



**FEDERAL PKI POLICY AUTHORITY**

**July 12, 2011 MEETING MINUTES**

**USPS Headquarters  
475 L'Enfant Plaza, SW  
Conference Room: 4841  
Washington, DC  
9:32 a.m. – 11:45 a.m.**

**Welcome, Opening Remarks & Introductions**

**Deb Gallagher,  
Chair**

**Discuss / Vote on June 14, 2011 FPKIPA Minutes**

**Matt King**

**FPKI Certificate Policy Working Group (CPWG)  
Report**

**Charles Froehlich**

- Change Proposal Updates - Discussion
  - Device Certificate Change Proposals
  - LDAP Change Proposal
  - Validation Certificates for test purposes
- C4CA Survey
- Oracle Discussion

**FPKI Management Authority (FPKI MA) Report**

**Cheryl Jenkins**

**MA Proposed change to SHA-256 Transition Plan**

- **Recommended revocation of non-revocable certificates - Discussion**

**Cheryl Jenkins**

## Other Agenda Items

Deb Gallagher

- *E-Governance Trust Services (EGTS) Overview*
- *ICAM Update*
- *If you cannot attend, please designate an alternate.*
- *Next FPKIPA meeting, August 9, 2011*

## 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)	Breland, MaryAnn	A
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.	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)	Levine, Susan	T
Nuclear Regulatory Commission (NRC)	Sulser, David	A
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Kless, Patricia for Dan Lindsey	T
Veterans Administration (VA)	Jurasas, Eric	T

**b. Observers**

<b>Organization</b>	<b>Name</b>	<b>T – Telephone P – In Person</b>
CertiPath	Spencer, Judy	P
DoD	Kruger, Denise	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
Entrust	Moore, Gary	P
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIMA (Contractor, Protiviti)	Louden, Chris	P
FPKIPA (Contractor, Protiviti)	Sonnier, Tiffany	P
GSA OGP (Contractor, Unisys)	Petrick, Brant	P
GSA, FPKIMA PM	Jenkins, Cheryl	T
NASA	Baldrige, Tim	T
State (Contractor)	Jung, Jimmy	T
USPTO (Contractor)	Jain, Amit	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
DHS	Shomo, Larry	T
FPKIMA (Contractor, Protiviti)	Kotraba, Matt	T
DoD (Contractor, BAH)	Jeffers, Dan	T

## 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 9:32 a.m. EST and introduced those present, both in person and via teleconference.

### Discuss / Vote on June 14, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the June 14, 2011 FPKIPA minutes. DOJ motioned to approve; Postal seconded. The motion was approved unanimously.

Approval Vote for June 14, 2011 FPKIPA Minutes			
Voting members	Vote (DOJ Motion; Postal Second)		
	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) - Absent			
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

## **FPKI Certificate Policy Working Group (CPWG) Report, Matt King**

Mr King informed the FPKIPA that the last CPWG there was discussion about new change proposals, none of which are final but they are in the process of working out the details. The change proposals included:

- **Device Certificate Change Proposals:** Creating policy OIDs that clarifies whether it is a human or device; one change proposal is for Common and one is for Federal Bridge. The CPWG is seeking guidance from NIST on both proposals. Mr. King informed us that this will be discussed again at the next CPWG meeting.
- **LDAP Change Proposal:** Making LDAP optional and HTTP mandatory in certificate profiles and changing the CP requirements from specific protocols to instead supporting repositories for whatever protocols are specified in valid certificates issued by a given CA. The change for Common Policy is dependent on a similar change in FIPS 201-2, which has been requested.
- **Validation Certificates for test purposes** This is a proposal to standardize practices many affiliates already implement. The purpose is to be able to issue temporary short lived certificates to validate that a change made in production is working before beginning to issue additional production certificates. Additional research is needed to ensure this proposal does not violate FIPS 201.

### C4CA survey-

During the last FPKIPA meeting, the question was raised if the C4CA was still necessary. This question was sent as a survey and Mr. King received a response from seven agencies who all said no. Health and Human Services (HHS) is still verifying if they need it. Mr King reminded meeting participants that if they have not yet responded, to please respond as soon as possible. Mr. King suggested that there be a discussion of how to proceed once all responses are in. Mr. Chris Loudon added that if there is consensus that the C4CA is not needed then the FPKIMA will need to take action to remove it. Ms. Deb Gallagher requested for Mr. King to formalize a list of what needs to happen if the C4CA is needed and if the C4CA is not needed. Mr. Toby Slusher stated HHS will not have a final position until the end of next month possibly by the first CPWG in August. Mr. King suggested setting that as a deadline: August 4, 2011. FPKIPA members were reminded that if any agency has a need for the C4CA, they should provide business use cases to illustrate that need.

