# Minutes of the 10 February 2009 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316

## A. AGENDA

1. Welcome / Introductions
2. Discuss/Vote on 13 January 2009 FPKIPA Minutes
3. DoD Presentation: "DoD External PKI Interoperability Testing"
4. FPKI Certificate Policy Working Group (CPWG) Report
    a. Discuss/Vote on Common Policy CP Change Proposal: 2009-01—Change the *nextUpdate* Period for Legacy PKIs
    b. Discuss FBCA CP Change Proposal: 2009-xx—In-Person Antecedent for Medium Hardware
    c. Discuss/Vote on FBCA CP Change Proposal:2009-01—Remove the Requirement to Back Up the Entity Archive
    d. Discuss CPWG Mapping Recommendation for Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
5. FPKI Management Authority (FPKI MA) Report
6. ISIMC/ICAM SC Briefing
7. Updating the FPKIPA Charter and By-Laws
8. Adjourn Meeting

## B. ATTENDANCE LIST

### VOTING MEMBERS

The meeting began with a quorum of 11/15 (or 73.3%) where a two-thirds majority was required. Additionally, another member joined late, bringing the ratio to 12/15.

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.fincher@pgs.protiviti.com.

| Organization | Name | Telephone |
|---|---|---|
| Department of Commerce (NIST) | ABSENT | |
| Department of Defense | Mitchell, Debbie | Teleconference |
| Department of Health & Human Services | Slusher, Toby | Teleconference |
| Department of Homeland Security | Miller, Shawneque | |

| Organization | Name | Telephone |
|---|---|---|
| Department of Justice | Morrison, Scott | |
| Department of State | PROXY to FPKIPA Chair | |
| Department of Treasury | Jim Schminky | |
| Drug Enforcement Administration (DEA CSOS) | Jewell, Chris | Teleconference |
| GPO | Hannan, John | |
| GSA | Spencer, Judith | |
| NASA | Levine, Susan (joined after vote on the Minutes) | Teleconference |
| Nuclear Regulatory Commission- NRC | ABSENT | |
| SSA | Eric Mitchell | Teleconference |
| USPS | Stepongzi, Mark | |
| USPTO | ABSENT | |

**OBSERVERS**

| Organization | Name | Telephone |
|---|---|---|
| FPKIPA Support/Secretariat (Contractor, Protiviti Government Services | Fincher, Judy | |
| IdenTrust | Schambach, Marco | Teleconference |
| FPKI/FICC Support (Contractor, APEX) | Petrick, Brant | |
| Department of State/ Co-chair, CPWG (Contractor, ManTech) | Froehlich, Charles | |
| DoD/DISA (Contractor, Booz Allen) | Spann, Curt | |
| Wells Fargo | Schwartz, Ruven | Teleconference |
| Treasury | Robinson, Michael | |
| eValid8 | Dilley, Brian | |
| FPKI MA Technical Liaison (Contractor, Protiviti Government Services) | Brown, Wendy | |
| FPKIPA Support, Co-Chair CPWG (Contractor, Protiviti Government Services) | McBride, Terry | |
| DHS(Contractor) | Shomo, Larry | Teleconference |
| DOE | Lonnerdal, Nils “Daniel” | |
| DOE | Varghese, Jebby | |
| Cipher Solutions, Inc. | Ahuja, Vljay | |

**C. MEETING ACTIVITY**

**Agenda Item 1**

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

The FPKIPA met at the USPS Headquarters Building located at 475 L’Enfant Plaza, SW, Washington, DC, in Conference Room 2P316. Judith Spencer, Interim 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 the USPS for hosting the meeting.

## Agenda Item 2

### Discuss/Vote on 13 January 2009 FPKIPA Minutes— Judy Fincher

The FPKIPA approved the minutes, unanimously (11/11) or 100% where a 50% majority vote was required, with the condition that three observers be added. (Done) USPTO, NRC, Commerce and NASA were absent for this vote.

| **Approval vote for 13 January 2009 FPKIPA Minutes – red line version** | | | |
|---|---|---|---|
| | **Vote (Motion- SSA, 2nd- USPS)** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | ABSENT | | |
| 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 | ABSENT for this vote | | |
| Nuclear Regulatory Commission (NRC) | ABSENT | | |
| SSA | √ | | |
| USPS | √ | | |
| USPTO | ABSENT | | |

