



**Minutes of the 9 March 2010 Meeting**  
**USPS, 475 L'Enfant Plaza, SW, Washington, DC.**  
**CR 2P316 (inside CR 2P310)**  
**9:35 a.m. – 11:44 a.m.**

**A. AGENDA**

- 1. Welcome / Introductions**
- 2. Discuss/Vote on 12 January 2010 FPKIPA Minutes**
- 3. Welcome to New Voting Member, Eric Jurasas of the VA**
- 4. ICAM Update**
  - 1. Trust Framework Providers (Kantara and OIX)**
  - 2. National Strategy for Secure on-line Transactions**
  - 3. PKI in the Cloud**
  - 4. Scott Rea Request for Links to Federal Agency CPs**
  - 5. DoD ECA Request to cross-certify ORC at Medium Hardware**
- 5. Discuss the Triennial Compliance Audit Requirements**
- 6. FPKI Management Authority (FPKI MA) Report**
- 7. FPKI Certificate Policy Working Group (CPWG) Report**
  - *Discuss: CertiPath Annual Audit Report*
  - *Review/Vote on Common CP Change Proposal: UUIDs in Card Authentication Certificates (with new Practice Note)*
- 8. Adjourn Meeting**

**B. ATTENDANCE LIST**

**VOTING MEMBERS**

The meeting began with a quorum of 12/15 (or 80%) where a two-thirds majority was required. Two other voting members joined after the quorum was established, before any votes were taken, thus bringing the quorum to 93.4%.

We redacted contact information in the published FPKIPA minutes at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members only at some point in the future. FPKIPA minutes already posted on the website were redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at [Judith.Fincher@pgs.protiviti.com](mailto:Judith.Fincher@pgs.protiviti.com).

<b>Organization</b>	<b>Name</b>	<b>Telephone</b>
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference

Organization	Name	Telephone
Department of Homeland Security	Miller, Tanyette	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission ( NRC)	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Lindsey, Dan	
Veterans Administration (VA)	Jurasas, Eric	

**OBSERVERS**

Organization	Name	Telephone
Treasury PKI PMO	Bracy, Gayle	Teleconference
Treasury (Intern to Jim Schminky)	Dy, Albert	
FPKI MA/PM	Jenkins, Cheryl	
State of Illinois	Anderson, Mark	Teleconference
FBI (Contractor, KEANE Federal Systems)	Palma, Lisa	
IdenTrust (Vendor)	Schambach, Marco	Teleconference
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoD (Contractor, ManTech)	Froehlich, Charles	Teleconference
ICAM Senior Policy Analyst (Consultant, A&N)	Schlecht, R.J.	
FPKIPA (Contractor, PGS)	Fincher, Judy	
FPKIPA (Contractor, PGS)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
DOE (Contractor, M Squared Strategies, Inc.)	Olson, Evan	
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
EValid8 (Contractor)	Dilley, Brian	
GPO (Contractor, Ernst & Young)	Iijima, Timothy	
SSA (Contractor, Jacob & Sundstrom)	Jackmon, Kenya	Teleconference

**C. MEETING ACTIVITY**

**Agenda Item 1**

**Welcome / Introductions—Judith Spencer, Chair**

The FPKIPA met at the USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC, CR 2P316 (inside CR 2P310). Judith Spencer, Chair, called the meeting to order at 9:35 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of USPS for hosting this meeting. Ms. Spencer also

welcomed Eric Jurasas (Veterans Administration) as the 15<sup>th</sup> voting member of the FPKIPA.

**Agenda Item 2**

**Discuss/Vote on 12 January 2010 FPKIPA Minutes—Judy Fincher**

Ms. Fincher said all comments were incorporated into the revised Minutes and Ms. Spencer called for a vote to approve the minutes, as edited. The motion passed by 13/15 or 86.7% where a 50% majority vote was required. The VA abstained and the DEA CSOS was absent for this meeting.

