



**Minutes of the 10 November 2009 Meeting**  
**USPS, 475 L'Enfant Plaza, SW, Washington, DC.**  
**CR 2P316 (inside CR 2P310)**  
**9:40 a.m. – 11:24 a.m.**

**A. AGENDA**

- 1. Welcome / Introductions**
- 2. Discuss/Vote on 13 October 2009 FPKIPA Minutes**
- 3. Discussion Paper: SSL Inspection and Mutual TLS Issue** Terry McBride
- 4. Review FY 09 Year End Report** Judy Fincher
- 5. FPKI Certificate Policy Working Group (CPWG) Report** Co-Chair  
Terry McBride
  - 1- Discuss / Vote: Revised FPKIPA By-Laws*
  - 2- Discussion Only: COMMON CP Change Proposal: UUIDs in Card Authentication Certificates (with Practice Note)*
  - 3- Discussion Only: FBCA CP Change Proposal on Cryptographic Key Length*
  - 4- Discuss / Vote: Entrust SSP Clone Cross-Certification*
  - 5- Discuss IdenTrust ACES Audit*
- 6. FPKI Management Authority (FPKI MA) Report** Wendy Brown
- 7. ICAM Update** Judith Spencer
- 8. White Paper on Realized Value of FPKI** Judith Spencer
- 9. Other Agenda Items**
- 10. Adjourn Meeting**

**B. ATTENDANCE LIST**

**VOTING MEMBERS**

The meeting began with a quorum of 13/14 (or 92.9%) where a two-thirds majority was required. One member, USPTO, was absent for the third time in a row.

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 have been redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at [Judith.fischer@pgs.protiviti.com](mailto:Judith.fischer@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   |
| 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) | Jewell, Chris    | Teleconference   |
| GPO  | Hannan, John     | Teleconference   |
| GSA  | Spencer, Judith  |                  |
| NASA                                       | Levine, Susan    | Teleconference   |
| Nuclear Regulatory Commission- NRC         | Sulser, David    |                  |
| SSA  | Mitchell, Eric   | Teleconference   |
| USPS                                       | Stepongzi, Mark  |                  |
| USPTO                                      | ABSENT           |                  |

#### **OBSERVERS**

| <b>Organization</b>  | <b>Name</b>        | <b>Telephone</b> |
|--|--------------------|------------------|
| DOI  | Abar, Amanda       |                  |
| FPKIPA Support/Secretariat (Contractor, Protiviti Government Services) | Fincher, Judy      | Teleconference   |
| IdenTrust  | Schambach, Marco   | Teleconference   |
| GSA Support (Contractor, Unisys)                                       | Petrick, Brant     |                  |
| Department of State/ Co-chair, CPWG (Contractor, ManTech)              | Froehlich, Charles |                  |
| GSA Support (Consultant, RJ Schlecht Consulting)                       | Schlecht, R.J.     |                  |
| FPKI PA (Contractor, PGS)  | McBride, Terry     |                  |
| FPKI MA Technical Liaison (Contractor, Protiviti Government Services)  | Brown, Wendy       |                  |
| GPO/Office of the Federal Registrar                                    | Massimini, Mike    | Teleconference   |
| Wells Fargo  | Schwartz, Ruven    | Teleconference   |
| DoE (Contractor, M Squared Strategies, Inc.)                           | Olson, Evan        |                  |
| DoE  | Varghese, Jebby    | 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 9:40 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. The meeting started with a quorum (13/14) or 92.9% of voting members

**Agenda Item 2**

**Discuss/Vote on 13 October 2009 FPKIPA Minutes**

Ms. Fincher said that all comments had been incorporated on the 13 October FPKIPA Minutes. There was no discussion. The FPKIPA voted unanimously (100% of those voting) to approve the minutes, as edited, **where a 50% majority vote was required.**

| <b>Approval vote for 13 October 2009 FPKIPA Minutes – red line version</b> |  |           |                |
|--|--|-----------|----------------|
|  | <b>Vote (Motion- Treasury 2<sup>nd</sup>-USPS)</b> |           |                |
|  | <b>Yes</b>   | <b>No</b> | <b>Abstain</b> |
| 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)                                 | √  |           |                |
| GPO  | √  |           |                |
| GSA  | √  |           |                |
| NASA   | √  |           |                |
| Nuclear Regulatory Commission (NRC)  | √  |           |                |
| SSA  | √  |           |                |
| USPS   | √  |           |                |
| USPTO  |  |           | ABSENT         |

**Agenda Item 3**

**Discussion Paper: SSL Inspection and Mutual TLS Issue**

**Terry McBride**

The FPKIPA discussed the problems agencies are having when using the “Blue Coat” vendor web proxy device when trying to access MAX.gov. Trusted traffic is not being passed through. This is one of the “unintended consequences” of security. The only workaround in the bounds of the protocol is to bypass the proxying.