## Agenda Item 3

**DoD Presentation: "DOD External PKI Interoperability Testing"—Curt Spann (DISA)**

Curt Spann (DISA) gave a PowerPoint presentation on the DoD External PKI Interoperability testing and its current status. This testing was performed at the JITC PKE Lab by JITC personnel at Ft. Huachuca. Both direct and cross certificate trust models were used for testing. For direct trust, external PKI CA certificates were loaded into the trust store. For cross-cert trust, external PKI CA certificates were obtained in real time by following the AIA extension of the certificate. In both cases, the revocation data were obtained in real time by following the CDP (CRLs) or AIA (OCSP) extension of the certificate.

There were two test cases:

1) Email—Open signed e –mail sent from an external PKI user (Outlook client)
2) Web Authentication-–External PKI user accesses DoD PK-enabled web site (SSL with client authentication).

The DoD used a PKI Path Processing Tool built by Cygnacom for the DoD (PKITHING). It is used to verify the infrastructure.

ACTION: Debbie Mitchell will ask Camie Webster if the PKITHING tool and other tools used in the testing are available to the FPKIPA community.

**Test Findings**

All eight External PKIs passed the direct trust model testing, but all eight External PKIs failed the cross certificate trust model testing because:

1) Production DoD I-Root CA is only cross certified at the High Assurance Level, and the certificates provided by the eight External PKIs for testing were Medium Hardware assurance because the FBCA to DoD certificate is only Medium Hardware.
2) Client AIA path processing failures
3) Currently only DoD CAs 19 and 20 contain the required AIA extension for external partners to path process correctly.

Ms. Spencer said that if you are using the cross certification; model, as opposed to direct trust, DoD only trusts High credentials from external -- to DoD -- PKIs; whereas we trust them at Medium and Medium Hardware. Terry McBride said that as a result, the cross-certification tests were doomed to fail.

Testing has been completed with DoS, DOJ, Treasury, Northrop Grumman (CertiPath), Lockheed Martin (CertiPath), Raytheon (CertiPath), Boeing (CertiPath), DoT, EPA, and SSA. On the schedule to test are FAA, GSA, DHS, and NASA.

Charles Froehlich wanted to know when the other half of the equation would be tested. This has been a problem for about two years and it does not appear that much progress has been made. Mr. Spann said that higher-level coordination would be required. Ms. Spencer said that she believes a lot of progress has been made in that Morris Hymes has already signed off on that policy, e.g., of requiring DoD applications to trusting certificates from external PKIs. "We need to get the technical bits resolved," she said.

**Next Steps**
Ms. Spann said there is a need to share the lessons learned and configuration guidance gained from interoperability testing with the rest of the Federal community and industry partners. This would be accomplished with a Federal Interoperability collaboration site.

Ms. Spencer said that the GSA has already put up an interoperability collaboration site on CORE.GOV. We can enroll anyone who wants to play in this space, she said. Charles Froehlich said that DoS may have items to contribute also.

ACTION: Brant Petrick will re-send notice of signing-up for the CORE.GOV Public Key Enabling (PKE) Community to the FPKIPA voting members and to the DoD. (Done)

Debbie Mitchell said that the JITC web site shows all testing partners and the status of their testing. http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html.
She also urged all Legacy PKIs we have not tested with to move to Medium Hardware.

Ms. Mitchell urged Legacy PKIs that are cross-certified with the Federal Bridge at medium hardware to contact her when they are ready to conduct interoperability testing with the DoD so coordination can begin to take place.

DoD would also like to hear from those Federal agencies that are interested in participating in interoperability testing that are being issued certificates under the Shared Service Providers so that additional testing can be conducted in this area.

Terry McBride noted that the MA has tested product path validation against PKITS, not the actual architecture, and that they want the FPKI MA Interoperability Lab retest those validated products with the actual architecture, validating certificate paths back to the Common Policy root.

## Agenda Item 4

**FPKI Certificate Policy Working Group (CPWG) Report—Charles Froehlich, Terry McBride**

a. Discuss/Vote on Common Policy CP Change Proposal: 2009-01—Change the *nextUpdate* Period for Legacy PKIs

The FPKIPA voted unanimously to approve this Change Proposal (12/15, or 80%) where a 75% majority vote of all voting members was required. Before the vote, Ms. Spencer defined “legacy PKI” as a Federal Agency PKI run by that agency and cross-certified with the Bridge, as opposed to obtaining their credential through an SSP under the Common Policy. Legacy Agencies include DoS, Justice, DoD, Treasury, USPS, USPTO, DEA CSOS, and GPO, she said.