### Oracle discussion-

There will be a discussion regarding Oracle at the next SHA 256 working group meeting on July 19, 2011. Mr. King reminded those who have issues with Oracle to submit those issues to him by next week.

### **ACTION:**

1. Mr King placed a deadline for C4CA responses for the first August CPWG for all agencies to provide their position on the necessity of the C4CA.

## **FPKI Management Authority (FPKIMA) Report, Cheryl Jenkins**

Ms. Wendy Brown and Mr. Jeff Jarboe presented a PowerPoint report which Mr. King mailed to members of the FPKIPA. The report included:

- A. Update on Common Policy root certificate in vendor trust stores:**
  - a. Opera is requesting information regarding the FPKIMA and additional input from the embassy.
  - b. Ms. Cheryl Jenkins asked if it is important for the vendors to have Opera because it is taking a lot of the FPKIMA's resources to continue its pursuit. She added, if it is necessary the MA will continue but if not the MA will not continue the application with Opera.
  - c. Ms. Judy Spencer mentioned that Dave Cooper wanted to include them initially.
  - d. Mr. Gary Moore stated that Opera is among the top 5 browsers; Mr. Tim Baldrige recommended pursuit continue because of this browser status and because they are international.
  - e. Ms. Jenkins said they will continue pursuit because of the feedback from today's meeting.
  - f. There was also a discussion about Chrome and their trust store. It was brought to the participants' awareness that Chrome has overtaken IE and is in the top 2 for browsers. Due to this fact, the FPKIPA requested the MA apply for the Common Policy root certificate to be distributed in the trust store for Chrome. The FPKIMA had not started the application with Chrome, because they believed Chrome makes use of the CAPI store and does not distribute its own trust store. Gary Moore stated Chrome does have its own trust store for non-windows platforms. Cheryl Jenkins said the FPKIMA would add Chrome to the list of vendors to be pursued.
- B. New infrastructure-Complete**
  - a. The Compliance Audit for Legacy is nearly complete
    - i. The next step is to get a letter to the Policy Authority for approval.
- C. TWG meeting update.**
  - a. The TWG was held June 16, 2011; Consensus was reached on making LDAP optional and HTTP mandatory. See description of LDAP change proposal presented to the CPWG.
- D. Microsoft requirement for a Time Stamp Authority (TSA) service for any CA in their trust store that includes code signing.**
  - a. A representative from Microsoft was at the last TWG and answered questions from the TWG about the Microsoft requirement and how Microsoft products validate signature on code. The TWG object to the requirement to have a TSA but not require its use, and proposed a more efficient method for validating the signature on code after the code signing

certificate has expired. Mr. Gary Moore and Mr. Santosh Chokhani volunteered to draft a paper on this position to be sent to Microsoft. Also addressed is the behavior of a Microsoft client when you don't have EKUs in the certificates. Microsoft processing requires revoked certificates to be kept on a CRL after their expiry date in order to verify whether the certificate was valid at the time of its use. Mr. Chris Loudon recommended that if participants do code signing, to have this on their radar. Mr. Gary Moore mentioned they highlighted these issues and how to address them. Mr. Moore's suggestion is to create a package with the time stamp which has everything you need to validate the signature and include that with the signed code if needed. Mr. Loudon suggests keeping two issues in mind: 1-Technical issues are being discussed at the TWG and 2-Policy Impact- Microsoft is requiring a CA to stand up a time stamp authority if the root certificate for that CA is included in the Microsoft trust store with the EKU indicating it supports code signing. Mr. Loudon requested members to send someone to the next TWG for this discussion if they will do code signing at all, even if they do not currently support code signing but may in the future. Mr. Moore added that the question is can a Federal TSA Provider be used for this or will a commercial provider be required. Ms. Deb Gallagher offered that this should be a CPWG agenda item for an in-depth discussion. Mr. Loudon reminded that this is an ongoing discussion in the TWG.