Jim Schminky [or David Sulser]: The problem is that the PKI is working well (as designed) and is blocking the “man in the middle.”

Terry McBride of PGS developed a White Paper on this problem, entitled, “SSL Inspection and Mutual TLS Issue, and an accompanying slide set which were distributed to the FPKIPA prior to the meeting.

Ms. Spencer said that with this group’s agreement, we want to provide this White Paper and slide set to the ICAMSC and then to the Network Infrastructure subcommittee of ISIMC.

Judy Spencer: My thoughts are that the whole concept is broken; if I can put a “legitimate” trusted man in the middle, someone could masquerade as a trusted man in the middle.

**ACTION:** Judy Spencer will send the Discussion Paper: “SSL Inspection and Mutual TLS Issue” to the ICAMSC with today’s date as an information paper, not a recommendation from the FPKIPA.

**ACTION:** The Secretariat will add a reference to the Discussion Paper: “SSL Inspection and Mutual TLS Issue,” in the FY2009 Accomplishments paper.

#### **Agenda Item 4**

##### **Review FY 09 Year End Report**

**Judy Fincher**

Judith Fincher said that the November 2, 2009 version has been sent out. We are asking the FPKIPA to review it and provide any additional comments by COB, Nov. 18, 2009. It will go to Carol Bales and to the Chairs of the ISIMC as soon as the FPKIPA releases it.

#### **Agenda Item 5**

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

**Co-Chair, Terry McBride**

##### **1. Discuss / Vote: Revised FPKIPA By-Laws**

Ms. Spencer said that the By-Laws had been aligned with the new Charter and that redundant language had been removed. For example, we took out references to Charter Members and ACES. We made sure anything in the Charter was also addressed in the By-laws and changed “working days” to “business days.”

There was no further discussion, so a motion was made to vote to accept the new By-Laws, as written. The FPKIPA approved the By-Laws by 13/14, or

92.9% of all voting members, where a  $\frac{3}{4}$  majority vote was required. USPTO was absent.

| Approval vote to accept the Revised FPKIPA By-Laws – red line version |   |    |         |
|---|---|----|---------|
|   | Vote (Motion- State 2 <sup>nd</sup> - Treasury) |    |         |
|   | 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)                            | √   |    |         |
| GPO   | √   |    |         |
| GSA   | √   |    |         |
| NASA  | √   |    |         |
| Nuclear Regulatory Commission (NRC)                                   | √   |    |         |
| SSA   | √   |    |         |
| USPS  | √   |    |         |
| USPTO   | ABSENT  |    |         |

## 2. Discussion Only: COMMON CP Change Proposal: UUIDs in Card Authentication Certificates (with Practice Note)

We will not vote on this Change proposal until NIST SP 800-73-3 is published. NIST SP 800-73-3 is currently out for public review.

The Problem: The FASC-N is not unique outside of the Federal Government, so the UUID was introduced in NIST SP 800-73-3 to create a universal unique identifier. It specifies how to use the UUID in card authentication. It affects Common CP 3.1.1 regarding the types of names in the *cardAuth* certificate of the card. The proposal is to add a sentence, stating that *cardAuth subjectaltname* may include the UUID. There is some consideration being given as to whether the UUID can be used in addition to FASC-N for Federal Agencies. This is still under review because the FPKIPA and FPKI MA are not sure what effect this would have on operational relying party systems.

Judith Spencer: The reason we're doing this is to accommodate the PIV-I environment. If you see 9999 in FASC-N, look for a UUID. Today, COMMON limits you to the FASC-N.

Judith Spencer: This will also enhance interoperability of PACS systems.

**ACTION:** Judith Spencer: We need to write a Change Proposal, adding a *cardAuth* policy to FBCA. FBCA will require either a FASC-N or UUID, as opposed to being optional.

If you have a problem with this change proposal, comment on NIST SP 800-73-3; this Change Proposal is only aligning with 800-73-3.

Any changes made to FIPS 201 or any supporting document, must be backwards compatible. There is no danger of FASC-N going away in the next year or so.