Vote to approve 12 January 2010 FPKIPA Minutes			
	Vote (Motion- Treasury 2 <sup>nd</sup> - USPS)		
	Yes	No	Abstain
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration			√

**Agenda Item 3**

**Welcome to New Voting Member, Eric Jurasas, VA—Judith Spencer**

Ms. Spencer welcomed Eric Jurasas of the Veterans' Administration as the fifteenth voting member of the FPKIPA and invited him to introduce himself and describe the VA PKI program. Mr. Jurasas said he was pleased that the VA is now a member of the FPKIPA. He welcomed the challenge of reconciling the VA PKI program with overarching FPKI and PIV policy.

## Agenda Item 4

### ICAM Update—Judith Spencer

#### 1-Trust Framework Providers

Ms. Spencer said that the Federal Government had approved the first two trust framework providers at E-Auth levels 1-3 (non-PKI).

- a) The first two Trust Framework Assessors, Kantara and the Open Identity Exchange (OIX), were given provisional approval as Trust Frameworks at the end of February. Approval is provisional pending adoption of additional guidance for assessors from the Federal CIO Council's Privacy Committee, which is in development.
- b) Kantara is a rebranding of Liberty Alliance. It was provisionally approved at E-Auth Levels 1, 2, and non-crypto level 3. See the Kantara website at <http://kantarainitiative.org/>
- c) OIX was established by the OpenID Foundation and the Information Card Foundation. The purpose of this a non-profit organization to oversee the exchange of online identity credentials on public and private sector Web sites. OIX has been provisionally approved at E-Auth Level 1. See the OIX website at <http://openidentityexchange.org/>

OIX and Kantara will serve as Trust Framework Providers utilizing the criteria set forth in the Trust Framework Provider Approval Process document. Each will implement a certification program that allows organizations and individuals to exchange digital credentials and to trust the identity, security, and privacy assertions associated with those credentials at the stated level of assurance.

Ms. Spencer said that we have developed Federal profiles for both OpenID 2.0 and IMI 1.0 (InfoCard). The SAML 2.0 eGovernment profile has been released for comment.

#### 2- National Strategy for Secure on-line Transactions

Ms. Spencer said she is also involved in developing a national strategy for secure on-line transactions. The draft document will be available at the end of April 2010 for all Federal agencies. This initiative will create guiding principles and a roadmap. It is extending ICAM out to the next level: Business to Business, Business to Consumers. We still have stovepipes in the identity management space, she said. We all have multiple user IDs for our various accounts. We need a higher level of trust for a consumer trust framework. There is a growing trust framework where the Federal Government may or may not be first party to the transaction. This is not just about PKI. One federal PKI cannot accommodate 240 million Americans. There are different levels of need, requiring additional technologies. We need to find a model that will incentivize the industry to move forward. We are hoping this will get signed out by the White House. We already have industry input.

#### 3- PKI in the Cloud

Judy Spencer visited a vendor with a solution known as Application White Listing at the RSA conference earlier this month. This solution addresses the problem of enabling end users to know with veracity that they are at a legitimate web site and not that of an imposter. This solution is also associated with the concept of "PKI in the cloud". PGS stopped by the booth and received demo software to test in the lab.

#### **4) Scott Rea Request for Links to Federal Agency CPs**

Scott Rea, the Dartmouth representative to the Higher Education Bridge CA (HEBCA), has an automated policy mapping tool and is requesting we make federal agency CPs available in an automated, centralized manner to him to facilitate testing the mapping tool.

This could be accomplished by referencing URL links to their CPs via an extension in their profiles, via a meta-directory, or as an addition to the distinguished names list. Ms. Spencer said she also had urged Mr. Rea to approach each agency individually.

The FPKIPA discussed at length the feasibility and desirability of providing such a link from the FPKIPA web site to agency CPs. Some members felt strongly that redacted CPs should be available to all Relying Parties. Others felt this weakened the trust fabric by providing too much information to external parties. In the end, it was decided to refer this issue to the CPWG. Mr. Schminky wanted the CPWG to explore whether we want this and also tell us what a meta-dictionary with links would look like.

Ms. Spencer said Scott Rea is giving us an update of the latest version of his automated policy mapping tool at the March 16, 2010 CPWG meeting and encouraged interested members to participate in that meeting. Contact Judith.fischer@pgs.protiviti.com or at 703-795-8946 (cell) to receive the meeting notice and directions to the Linthicum, MD facility where the meeting is being held.

