP mappings are expected from CertiPath and DoS also within the next month.

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

Mr. Jerry Cox indicated that the D-Trade application at the Department of State is an Identrust ACES customer and they will be requesting an extension for using SHA-1 certificates that will align with DoD's request. Unofficially, there are indications that DoD will not stop issuing SHA-1 certificates until FY-18.

The FPKIMA will need information about any requests for extensions to allow time to adjust the Federal Root CA (FRCA)

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

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

<b>Meeting</b>	<b>Date</b>
ISIMSC	March 13, 2013

Meeting	Date
Mobile Technical Exchange Meeting	March 11 & 12, 2013
CPWG	March 19 & April 4, 2013
ICAMSC	March 27, 2013
IAB	March 27, 2013
E-PACs document	March 20, 2013
Relying Party guidance out for comment	April 11, 2013
First Identity Federation Committee meeting	March 13, 2013

Highlights of Ms. Gallagher's report include:

- The E-Signature Guidance document has been posted.
- There are potential opportunities for grant-funded pilots to encourage growth in the NSTIC ecosystem.
- There are several activities ongoing as part of the NSISS including implementation of FICAM across the various fabrics
- As part of the MPAWG, FIPS 201 testing is being re-evaluated and it will likely become FICAM testing.
- The FCCX evaluation team is performing evaluations of products over the next three weeks

The next FPKIPA meeting is April 9, 2013. The meeting will be at USPS.



FPKIPA Chair  
Report\_12MAR13\_fin

### **Adjourn Meeting**

Ms. Gallagher adjourned the meeting at 11:45 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