FEDERAL PKI POLICY AUTHORITY

12 APRIL 2011 MEETING MINUTES

USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:35 a.m. – 10:45 a.m.

Welcome, Opening Remarks & Introductions	**Deb Gallagher, Chair**
Discuss / Vote on 8 March 2011 FPKIPA Minutes	**Matt King**
FPKI Certificate Policy Working Group (CPWG) Report • **Discussion / Vote to Approve Entrust at PIV-I** • **Common Policy Change Proposal: Device Certificates Validation Clarification – Discussion** • **PIV-I Retesting Requirements - Status** • **Other Items** •	**Charles Froehlich**
FPKI Management Authority (FPKIMA) Report	**Cheryl Jenkins**
Other Agenda Items • **SSPWG Update** • **ICAM Update** • **Next FPKIPA meeting: May 10, 2011**	**Deb Gallagher**
Adjourn Meeting	**Deb Gallagher**

A. ATTENDANCE LIST

A.1 Voting Members

Organization	Name	Present?
Department of Energy	Thomas, Michelle	T
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T

Organization	Name	Present?
Department of State	Frahm, Jarrod M.	P
GSA	Gallagher, Deb	P
GPO	Smith, Steve (Proxy for John Hannan)	T
Veterans Administration (VA)	Miller, Jason (Proxy for Eric Jurasas)	P
USPTO	Lindsey, Dan	A
Department of Homeland Security	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Defense	Mitchell, Debbie	T
SSA	Mitchell, Eric	T
NASA	Wyatt, Terry (Proxy for Susan Levine)	T
Department of Justice	Morrison, Scott	P
Department of Treasury	Wood, Dan	T
Department of Health & Human Services	Slusher, Toby	T
USPS	Stepongzi, Mark	P
Nuclear Regulatory Commission (NRC)	Sulser, David	P

T – Telephone
P – In Person
A – Absent

A.2 Observers

Organization	Name	Present?
NASA	Baldridge, Tim	T
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoD (Contractor, Booz Allen)	Frank, Larry	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
USPTO (Contractor)	Jain, Amit	T
GSA, FPKI MA PM	Jenkins, Cheryl	T
State (Contractor)	Jung, Jimmy	T
FPKIPA (Protiviti)	King, Matt	P

Organization	Name	Present?
DoD	Kruger, Denise	T
FPKI MA (Contractor, Protiviti)	Jarboe, Jeff	P
Entrust	Moore, Gary	P
GSA (Contractor, Unisys)	Petrick, Brant	P
EPA (Contractor, Jacob & Sundstrom)	Simonetti, Dave	T
FPKIPA (Protiviti)	Sonnier, Tiffany	P
CertiPath	Spencer, Judy	P
DOS (Contractor)	Shomo, Larry	T
	Rodriquez, Renee	T
SSA	Hardy, Amy	T
Treasury	Schminky, Jim	T
	Hodge	T

T – Telephone
P – In Person
A – Absent

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 introduced those present, both in person and via teleconference.

Ms. Gallagher discussed the Vision Statement for FIPS 201 that she sent to the FPKI Certificate Policy Working Group on April 11th. She will send it again for those who do not have it. The Vision Statement will be shared with NIST during discussions about FIPS 201-2 and is intended to be forward looking. It recommends that FIPS 201 introduce additional form factors that are interoperable in the PIV System that support technologies such as cloud computing and mobile devices.

Ms. Gallagher also mentioned that the FPKI Security Profile was sent to the CIO Council via the Information, Security & Identity Management Sub Committee (ISIMSC) and no comments were received. Therefore, the profile will be briefed to the ISIMSC as a final document on April 13, 2011.

Discuss / Vote on 8 March 2011 FPKIPA Minutes

Matt King

Mr. Matt King informed the FPKIPA that all changes were made to the March 8, 2011 FPKIPA minutes based on comments received. NRC motioned to approve the minutes, and the motion was seconded by HHS. The minutes were approved by a 15/15 (100%) vote by members present.

Approval Vote for 8, March 2011 FPKIPA Minutes			
Voting members	**Vote (NRC Motion; HHS 2nd)**		
	Yes	**No**	**Abstain**
Department of Defense	√		
Department of Energy	√		
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	√		
USPS	√		
USPTO - ABSENT			
Veterans Administration	√		

FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich

Discussion / Vote to Approve Entrust at PIV-I

Entrust recently completed all mapping and testing requirements and is now ready for the FPKIPA to vote for acceptance as a PIV-I provider. DOJ motioned to approve their application and NRC seconded.

The vote to approve Entrust as a PIV-I provider was approved by a 15/16 (94%) vote by all voting members.