- b. Currently the Common Policy root certificate is included in the Microsoft trust store with the EKU for code signing. Their requirement for a TSA begins in October and we need a definitive answer if Microsoft will remove the code signing EKU at that time. Ms. Gallagher asked that once the TWG completes the discussion on this issue, the paper be presented to the CPWG for discussion of the policy impacts.

**E. New listserv mail list replacing FPKIPA\_FBCA\_TWG@listserv.gsa.gov**

- a. LISTSERV is now [FPKI-ttips@listserv.gsa.gov](mailto:FPKI-ttips@listserv.gsa.gov) – notify Mr. Matt Kotraba if you want to be included on this new list.
- b. Mr. Gary Moore asked if affiliates can get a notification when additions and deletions occur in the repositories. Ms. Wendy Brown answered that the FPKIMA currently maintains a list of who to notify for each affiliate about changes in the trust infrastructure. This contact information for each affiliate is preferably a mailing list maintained by that affiliate, so the FPKIMA does not need to know when each affiliate has internal turnover.

**F. Community Interoperability Test Environment (CITE)**

- a. A consensus regarding CITE was reached which is a production-like test environment, where the MA manages a test infrastructure. This test

environment is used to test CAs during the application phase and can be used to test versions of affiliate PKIs as they will be in production. The MA would like affiliates to keep their test infrastructure online and to use ongoing. The MA strongly encourages participation in CITE, but participation is voluntary. They are currently looking for online scheduling capabilities so that affiliates can schedule their own testing. The CITE document should be available later this week.

- b. The listserv for CITE is [FPKI-CITE@listserv.gsa.gov](mailto:FPKI-CITE@listserv.gsa.gov)
  - c. Ms. Jenkins stated that this is a major accomplishment that they have been trying to get consensus since 2004.
  - d. CITE has already been used for the technical interoperability testing, SHA 256, and supporting the PIV-I card testing
  - e. Mr. Charles Froehlich asked if participants in CITE would be expected to stand-up a duplicate version of their entire infrastructure, namely the Root CA, subordinate CAs, OCSPs, repositories, etc. Ms. Wendy Brown stated that only the repository was required to be up and available for others to test against; but also pointed out that all mechanisms specified in production certificates to support revocation information should be supported in the CITE environment in order to make it most closely represent the production environment.
- G.** It was mentioned that Mr. Gary Moore's PKI issue is currently in the TWG agenda.
- H.** Chain validation
- a. Microsoft CAPI-The MA will reach out to the CPWG and TWG for issues regarding Microsoft CAPI path validation. Mr. Loudon mentioned that Microsoft's bugs are significant and may need to be discussed at an upcoming FPKIPA meeting.

**ACTION:**

1. Ms. Brown will send the MA report to the PA after changing the TWG date.
2. Ms. Cheryl Jenkins said the FPKIMA will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011.

**MA Proposed change to SHA-256 Transition Plan**

The FPKIMA is seeking approval/direction for stakeholders of the current decommission plan. Last year it was decided that the legacy Common Policy CA should issue cross certificates to the new Common Policy CA and the SHA1 FRCA to facilitate path validation for those who had not yet added the new Common Policy CA as a trust anchor. These two cross certificates would not be revoked prior to the legacy Common Policy CA being shut down, therefore these two cross-certificates would be non-

revocable when the final CRL was issued. However, the decommission was delayed so the FPKIMA wanted to know if agencies felt enough time had passed that these two cross-certificates were no longer required to be left as non-revocable. The CPWG had the discussion and the issue that Apple had not yet started distributing the new Common Policy CA root certificate in the trust store for MAC platforms requires the certificates from the legacy to the new trust infrastructure remain in order to not disenfranchise Apple users. Mr. Tim Baldrige stated that many of the desktops from agencies don't get online updates. If current clients don't receive the online update they will not receive the new path. He also stated that end users often do not have an option to install the new trust infrastructure. Mr. Chris Loudon added that the actual question should be is there anyone who wants to argue for revoking them? If so, another 30 day CRL may need to be issued if the FPKIPA needs to vote on this at the August PA meeting. Otherwise, the current plan is to issue a permanent CRL before the current 30-day CRL expires at the end of July. Ms. Debbie Mitchell asked if there is not negative impact to them staying then why revoke. Mr. Loudon answered that most people don't feel comfortable with un-revocable certificates. He added if there is a compromise you need to remove the roots from the trust store. Mr. Dan Jeffers from DoD asked for an advanced notice if they get revoked.