### **3. Discussion Only: FBCA CP Change Proposal on Cryptographic Key Length**

In 2006 NIST SP 800-57 started talking about migration of key sizes. It talked about sun-setting RSA keys of 2048 bit key length by 2030. Anyone who is going to re-key a root CA or self-signed CA for more than 20 years, beware that this will take effect at Midnight December 31, 2010. The work-around is to make sure the expiry is before December 31, 2030 until you are ready to adopt 3072 bit keys. There is no requirement to remove SHA 256 before 2030, Ms. Spencer said.

Judith Spencer: Dave Cooper wants us to be aware and institutionalize it now so we are not caught unawares.

This change proposal is for discussion only today. We need to pass this change proposal this year, to give people a year to get ready. It is up for a vote next month (Dec. 8, 2009). CertiPath and SAFE-Biopharma are aware of this requirement and apparently do not have problems. There are ways to mitigate the risk by the end of next year and over the next 20 years.

Judith Spencer: Go back and talk to your people.

### **4. Discuss / Vote: Entrust SSP Clone (NFI) Cross-Certification**

The Entrust SSP Clone (Non-Federal Issuer, or NFI) policy mapping and technical testing are done, along with white space mapping. John Cornell signed off on the Entrust audit yesterday afternoon. The auditor was eValid8. So, this is ready for a vote at this meeting or e-vote if there are any objections because we did not provide 5 day's notice. The cross-certification vote was approved unanimously by those voting, or 92.9%, where a  $\frac{3}{4}$  majority vote was required.

Ms. Spencer: We now have three (3) NFI SSP clones cross-certified. This is good for external organizations that want a relationship with us, because they

can come in under an NFI SSP Clone and not have to stand up their own PKI or go through the FBCA cross-certification process.

| <b>Approval vote to Cross Certify Entrust SSP NFI Clone at Basic, Medium, Medium Hardware</b> |  |           |                |
|---|--|-----------|----------------|
|   | <b>Vote (Motion- Treasury 2<sup>nd</sup>- GPO)</b> |           |                |
|   | <b>Yes</b>   | <b>No</b> | <b>Abstain</b> |
| 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)  | √  |           |                |
| GPO   | √  |           |                |
| GSA   | √  |           |                |
| NASA  | √  |           |                |
| Nuclear Regulatory Commission (NRC)   | √  |           |                |
| SSA   | √  |           |                |
| USPS  | √  |           |                |
| USPTO   | ABSENT   |           |                |

**5. Discuss IdenTrust ACES Audit**

The approval of the IdenTrust ACES audit occurred this past week when John Cornell approved it. This agenda item is for information only since approval of the audit does not require a vote by the FPKIPA. The FPKIPA acknowledged receipt of the IdenTrust ACES audit.

**Agenda Item 6**

**FPKI Management Authority (FPKI MA) Report Wendy Brown for Cheryl Jenkins**

Wendy Brown made the FPKI MA report in the absence of Ms. Jenkins, who was ill.

**1. Program Management**

- Possible space in a federal data center located in Chantilly, VA has been found to: (1) relocate the back-up site at 7th & D Sts., SW and (2) build part of the target architecture. If the space is acquired, it will

allow us to resume full back-up operations and keep on schedule for the re-design.

Ms. Jenkins will continue to work with senior management to search for additional space that will house other components of the architecture.

## **2. Security and Architecture Management**

- Repository availability for October was 99.7 %. It is understood that this percentage represents the repositories' availability from inside the architecture. However, when the bandwidth for the data circuit is increased this month, this percentage should include the availability to the customers.
- Repository usage continues to grow, with over 22 million directory searches in October.

The report was distributed yesterday. It shows that over the last 10 months, HTTP requests have grown steadily, while LDAP requests have increased more slowly. Ms. Spencer suggested LDAP requests are probably legacy systems and HTTP are PIV requests, but there is no way to verify this theory.

Judith Spencer: I still have to justify spending money on the re-design, so this data is great.

**ACTION:** Jim Schminky will provide the FPKI MA with a report of availability from a customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.

When the FPKI MA increases the data bandwidth this month, it will entail a change to the IP address at the primary site. The FPKI MA will send a notice, with details about the change, to the FPKI community when the new IP address and dates are known.

## **3. Technology Management**

- The ECC paper that was mentioned last month has been reviewed by NIST and the FPKIA Technical Advisory Group (TAG) is incorporating the comments received. The revised paper will be released this month. Also, this topic will be discussed at the TWG.
- In effort to help with properly implementing PKIs, the TAG is working on another paper that will evaluate path quality and management of paths within the FPKI to improve interoperability.