Approval Vote for Entrust at PIV-I			
Voting members	**Vote (DOJ Motion; NRC 2nd)**		
	Yes	**No**	**Abstain**
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Departmentof 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	√		
USPS	√		
USPTO - ABSENT			
Veterans Administration	√		

Common Policy Change Proposal: Device Certificates Validation Clarification – Discussion

The CPWG reviewed the draft change proposal for device certificate clarification at the April 7th CPWG meeting. The proposed changes align the policy language with the Federal Bridge Certification Authority (FBCA). The change proposal is a result of comments received as a result of Mozilla's public discussion process. Mr. Tim Baldridge asked if anyone has coordinated with Mozilla to ensure the language is strong enough before submitting a final proposal to the FPKIPA. Ms. Wendy Brown replied that public discussion is open continually. The change proposal has been sent to the FPKIPA for review and will be finalized at the next CPWG meeting on May 5th (per the new process agreed to at the last FPKIPA meeting). FPKIPA members are encouraged to participate in the discussion. The final change proposal will be presented at the May 10th FPKIPA meeting for a vote.

ACTION: Ms. Wendy Brown will submit proposed language from the Device Certificates Validation Clarification change proposal to the Mozilla public discussion to see if the change would satisfy their concern.

PIV-I Retesting Requirements - Status

During the April 7th 2011 CPWG meeting, PIV-I Issuer re-testing requirements were discussed. The requirements will be circulated to the CPWG for comment and the document will be finalized at the May 5th CPWG meeting. Participation in this discussion is encouraged.

Other Items

The April 19th CPWG meeting is canceled due to a conflict with the NIST FIPS 201-2 workshop and other conferences affecting members. The next CPWG meeting is May 5th. The SHA 256 meeting originally scheduled at the beginning of the April 19th CPWG meeting has been rescheduled for the May 5th CPWG meeting.

Mr. Charles Froehlich reminded everyone that the CPWG will hold a special joint session with the Architecture Working Group (AWG) on the morning of the May 5th CPWG meeting to discuss comments on FIPS 201-2. The comments will be consolidated prior to the meeting, finalized at the meeting and submitted to NIST by June 6th.

FPKI Management Authority (FPKI MA) Report

Cheryl Jenkins

Ms. Cheryl Jenkins noted that Adobe will be adding the Common Policy Root CA certificate to their trust store by the end of April. Microsoft added the Common Policy Root to their trust store March 22, 2011. The FPKIMA is continuing to make progress with Apple and Java. As mentioned previously, participation in the Mozilla discussion is encouraged.

Ms. Jenkins provided an update on the SHA 2 transition project and noted that all certificates have been issued, except for USPS and Illinois. The SHA-256 transition status report will be sent to the FPKIPA after today's meeting.

The discussion that followed included the testing certificate path validation of the new certificates is complicated by still having legacy certificates in the public repositories. It was requested that the FPKIMA send a notice to Affiliates requesting that legacy certificates be removed from public repositories by the end of April, sooner if possible, to assist testing the new certificate paths. This will not be a revocation of those certificates, simply removing them from the repositories for testing. If testing identifies problems, the certificates can then be restored to the repositories until the problems are resolved; revocation would not permit this temporary recovery action.

ACTION: The FPKIMA will resend the request for Affiliates to test and notify the FPKIMA when legacy certificates can be revoked; but, this time will include a request to remove the legacy certificates from public repositories.

Dan Jeffers requested that the FPKIMA ask agencies to supply their Root certificates along with the end-entity certificates the FPKIMA is gathering for testing. Root certificates may not be readily available in repositories but are necessary for those that configure their applications for direct trust.

ACTION: The request to send sample end-entity certificates for testing should also be resent; this time with a request that Root certificates be included.

Ms. Jenkins indicated that the Legacy CAs will run until all agencies transition to the new infrastructure. However, this means that the system will simply run with no maintenance or management. Ms Jenkins informed the FPKIPA that she is not sure how long the Legacy CAs will be allowed to run; she is hoping they will stay up until everyone has transitioned. A decision regarding how long they can continue running is up to the Designated Approving Authority (DAA).

There was debate about removing the legacy certificates out of the repositories and the best way to do so. A decision was made to remove old certificates from the FPKI repository by April 27th. A three phased approach was recommended for revocation.

Phase 1: Ask for volunteers to remove their certificates; Phase 2: remove old certificates from repositories by April 27th; Phase 3: certificates will be revoked at some future date to be decided. Ms. Brown noted that Microsoft and Adobe do not remove expired certificates. Therefore, there will still be a path back to the legacy roots.

ACTION: Any agency that would like their cross certificates removed from the FPKI repository before April 27th will notify the FPKIMA.

ACTION: Ms. Wendy Brown will send a notice to agencies informing them that all legacy certificates will be removed from the FPKI repositories by April 27th and that all legacy cross certificates should be revoked no later than May 25, 2011.

Agenda Item 6

Other Agenda Items

SSPWG Update-Ms. Gallagher (Matt King)

Mr. King provided an update on the SSPWG meeting held on March 15th. The prominent discussion during the meeting was on how to get a clearer picture of the trust paths from the community. Ms. Brown sent a request for end entity certificates to help with testing and discovery on the new infrastructure. Mr. King encouraged everyone to respond to Ms. Brown's request.

ICAM Update - Ms. Gallagher

Ms. Gallagher informed participants that the next chapters of the FICAM Roadmap and other documents from the Architecture Working Group (AWG) will be circulated to the FPKIPA for review.

The next ICAMSC Meeting is April 27, 2011.

The next FPKIPA meeting is May 10, 2011.

Agenda Item 7

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 10:45 a.m. EST.