#### **5) DoD ECA Request to cross-certify ORC at Medium Hardware (Debbie Mitchell)**

Debbie Mitchell assumed that since the item was not on the agenda, it was not going to be discussed at the 9 March 2010 PA meeting. Therefore, she had not invited the DoD ECA program representatives to the meeting and was not fully prepared to discuss it today.

DoD wants ORC to be able to issue PIV-I cards like other SSPs are doing with their NFI "clone" offerings. ORC asked for inclusion via the DoD ECA. This request was countersigned by Trish Janssen of the DoD, as their sponsor.

#### **Background**

Ms. Spencer said we have been doing work with states and external communities such as FRAC, ACIS, TWIC and also, industry. The Feds have PIV cards and these mixed federal/state/local groups, as well as industry, want cards that are interoperable with us. The PIV-Interoperability requirements document was issued in May 2009, as "Personal Identity Verification Interoperability for

Non-Federal Issuers.” The requirement for PIV interoperability is that you include “an Authentication PKI Certificate issued by a Certification Authority (CA) that chains to the Federal Bridge Certification Authority (FBCA) at the Medium Hardware assurance level via cross-certification.” (Section 2.4.1)

As a result, three large vendors have been cross-certified at Medium Hardware: 1) Entrust, 2) VeriSign, 3) Verizon Business.

Ms. Spencer recommended that we reject the application because the DoD ECA is one-way cross-certified. There is no reciprocal trust with the FBCA. States would want two-way trust. We can trust the DoD ECA entities, but they don't trust us in the opposite direction. They are not full participants in the trust framework we have created for the FPKI. In order for ORC to be cross-certified in a manner that would enable it to chain to the FBCA at Medium Hardware, the DoD ECA would have to be two-way cross-certified with FBCA.

Debbie Mitchell: Where is it written that you have to be two-way cross-certified to qualify as a NFI “Clone”? Debbie Mitchell said she would put this out to the DoD ECA Program Manager.

Ms. Spencer said she told ACES the same thing. Would ORC or ACES qualify as currently written? NFI “clones” would because they are well aligned with new PIV-I policy and Common. She said she was also leery of anyone joining at this point until the PIV-I specification is issued and the change proposals are processed. A PIV-I OID would have to be asserted by all NFI “clones”, as well as the DoD ECA, should it become two-way cross-certified.

Jim Schminky recommended we shelve this issue until the DoD can bring in their representative to discuss it. We do not want anyone to start issuing PIV-I certs until the change proposals to the FBCA CP are approved, he said.

Ms. Spencer said the DHS “Spring Forward” exercise with the states commences Friday, March 12, 2010. She is encouraging them not to slow down. They can count on the NFI “clones” to be PIV-Interoperable due to their CPs being based on the SSP use of the Common Policy CP.

Furthermore, some things are being added to PIV-I that will impose additional requirements on NFI “clones”. They will have to meet the requirements for the PIV-I OIDs. NFI's are much closer than the DoD ECA Certificate Policy is. You will probably have to change the DoD ECA policy because it doesn't meet the Common Policy. My main objection is it's one-way trust, she said.

Jim Schminky encouraged Ms. Mitchell to cross certify the DoD ECA in both directions. I cannot imagine that the original rationale for a one-way cross-certification still holds water.

Debbie Mitchell: I will send it back to the DoD ECA Program Office for consideration.

## Agenda Item 5

### Discuss the Triennial Compliance Audit Requirements—Jim Schminky

Jim Schminky (Treasury), chair of the Audit Working Group that developed the proposed Triennial Compliance Audit methodology, displayed the Audit Requirements document and walked the FPKIPA members through the three sets of comments—from DoS, GPO, and CertiPath. He explained his response to each comment.

The new approach is a shift away from a one-time look at everything to a model of continuous monitoring, he said. He explained the methodology in some detail for those who had not been briefed previously. (For more detail, refer to the 12 January 2010 FPKIPA Minutes, published on the FPKIPA web site.)