Ms. Gallagher requested a statement from the FPKIMA that gives the pros and cons so everyone understands and can vote next month. Therefore another 30 day certificate may be needed. Ms. Jenkins stated that if the original decommission plan was still in effect then the certificates can be shut down in July. The FPKIMA has direction to follow the original plan. Ms. Gallagher added that if any agency has an objection to the original plan to submit the objection to her in writing and copy Matt King within one week (next Tuesday, July 19). The FPKIMA is not asking for suggestions on how to do it, but asking if the current plan should stand. Ms. Gallagher will make a decision about how to continue if objections to the current plan are raised and will determine if a vote is required.

**ACTION:**

1. 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.

**Other Agenda Items-E-Governance Trust Services (EGTS) Overview**

Mr. Loudon gave background on the E-Governance Certification Authorities (EGCA). The EGCA's were originally stood up for the E-Authentication initiative. ICAM is moving forward with an effort to establish the E-Governance Trust Services (EGTS) needed to support the ICAM's evolving Identity Management activities:

- a. Back end attribute exchange
- b. Identity providers
- c. Relying party applications
- d. Trusted Metadata
- e. Legacy E-Auth Program

The recent development is to support Backend Attribute Exchange (BAE) and adding policy OIDs for different levels of assurance. There is no relation to the Common Policy CA currently but could be in the future. Mr. Louden informed participants that the new specifications for BAE and Metadata are being developed by the AWG. New EGCA certificate policies were defined as well as new certificate profiles. No objections to this plan were raised and the EGTS progress will continue.

**ACTION:**

1. Mr. Matt King will send the EGTS briefing to the group.

**ICAM Update**

Ms. Deb Gallagher was pleased to see some members of the FPKIPA at the last ICAM Subcommittee (ICAMSC) meeting. The ICAMSC is being tasked with working with other communities. They also did a gap analysis between the CNSS and the FICAM to see where there are gaps and develop a report. Buy-in and support has come from intelligence CNSS, PNSC-DNI, and several other groups. This group is being enlarged from the National Security Staff of the White House. Ms. Gallagher reminded that it is important that everyone have representatives at the ICAMSC to stay abreast of what is going on. Ms. Gallagher stated that the e-Signature Guidance which will be released as a final document soon.

**ACTION:**

1. Ms. Gallagher will publish the e-Signature Guidance once a final review is complete; will be published on the IDManagement.gov website as well.

The next ICAMSC meeting is July 27, 2011.

The next FPKIPA meeting is Aug 9, 2011.

**Adjourn Meeting**

Ms. Gallagher adjourned the FPKIPA meeting at 11:45 EST.

### FPKIPA Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
316	Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.		13 Nov 2007	26 Nov 2007	Open
366	Debbie Mitchell will share the finalized DoD Test Plan; the FPKIPA will then review it and decide what pieces they can and cannot do. Then Ms. Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Ms. Jenkins	13 May 2008	10 Jun 2008	Open
375	The FPKIPA Chair will take the enduring proxy and meeting schedule issues under advisement and will notify non-attendees that they risk losing their voting privileges if they persist in unexplained absences and do not designate a proxy when they cannot attend.		14 Oct 2008	12 Nov 2008	Open
378	Ms. Jenkins will send out guidance to the agencies on how to use the various root stores.	Ms. Jenkins	9 Jun 2009	14 Jul 2009	Open

No.	Action Statement	POC	Start Date	Target Date	Status
379	Ms. Jenkins will provide a milestone and timeline sheet for the redesign effort. This will be provided as a dashboard on a monthly basis to the FPKIPA.	Ms. Jenkins	9 Jun 2009	14 July 2009 and monthly afterwards	Ongoing
381	Judith Spencer will check with NIST for additional guidance on device certificates.		9 Jun 2009	18 Jun 2009	Open
382	Judy Spencer will send the Discussion Paper: "SSL Inspection and Mutual TLS Issue" to ICAMSC with today's date as an information paper, not a recommendation from the FPKIPA.		10 Nov 2009	16 Nov 2009	Open
383	The Secretariat will add a reference to the Discussion Paper: "SSL Inspection and Mutual TLS Issue," in the FY2010 Accomplishments paper.		10 Nov 2009	Oct 2010	Open
384	Ms. Brown is to draft an email memo for the ICAMSC re the Mozilla root store request and send to Brant Petrick for distribution to the ICAMSC.	Ms. Brown	10 Nov 2009	16 Nov 2009	Open
385	We need to write a Change Proposal, adding a cardAuth policy to FBCA. FBCA will require a UUID, as opposed to being optional.		10 Nov 2009	30 Nov 2009	Obsolete by PIV-I
386	Mr. Jim Schminky will provide the FPKIMA with a report of availability from a	Jim Schminky	10 Nov 2009	30 Nov 2009	Obsolete