- The FPKI TWG meeting will be held next Monday, 16 November. If you are sending a technical representative or will attend, please RSVP to Matt King by Thursday, 12 November at [Matthew.King@pgs.protiviti.com](mailto:Matthew.King@pgs.protiviti.com)

Judith Spencer: We need to start doing regular updates on the FPKIA re-design. There have been recent changes to planning for the re-design and the FPKIPA should be aware of them. The old concept was to have 4 replicated directories spread across the country, load balanced, etc., with a primary and secondary site. There has been a slight change to that construct: P1 and P2 are unchanged. But, one of the replicated directory sites will become a Trusted Operations Center. The TOC will allow remote administration of the two sites, P1 and P2. It also provides for better survivability in case of disaster or man-made emergency.

Judy Spencer asked if the MA plans to do remote certificate issuance from the TOC.

Wendy Brown: This concept is still to be determined, since it has not been tested yet.

## **Agenda Item 7**

### **ICAM Update**

- 1- Approval of the ICAM Segment Architecture is expected this week.

The National Security Systems met last Friday and created a Member Governing Body (MGB) for the newly conceived classified PKI. The Classified PKI formed a CNSS WG. This WG developed a policy and are building a PKI. The CNSS Root will be up by end of November, 2009 for Secret and below systems (CNSS) for National Security. The WG under CNSS has changed into a MGB for the newly conceived, secure PKI. CNSS Policy 25 provided for a MGB.

- 2- At the Nemaquin, PA, conference on Identity and Access Management last week, a small working Group, the Identity & Access Management working group (IDAM) was started with Deb Gallagher (DHS) and Sheron Randall (DoD) as co-chairs. Why have a MGB? Ms. Spencer reported that Dave Wennergren and Ron Carey, chair of ISIMC, agreed to combine the MGB with the FPKIPA. The concept is that the MGB will be an adjunct of FPKIPA. Debbie Mitchell suggested that the IDAM WG will, instead, combine with ICAMSC. Ms. Spencer said that the CNSS does not want to

own the MGB. Deb Mitchell: The MGB owns the CP under which the CNSS operates. It has both an operational and policy mission.

### **Agenda Item 8**

#### White Paper on Realized Value of FPKI

Ms. Fincher said that the final FPKI Value Paper would be released soon. It is currently under review at PGS. The White Paper will go out to the FPKIPA for a final review and then Ms. Spencer will send it to the ICAMSC.

### **Agenda Item 9**

#### Other agenda items:

- 1- Yesterday at the ISIMC meeting, there was discussion of a new strategic plan coming out of Federal CIO Council. The ICAM, as well as the FPKIPA, are objectives. This will be discussed next week and on November 23, 2009 at the Federal CIO Council.
- 2- The December 8, 2009 FPKIPA meeting will be short, followed by a holiday party. Everyone is encouraged to bring food and drink to be shared.
- 3- The December CPWG will be held on Monday, December 14 at the Snowden River, Columbia, MD, A&N office location.
- 4- Debbie Mitchell asked for a future meeting to discuss the desire on part of the legacy Agency PKIs to assert Common Policy OIDs outside the *PIVauth* and *cardAuth* certificates for signature or encryption.

**ACTION:** The Secretariat will put Debbie Mitchell's discussion of asserting Common Policy OIDs outside the *PIVauth* and *cardAuth* certificates for signature or encryption on the FPKIPA agenda for Dec. 8, 2009.

- 5- Wendy Brown is trying to get the Common Policy root certificate into Mozilla. She wants to identify Common Policy partners issuing SSL certificates under the Common Policy. She asked if anyone had web servers using those certificates that could be contacted over the Internet for purposes of Mozilla Testing. Ms. Spencer commented that the GSA MSO might be.

**ACTION:** Wendy Brown is to draft an email memo for the ICAMSC regarding the Mozilla root store request and send to Brant Petrick for distribution to the ICAMSC.

### **Agenda Item 10**

## 6. Adjourn Meeting

Treasury made a motion to adjourn, seconded by NRC, and everyone agreed by voice vote at 11:24 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   |
| 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,<br>FPKIPA,<br>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   |

| No. | Action Statement  | POC            | Start Date   | Target Date  | Status |
|-----|---|----------------|--------------|--------------|--------|
| 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 | Closed |
| 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 | Open   |
| 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 | 30Nov. 2009  | Open   |
| 387 | The Secretariat will put Debbie Mitchell's discussion of asserting Common Policy OIDS outside the <i>PIVauth</i> and <i>cardAuth</i> certificates for signature or encryption on the FPKIPA agenda for Dec. 8, 2009 | Judith Fincher | 10 Nov. 2009 | 8 Dec. 2009  | Open   |