Minutes of the 14 October 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316 (Inside 2P310)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 9 September 2008 FPKIPA Minutes
3. Results of the e-vote on the 12 August FPKIPA Minutes
4. Results of the e-vote on making the SIA Extension Optional
5. Results of the e-vote on cross-certifying DoS at C4, Rudimentary and the DOS request to assert id-fpki-common-authentication
6. Results of the e-vote on cross-certifying DoS at Basic, Medium, Medium Hardware and High
7. Discuss / Vote on AAAE Application to Cross Certify with the Federal Bridge at Rudimentary, Basic, Medium (for devices) and Medium Hardware
8. Discuss / Vote on the Preferred High Assurance Scenario for non-Federal Entities (2 Scenarios)
9. FPKI Certificate Policy Working Group (CPWG) Report
    a. **Discuss CPWG Mapping Report for VeriSign non-federal PKI SSP clone at Rudimentary, Basic, Medium and Medium Hardware (revised 2 Oct.)**
    b. **Review VeriSign WTCA Audit Letter and CPWG Response**
    c. **Discuss CPWG Mapping Report for DoD ECA (one-way) at Medium and Medium Hardware (revised 2 Oct.)**
    d. **Discuss FBCA CP Change Proposal: 2008-06 (CA validity period)**
    e. **Discuss /Vote FBCA CP Change Proposal: 2008-05 (Role-Based Certs), as revised 2 Oct.**
    f. **Discuss / Vote Common Policy Framework CP Change Proposal: 2008-03 (Role-Based Certs), revised 2 Oct.**
    g. **Discuss / Vote to cross-certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP**
    h. **Discuss / Vote on cross-certifying DoS at C4 and Rudimentary**
    i. **Discuss / Vote on DoS request to assert id-fpki-common-authentication**
10. FPKI Management Authority (FPKI MA) Report
11. Discuss Forum of the 4 Bridges (4BF) Revised Audit Cook Book
12. Final Meeting Items
    a. Proposed Agenda Items for the next FPKIPA meeting, 12 November 2008
    b. IdM Initiative
    c. 2009 Meeting Schedule
13. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of ten (or 67%) where a two-thirds majority was required.

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	Hagerling, Don	
Department of Justice	Morrison, Scott	
Department of State	Frahm, Jarrod	
Department of Treasury	Proxy to DoD	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan John	
GSA	Spencer, Judith	
NASA	ABSENT	
Nuclear Regulatory Commission- NRC	ABSENT*	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	ABSENT	

- NRC submitted a proxy designation that arrived after the meeting concluded.

OBSERVERS

Organization	Name	Telephone
FPKI MA PM/GSA	Jenkins, Cheryl	Teleconference
DOE	Lonnerdal, Nils	
GSA	Cornell, John	Teleconference
DHS OCIO	Gallagher, Deborah	
IdenTrust	Wilson, Ben	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
IdenTrust	Schambach, Marco	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
FPKI/FICC Support (Contractor--FC Business Systems LLC)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
FPKI MA Technical Lead (Contractor, Protiviti Government Services)	Brown, Wendy	
SAFE Bio-Pharma	Schoonmaker, Jon	Teleconference

Cipher Solutions	Ahuja, Vljay	
FPKIPA support (Protiviti Government Services, Contractor)	King, Matt	Teleconference
SSA	Jackmon, Kenya	Teleconference
NOAA (Contractor, General Dynamics)	Wright, BIll	
FPKIPA Support, Co-Chair CPWG (Protiviti Government Services, Contractor)	McBride, Terry	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Ms. 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 (inside 2P310). Ms. 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.

Agenda Item 2

Discussion / Vote on 9 September 2008 FPKIPA Minutes—Judith Fincher

The FPKIPA approved the 9 September 2008 FPKIPA minutes by the unanimous count of votes cast (10/10) or 100%.

Approval vote for 9 September 2008 FPKIPA Minutes – red line version			
	Vote (Motion- DHS, 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	ABSENT		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	ABSENT		
USPS –	√		
USPTO	ABSENT		

Agenda Item 3

Results of the e-vote on the 12 August 2008 FPKIPA Minutes—Judith Fincher

This e-vote passed, Ms. Fincher said.

Agenda Item 4

Results of the e-vote on making the SIA Extension Optional—Judith Fincher

This e-vote passed, Ms. Fincher said.