No.	Action Statement	POC	Start Date	Target Date	Status
	customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.				
388	Ms. Jenkins will reach out to Marianne Swanson (and Ron Ross) of NIST to determine what their audit standards strategy is vis-à-vis aligning the FBCA and NIST SP 800-53 with ISO standards.	Ms. Jenkins	9 Mar 2010	13 Apr 2010	Open
393	Patricia Kless will discuss USPTO's desire to Move to Common with Dan Lindsey and respond to the FPKIPA	Dan Lindsey	10 Aug 2010	14 Sep 2010	Closed – by default they stayed with FBCA since they did not request a move
394	DOE will indicate their desire about whether to cross certify with the FBCA or Common	Mary Ann Breland	10 Aug 2010	14 Sep 2010	Open
396	Ms. Spencer agreed to send additional clarification about requirements surrounding SHA-256 that appear in NIST SP 800-78, 800-131, and other related Special Publications		10 Aug 2010	14 Sep 2010	Closed
398	Ms. Brown will send an email notifying interested parties that she will accept and respond to requests for test CA certificates with either SHA-1 or SHA-256 for testing	Ms. Brown	10 Aug 2010	14 Sep 2010	Ongoing

No.	Action Statement	POC	Start Date	Target Date	Status
401	Ms. Jenkins will draft SOP for the PA regarding how to enforce corrections for problems in the FPKI repositories and then forward a draft to CPWG	Ms. Jenkins	14 Sep 2010	12 -Oct 2010	Open
403	CPWG will draft a memo about Trusted Internet Connection (TIC) and PKIs	CPWG	14 Sep 2010	12 Oct 2010	Open
404	Matt King will write a SHA-256 FAQ and distribute it on or about 1 December	Matt King	9 Nov 2010	1 Dec 2010	Closed
406	Ms. Jenkins will provide guidance on how to transition to the new SHA-256 FPKI	Ms. Jenkins	9 Nov 2010	1 Dec 2010	Closed
407	CPWG to discuss what changes require retesting of a PIV-I Issuer (e.g., Is retesting required if new CMS is used or other major changes are implemented?).	Matt King	14 Dec 2010	18 Jan 2011	Open
408	Once Verizon Business PIV-I testing is complete, an email vote will be held to approve Verizon Business at PIV-I	Matt King	14 Dec 2010	18 Jan 2011	Closed
409	Matt King will add an agenda item to a future CPWG meeting related to processes for enforcing compliance with change proposals approved by the FPKIPA.	Matt King	20 Jan 2011	28 Jan 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
410	Mr. Toby Slusher agreed to send the HHS briefing on the Federal Issuers of PIV-I Cards to the FPKIPA List	Toby Slusher	20 Jan 2011	28 Feb 2011	Open
411	Mr. Matt King agreed to send the new change proposal, "CMS Requirements Clarification," for an E-Vote after the change proposal is approved by the CPWG (expected by 15 or 16 February).	Matt King	8 Feb 2011	16 Feb 2011	Closed
412	Mr. Brant Petrick will post OMB Memo 11-11 to the IDManagement.gov web site	Brant Petrick	8 Feb 2011	16 Feb 2011	Closed
413	Mr. King will update the SHA-256 Transition Lessons Learned document at the 15 February 2011 CPWG meeting and distribute the revised document to the SHA-256 Working Group and FPKIPA mail lists	Matt King	8 Feb 2011	28 Feb 2011	Open
414	Ms. Ms. Jenkins will redistribute the TAG Paper on ECC to the FPKIPA Mail List	Ms. Jenkins	8 Feb 2011	28 Feb 2011	Open
415	Ms. Gallagher will develop a plan for change management within the FPKI Community and notify the FPKIPA on how it will proceed to address change management issues such as algorithm transitions	Deb Gallagher	8 Feb 2011	31 Mar 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
416	Ms. Brown will distribute the information about how to participate in the public discussion for Mozilla to the FPKIPA	Wendy Brown	8 March 2011	15 March 2011	Closed
417	Ms. Cheryl Jenkins is scheduled to meet with the GSA DAA to request permission to keep the Legacy CAs alive past the March 31, 2011 deadline. Ms. Jenkins will notify the community of the decision.	Cheryl Jenkins	8 March 2011	15 March 2011	Closed