ACTION: The definition of a legacy PKI will be added to the Glossary in the policy.

| **Vote on Common Policy CP Change Proposal: 2009-01— Change the *nextUpdate* Period for Legacy PKIs** | | | |
|---|---|---|---|
| | **Vote (Motion- DoD, 2nd SSA)** | | |
| | **Yes** | **No** | **Abstain** |

| | | | |
|---|---|---|---|
| Department of Commerce | ABSENT | | |
| 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) | ABSENT | | |
| SSA | √ | | |
| USPS | √ | | |
| USPTO | ABSENT | | |

b. Discuss FBCA CP Change Proposal: 2009-xx --In-Person Antecedent for Medium Hardware

The CPWG discussed in-person antecedent and has formed a committee headed up by Jon Schoonmaker of SAFE Bio-Pharma to formulate policy for the in-person antecedent. Mr. Schoonmaker briefed us at the 5 February 2009 CPWG meeting on the progress made to date by his committee. Ms. Spencer described this as a "work in progress." Ms. Spencer said she had submitted a written comment to NIST (Donna Dodson) asking that NIST SP 800-63 relax the prohibition against in-person antecedent identity proofing at Medium Hardware. If 800-63 does not relax the requirement, she said, we're between a rock and a hard place.

c. Discuss/Vote on FBCA CP Change Proposal: 2009-01 —Remove the Requirement to Back Up the Entity Archive

The FPKIPA voted unanimously (12/15 or 80%) to approve FBCA CP Change Proposal: 2009-02, where a 75% majority vote of all voting members was required. This Change Proposal removed the requirement to back up the entity archive, but if an entity chooses to back up the archive, their CPS or referenced document "shall describe how the records are backed up and managed." Mr. Ahaju said that RFC 3647 introduced the requirement for entities to back up the archive.

| **Vote on FBCA CP Change Proposal: 2009-01— Remove the requirement to back up the entity archive** | | | |
|---|---|---|---|
| | **Vote (Motion - Treasury, 2nd GPO** | | |
| | **Yes** | **No** | **Abstain** |
| Department of Commerce | ABSENT | | |
| 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) | ABSENT | | |
| SSA | √ | | |
| USPS | √ | | |
| USPTO | ABSENT | | |

d. Discuss CPWG Mapping Recommendation for Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP

The CPWG had hoped to move forward with a motion to cross-certify Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware, and Medium Hardware CBP at this meeting. It was unable to do so, however, because the architectural diagram submitted by Verizon was unsatisfactory. It did not clearly delineate between the CA that would be cross-certified with the FBCA and the CA that supports their SSP offering. The CPWG is currently awaiting the corrected diagram and expects to approve it at the next CPWG meeting (February 19) and vote on this measure at the 10 March 2009 FPKIPA Meeting, else via e-vote.

**Agenda Item 5**

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

Wendy Brown reported that Microsoft has accepted putting the new Common Policy Certificate without SIA in its Trust List, it should be out approximately 2/24/09 and that talks have started with Apple and Mozilla. John Harris has reported that Adobe has accepted the Common Policy Certificate.

Ms. Brown said that the old DoS Cross-Certificate to the FBCA expired and that the MA is waiting to receive the new cross-certificate. The MA issued ORC SSP 2 a new certificate. The MA expects to issue Wells Fargo a cross-certificate at Basic to extend the life of that cert; a cross-certificate to Illinois at Basic; and 3 cross certificates for the VeriSign non-Federal clone PKI in February.

There is also a problem in the cross-certificate between the Common Policy and the Federal Bridge, which we expect to correct in February, she said. The policy mapping extension is marked as “critical.”

The directory availability was 97.8% in 2008, which did not meet the target of 99.0% availability. A patch to the Directory software and recent enhancements have addressed the problems we were having as a result of increased traffic, she said.