- (1) The Audit Working Group (AWG) identified 50 core elements or requirements that would be reviewed each year. The core group represents approximately ¼ of all “Shall” statements in the RFC.
- (2) The first year in the cycle would be a full audit. The first year following the full audit would be a subset of RFC, representing roughly one third of the non-core controls, including a review of previous findings and any changes made during the year. Hence,  
Year 1 = core elements, plus sections 1, 4, 7, 9 (plus previous findings, changes)  
Year 2 = core elements, plus sections 2, 3, 5, 8 (plus previous findings, changes)  
Year 3 = core elements, plus section 6 (plus previous findings, changes).
- (3) Brian Dilley elaborated on a comment from the GPO/IG regarding how this new methodology aligns with WebTrust (the audit methodology used by the GPO). Mr. Dilley said that ISO 21188, the international PKI standard, would align well with the Triennial Audit approach. WebTrust, as written today, would not.

Mark McCloy said that current budgetary considerations drove their view of the Triennial audit. We need flexibility in scheduling and budgeting, he said.

Jim Schminky responded that the Triennial audit methodology removes “delta” audits and management assertions, thereby adding to the costs some agencies will incur. He argued for consistency across the agencies, which would lead to greater trust in the model. The current process is not secure. We are raising the bar across the board. We hope it is less expensive in the aggregate. That is a hope, not a guarantee. We need to make sure the trust model is unquestioned. Currently, that is not the case. There are wide variations in what gets audited by which agency on any given time.

Mark McCloy: we want to maintain the “delta” option. Its elimination is a cost driver.

Jim Schminky: We will not be able to determine the amount or if there are any savings until after the first three-year cycle. The rationale for adopting this new model is to improve the trust model represented by the Federal PKI.

Mr. Schminky asked for an up/down vote at the 13 April 2010 FPKIPA meeting.

## **Agenda Item 6**

### **FPKI Management Authority (FPKI MA) Report--Cheryl Jenkins**

#### **Funding for the Re-Design and Stipulations**

Ms. Jenkins stated that the OMB approved \$3.3 Million in funding to complete the FPKIA re-design, with the following stipulations.

- 1) The targeted architecture had to be deployed by 30 September 2010.
- 2) P1 and P2 (the primary and secondary sites) had to be moved because we lost our space.
- 3) OMB requested we provide monthly status on our progress.

Both P1 and P2 are now housed in leased facilities; and, we have identified three of the six sites for the targeted architecture. These are tier 2 & 3 data centers. These may be housed in GSA data centers. We will negotiate a no-cost lease if we use GSA space.

This was an aggressive schedule. We had to move the current architecture (P1 and P2) to better facilities with adequate power, heat and cooling, and extra bandwidth to support growing network traffic. We have lease agreements in place in both facilities.

Cheryl Jenkins: The target architecture will be in the DC metro area. We will not have remote CA administration in place by 9/30/2010, due to time constraints. That will happen later.

Judy Spencer told OMB their deadline put us in bad position. Some cleanup work will continue past 2010, into 2011.

#### **Annual Compliance Audit**

Cheryl Jenkins: Another impact was on the required annual compliance audit. The contract vehicle was not in place to conduct the C&A and annual compliance audit in synch with the new aggressive re-design schedule. We briefed GSA and they gave us an extension of the C&A to 9/30/2010. The C&A would be on the targeted architecture, as would a Day Zero compliance audit.

Cheryl Jenkins: We are now requesting that the FPKIPA does the same. Instead of an annual compliance audit on the existing architecture, there would only be a Day Zero audit on the targeted architecture.

Several members of the FPKIPA took exception to this request.

Jim Schminky: An audit is a look backward. It should be conducted on the previous year- not on a nascent architecture.

Judy Spencer said that the FBCA policy requires an annual compliance audit. You need to do a compliance audit on 2009, coupled with a Day Zero audit on 9/30/2010. An audit is not the same as a C&A.

Judy Spencer: We do not have a current audit on our current PKI. Every agency gets cited because they don't have our audit results in their audit reports.

Brian Dilley: You have to follow what your policy says.

Judy Spencer tabled the issue of the compliance audit. There should be two audits, she reiterated: one Compliance Audit for 2009 and one Day Zero audit on 9/30/2010.