418	The FPKIMA will brief the IAB about the AIA Crawler at the March 23, 2011 IAB meeting.	Cheryl Jenkins	8 March 2011	23 March 2011	Closed
419	Mr. Jim Schminky will draft a change proposal to generate a live test card in a production environment. After generating the change proposal, FIPS 201 may need to be updated.	Jim Schminky	April 12, 2011	May 10, 2011	Open
420	Mr. Matt King will submit a request for comments to be received by next CPWG meeting on May 5 <sup>th</sup> .	Matt King	April 12, 2011	May 5, 2011	Closed
421	Mr. King will distribute the document as- is and add comments, implementation and enforcement to the next agenda.	Matt King	April 12, 2011	May 10, 2011	Closed
422	Mr. King will circulate proposed change proposal to the Policy Authority (PA) for review with the comment that members of the PA are encourage to attend May 5ths CPWG meeting if there are any	Matt King	April 12, 2011	May 5, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	concerns and they will be discussed during the meeting.				
423	If no concerns the change proposal will be presented for vote at the May 10 <sup>th</sup> PA meeting.	Matt King	April 12, 2011	May 10, 2011	Open
424	DOE will put what they heard in document form and send to the CPWG for confirmation, and will then re-submit their application based on the advice given	Mary Ann Breland	April 12, 2011	May 10, 2011	Open
425	Mr. King will coordinate with Mr. Baldrige and Mr. Dave Silver to request comments on FIPS 201-2 from both the AWG and CPWG, and to invite the AWG to the CPWG on the morning of 5 May to discuss FIPS 201-2 comments	Matt King, Tim Baldrige	April 12, 2011	May 5, 2011	Closed
426	Ms. Deb Gallagher will send comments regarding FIPS 201-2 that are gathered at the May 5 <sup>th</sup> joint CPWG/AWG meeting to ICAMSC	Deb Gallagher	April 12, 2011	June 2, 2011	Open
427	Mr. King will cancel the April 19 CPWG meeting, and move the SHA-256 meeting to May 5th	Matt King	April 12, 2011	April 19, 2011	Closed
428	After the joint CPWG/AWG meeting, the FIPS 201-2 document will be submitted to FPKIPA on the 10 <sup>th</sup> of May.	Matt King	April 12, 2011	May 10, 2011	Open
429	Mr. Matt King will ask ORC the following: <ul style="list-style-type: none"> <li>• Can they provide a detailed diagram that shows the entire ORC architecture</li> </ul>	Matt King	April 12, 2011	May 10, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	<p>including ECA and SSP CAs</p> <ul style="list-style-type: none"> <li>• Where do ACEs OIDs flow into the ORC CA or do they?</li> <li>• Can they assert that e-Validate meets the independence requirements in the CP due to the detailed level of involvement of Brian Dilley in the CP modifications specified at the 15 March CPWG meeting?</li> <li>• Can they provide Mr. King with a copy of their Audit Letter?</li> </ul>				
430	Wendy Brown will continue interoperability testing.	Wendy Brown	April 12, 2011	June 2, 2011	Open
431	Matt King will request an Operational Review and Audit Letter from DigiCert	Matt King	April 12, 2011	May 10, 2011	Open
432	Matt King will work with Deb Gallagher to draft a memo that explains how Government-operated PKIs are required to follow the FPKI Security Profile by the new FISMA reporting metrics	Matt King	May 10, 2011	June 2, 2011	Open
433	Matt King will place a deadline for C4CA responses for the first August CPWG	Matt King	July 12, 2011	August 8 2011	Open
434	Ms. Brown will send the MA report to the PA after changing the TWG date.	Wendy Brown	July 12, 2011	July 19, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
435	Ms Cheryl Jenkins, Ms. Brown and Ms. Gallagher will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011	Ms. Jenkins, Ms. Gallagher	July 12, 2011	September 15, 2011	Open
436	Ms. Gallagher will send an email with the request for an in-writing 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 Metadata briefing to the FPKIPA group	Matt King	July 12, 2011	August 9, 2011	Open
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