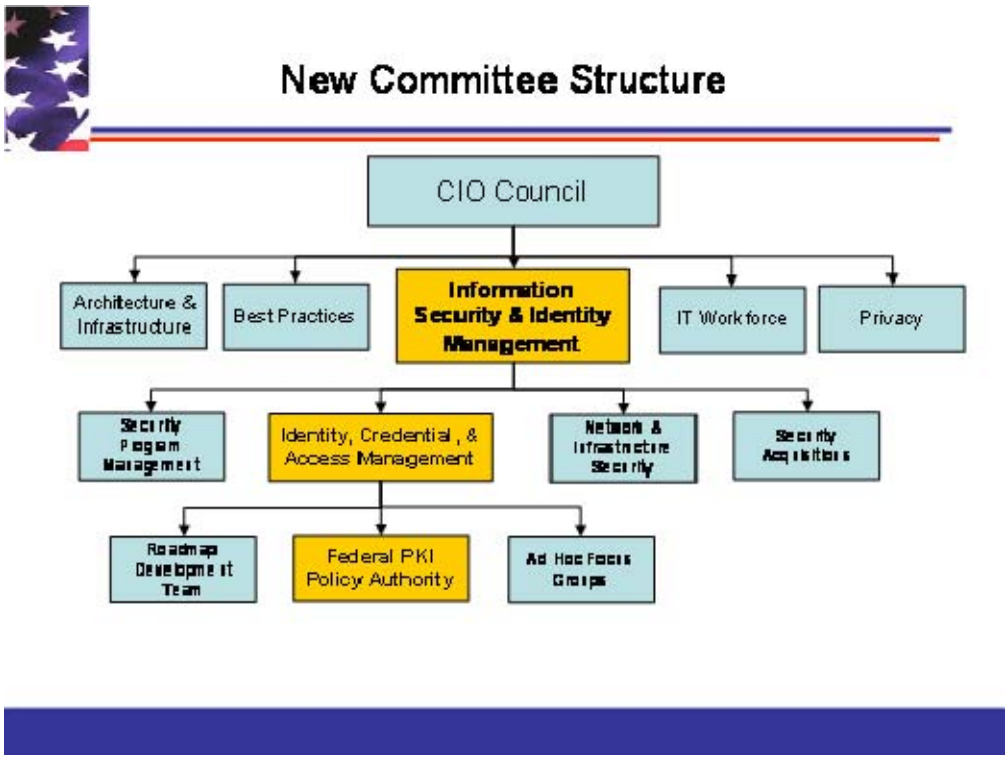
**Agenda Item 6**

**ISIMC/ICAM SC Briefing—Judith Spencer**

Judy Spencer briefed the FPKIPA on the new CIO Council structure, especially as it affects the FPKIPA. The CIO Council has stood up an Information Security and Identity Management Committee (ISIMC). Robert Carey (DON) and Vance Hitch (DOJ) are the co-chairs of the ISIMC. The ISIMC charter is posted at www.cio.gov. The CIO Council committees are listed on the right side of the page. Click on ISIMC to locate the Charter.