### **ISO Standards for PKI Audits**

Cheryl Jenkins wanted to know what the status of ISO 27001 is vis-à-vis NIST SP 800-53. She said NIST had been moving to align ISO 27001 and ISO 27006, the IT infrastructure standard with NIST SP 800-53. She wondered if that had changed.

Brian Dilley said that ISO 21188 is better for us to align with because it is designed for PKIs. Compliance with ISO 21188 would allow us to be on the ISO standards list.

**ACTION:** Cheryl 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.

### **PD-VAL WG**

The FPKI TAG did a White Paper on the quality of applications in PKI. They recommended that the PD-VAL WG be resurrected to develop some processes and guidance documents that will assist us in having better paths in the FPKI.

**ACTION:** Cheryl Jenkins will distribute the TAG White Paper on the need for a PD-VAL WG this week.

### **Directory Searches**

We had 31 million directory searches in Feb. and over 25 million HTTP Web server requests, for a total of over 56 million searches of the FPKIA repositories.

## **Agenda Item 7**

### **FPKI Certificate Policy Working Group (CPWG) Report—Terry McBride**

#### **1. Discuss: CertiPath Annual Audit Report**

Mr. McBride said there were no issues with the audit; despite the fact, the auditors used the WebTrust methodology, due to the way that CertiPath had worded the assertions to be audited.

**2. Discuss / Vote: The Common CP Change Proposal: UUIDs in Card Authentication Certificates (with new Practice Note)**

The FPKIPA voted by 14/15 (93.4%) to accept the Common CP Change Proposal: UUIDs in Card Authentication Certificates, where a 2/3 majority vote was required. The purpose of the change proposal is to align the Common Certificate Policy with NIST SP 800-73-3 by permitting Card Authentication certificates to include Universal Unique Identifiers (UUID).

Vote to approve the Common CP Change Proposal—UUIDs in Card Authentication Certificates			
	Vote (Motion- Treasury 2 <sup>nd</sup> - PTO)		
	Yes	No	Abstain
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

**Agenda Item 8**

**Adjourn Meeting**

USPS made a motion to adjourn and NRC seconded it. Ms. Spencer adjourned the meeting at 11:44 a.m.

**CURRENT 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

FPKIPA Minutes 9 March 2010

No.	Action Statement	POC	Start Date	Target Date	Status
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 Cheryl Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Cheryl Jenkins	13 May 2008	10 June 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.	Judith Spencer	14 October 2008	12 November 2008	Open
378	Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.	Cheryl Jenkins	9 June 2009	14 July 2009	Open
379	Cheryl 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.	Cheryl Jenkins	9 June 2009	14 July 2009 and monthly afterwards	Open
381	Judith Spencer will check with NIST for additional guidance on device certificates.	Judith Spencer	9 June 2009	18 June 2009	Open
382	Judith Spencer will talk with Bill Macgregor at NIST about guidance for Key Management history.	Judith Spencer	9 June 2009	18 June 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.	Judith Spencer	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 FY1010 Accomplishments paper.	Judith Spencer	10 Nov. 2009	Oct. 2010	Open
384	Wendy 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.	Wendy Brown	10 Nov. 2009	16 Nov. 2009	Open
385	We need to write a Change Proposal, adding a <i>cardAuth</i> policy to FBCA. FBCA will require a UUID, as opposed to being optional.	Judith Spencer	10 Nov. 2009	30 Nov. 2009	Closed

FPKIPA Minutes 9 March 2010

No.	Action Statement	POC	Start Date	Target Date	Status
386	Jim Schminky will provide the MA with a report of availability from a customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.	Jim Schminky	10 Nov. 2009	30 Nov. 2009	Open
387	The Secretariat will put Debbie Mitchell's discussion of asserting Common Policy OIDS outside the <i>PIVauth</i> and cardAuth certificates for signature or encryption on the FPKIPA agenda for Dec. 8, 2009	Judith Fincher	10 Nov. 2009	8 Dec. 2009	Closed
388	Cheryl 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.	Cheryl Jenkins	9 March 2010	13 April 2010	Open
389	Cheryl Jenkins will distribute the TAG White Paper on the need for a PD-VAL WG this week.	Cheryl Jenkins	9 March 2010	12 March 2010	Open