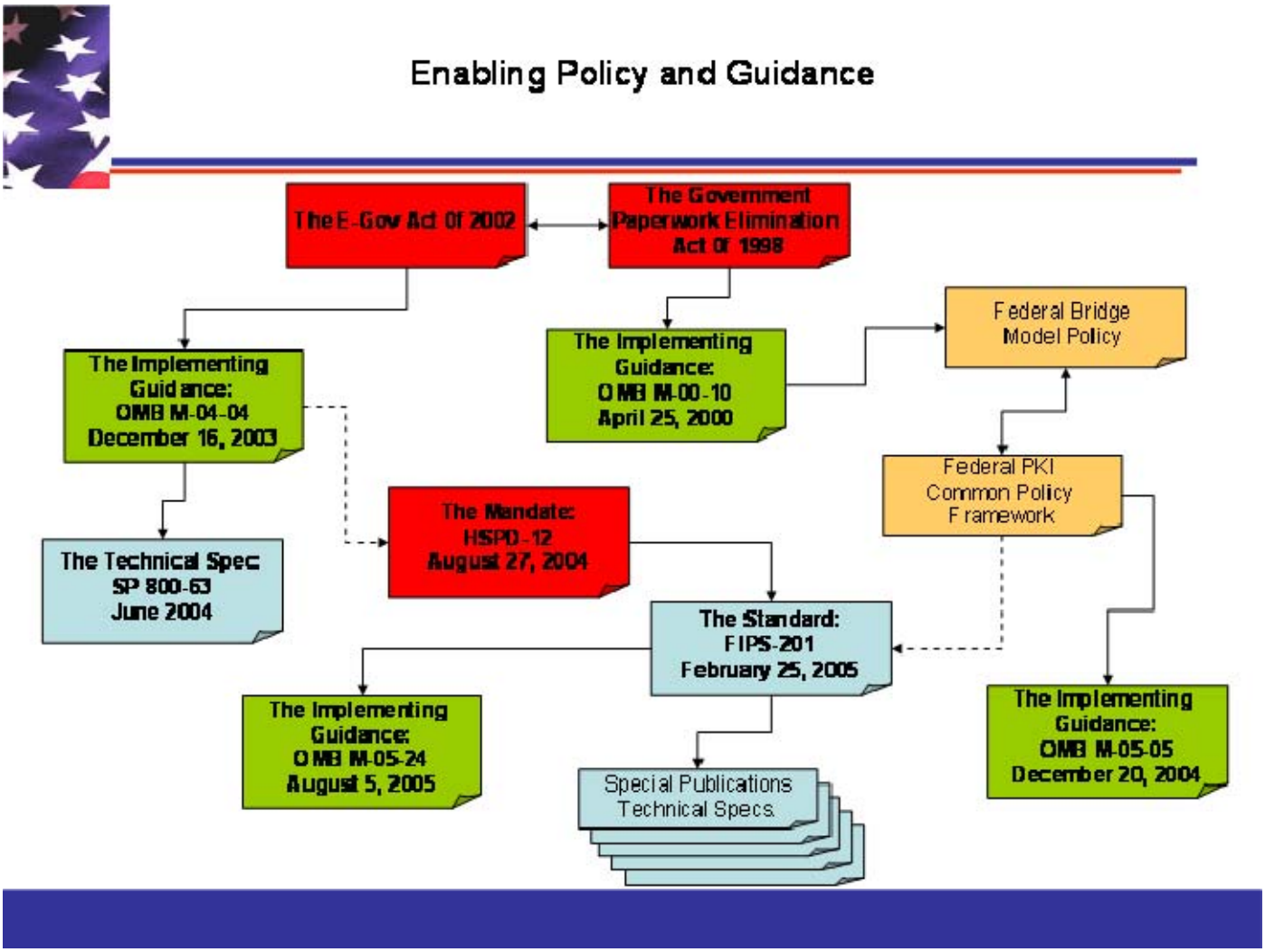
Under the ISIMC is the Identity, Credential and Access Management (ICAM) sub-committee. Paul Grant (DOD) and Judith Spencer (GSA) are the ICAM Co-Chairs. The FPKIPA now reports to the ICAM. The ICAM sub committee will replace the FICC, which will lose its separate identity; whereas, the FPKIPA will remain a separate organizational entity. The FICC will be sunset this Thursday, February 12, 2009, she said.

Under the ISIMC are four sub-committees: one deals with cyber security and three with site security. The establishment of these four sub-committees (one of which is ICAM) resulted from the publication of the Identity Management Task Force Report. Judith Spencer chaired that effort and was the editor of the final report. See the New Committee Structure, below.




The ICAM Mission is to foster effective government-wide identity and access management. It is not just a combination of PKI and HSPD-12. It seeks to ensure alignment across all identity and access management activities that cross individual agency boundaries. The Enabling Policy and Guidance are shown below.

- M-04-04 set up the E-Authentication categories and has as its technical specification NIST SP 800-63.
- M-05-05 created the policy requiring new Federal Agency PKIs to be outsourced from a Shared Service Provider (SSP) and is the technical specification for the FPKI Policy Authority.
- OMB M-05-24 describes how to identify consistent application of HSPD-12 logical and physical access solutions.




The ICAM has created a draft work plan and has identified four areas of work:

1) Access Management (OMB M-04-04)—Provide guidance on ensuring appropriate controls for web applications used for service to citizens and businesses. Ms. Spencer said the E-Authentication PMO was sunset two weeks ago and ICAM has now taken over its role. Key responsibilities are to: 1) develop guidance to provide for a unified architecture for ICAM, revising the IDM architecture in the process; 2) publish best practices implementation guidance for Access Management criteria at all levels of assurance; 3) and report on the role of ICAM in cloud computing and social media.

2) HSPD-12 (OMB M-05-24) Identify consistent application of HSPD-12 logical and physical access solutions - A key program will be the publication of the policy for "PIV Interoperability for Non-Federal Issuers." It will provide guidance on how to trust non-Federal issuers. Most technical issues have been resolved. Two notable exceptions are the FASC-N [and AID issues].
3) Public Key Infrastructure—Identity practical applications and lessons learned in implementing user authentication, multi-factor authentication, and device authentication/quarantine and Federal bridging of credentials/certificates between agencies. The ICAM is tasked with reporting on implementation of PKI and lessons learned. The work product will be a White Paper on the realized value of PKI, due by the end of March. Contractor help will be utilized in pulling together the ROI (tangible and intangible) from civilian agencies, the unclassified DoD components, and the Aerospace Defense Group. The ICAM will integrate current Federal PKI activities with ICAMSC, including the Federal PKI Policy Authority and Federal PKI Outreach Activities, such as the Transatlantic Secure Collaboration Program and the Four Bridges Forum. The ICAM will also brief the ISIMC on a quarterly basis, using as the basis of the briefing the minutes of the Federal PKI Policy Authority.

4) Federal Identity, Credential and Access Management Roadmap and Implementation Guide (to replace the FICC Handbook) - This will be a comprehensive guide for Federal agencies and industry partners on ICAM principles. The three areas above will feed into the Roadmap and Implementation Guide, which is developing a high-level Segment Architecture for ICAM. Carol Bales wants this by May ("early summer") so that it will make it into the FY 2011 Budget Submission. A guide on how to make the Segment Architecture real, including a description of a "segment architecture" and tools can be found at www.fsam.gov

**Next Steps**
The next steps are to sunset the FICC, to be replaced by ICAM, on February 12 and the ICAMSC meeting at 10 a.m. at the AIA building in downtown Washington, D.C., on February 25. Ms. Spencer read a list of the 22 existing members, noting that some FPKIPA agencies were not yet represented. She encouraged the FPKIPA agencies to join the ICAM, noting that they would need to get senior level endorsement to be a member. On February 19, members of the CPWG will discuss the realized value of PKI and present it to the ISIMC on March 1.

Ms. Fincher distributed Ms. Spencer's briefing after the meeting to the FPKIPA listserv.

**Agenda Item 7**

**Updating the FPKIPA Charter and By-Laws—Judith Spencer**

Ms. Spencer said that her intern, Rachael Murdoch, will take the first pass at updating the FPKIPA Charter and By-Laws to reflect the new reporting structure. FPKIPA members are urged to submit their comments to Brant Petrick (Brant.Petrick@gsa.gov), Rachael Murdoch (Rachael.Murdoch@gsa.gov), or to the FPKIPA webmaster (fpki.webmaster@gsa.gov) prior to the publication of the first draft on February 27.

**Agenda Item 8**

**Adjourn Meeting—Judith Spencer**
Ms Spencer adjourned the meeting at 10:57 a.m.

## CURRENT ACTION ITEMS

| No. | Action Statement | POC | Start Date | Target Date | Status |
|---|---|---|---|---|---|
| 285 | Judith Spencer and DoD will go off-line to discuss name uniqueness. She suspects there is name collision. | Judith Spencer, Debbie Mitchell | 8 May 2007 | 22 May 2007 | Open |
| 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 |
| 327 | Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA. | Cheryl Jenkins | 11 Dec. 2007 | January 2008 | Open |
| 331 | Dr. Alterman will draft language for the FBCA policy change procedure to do some “reality testing” and distribute it to the FPKIPA. | Dr. Peter Alterman | 8 April 2008 | 13 May 2008 | 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, FPKIPA, Cheryl Jenkins | 13 May 2008 | 10 June 2008 | Open |
| 371 | Dr. Alterman will inform Verizon Business Systems (VBS) that their application was approved and will ask for the ETA for the Policy. | Dr. Peter Alterman | 8 July 2008 | 15 July 2008 | Open |
| 373 | Deborah Gallagher will check with DHS to verify the FRAC requirement. | Deborah Gallagher | 9 Sept. 2008 | 14 Oct. 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 |
| 376 | Debbie Mitchell will ask Camie Webster if the PKITHING tool and other tools used in the testing are available to the FPKIPA community | Debbie Mitchell | 10 Feb. 2009 | 19 Feb. 2009 | |