Agenda Item 5

Results of the e-vote on cross-certifying DoS at C4 and Rudimentary and the DOS request to assert id-fpki-common-authentication—Judith Fincher

This e-vote did not pass because of the bundling of the assertion request for id-fpki-common-authentication with the request to cross-certify DoS at C4 and Rudimentary. The FPKIPA voted on these items as separate requests later in this meeting. (See Agenda Item 9.h., and 9.i.)

Agenda Item 6

Results of the e-vote on cross-certifying DoS at Basic, Medium, Medium Hardware and High—Judith Fincher

This e-vote passed, Ms. Fincher said. Charles Froehlich said that John Cornell (the GSA lawyer) is currently reviewing the MOA.

ACTION: PGS (Terry McBride) will draft the LOA for Ms. Spencer's signature to issue a cert to DoS at Rudimentary, Basic, Medium, Medium Hardware and High.

Agenda Item 7

Discuss / Vote on AAAE Application to Cross Certify with the Federal Bridge at Rudimentary, Basic, Medium (for devices) and Medium Hardware—Judith Spencer

At the September 2008 FPKIPA meeting, the FPKIPA reviewed the application submitted by the Security Biometric Clearing Network (SBCN) on behalf of the American Association of Airport Executives (AAAE) to cross-certify with the Federal Bridge at four assurance levels: Rudimentary, Basic, Medium (for devices) and Medium Hardware.

At that time, the FPKIPA asked for clarification on several issues. Ms. Spencer contacted Patrick Osborne of the AAAE and received the following information:

1) The AAAE wishes to be certified at Medium Hardware and assumes that all levels below this are included. Ms. Spencer noted that this assumption is incorrect, and the application must reflect all requested assurance levels.
2) Mr. Osborne said the official sponsor at TSA has not yet been identified.

3) The AAAE does fingerprint submissions for everybody at domestic airlines and employees at commercial airports, but does not process fingerprints for foreign air carriers.

Don Hagerling said he, on behalf of DHS, is the official sponsor of the ACIS program (for the time being), i.e., the airport version of the TWIC card, and of this initiative. He also confirmed that AAAE is not asking for credentials for foreign pilots. That is handled elsewhere, he said.

Ms. Spencer said the AAAE expects to be up and running by January 2009, using a PKI supplier. This is not an impediment to us voting to accept their application, she said. Only SSPs must have operational PKIs before they can start the application process.

The FPKIPA then voted unanimously (10/10) or 100% to accept the AAAE application where a 75% majority vote was required.

Approval vote on AAAE Cross-Certification Application			
Voting members	**Vote (Motion – USPS ; 2nd –DHS)**		
	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		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	ABSENT		
USPS	√		
USPTO	ABSENT		

Agenda Item 8

Discuss / Vote on the Preferred High Assurance Scenario for non-Federal Entities (2 Scenarios)

The CPWG recommended approval of option 2008-04(A), the version of this Change Proposal that would limit High Assurance to the U.S. Federal government only.

1. Option A would limit High to the Federal Government and the Federal Government entities would operate the CAs. Under this scenario, both Federal employees and their contractors could receive high assurance certs.
2. Option B would open the issuance of High credentials to non-government entities. Essentially, this would open up High to all. There does not appear to be a market for Option B certificates, and state, local, and tribal government probably do not understand the level of administrative effort required for High assurance. The CPWG did not recommend this Option.

3. Option C would allow issuance of High credentials to US Federal, State, local and tribal governments, but a US government entity must operate the CA. The CPWG felt that government entities below the Federal level are unlikely to establish their own PKIs. [The CPWG considered this the fallback position, should Option A not be accepted.]

The FPKIPA then discussed the merits of each approach. DHS favored Option A, as did DoS. Don Hagerling said that High must not be tainted by motivation, priorities or fiduciary interests of non-US Federal Government entities. Ownership must be in the hands of the US Federal Government, he said. NRC, previously, had spoken in favor of Option B, but was not in attendance at this meeting. Ms. Spencer said that M-04-04 e-auth assurance level 4 (high) also maps to Medium Hardware, so there is no need for the FRAC community, etc., to come in at FPKIPA High in order to satisfy M-04-04 and FIPS 201.

The FPKIPA voted unanimously to accept FBCA CP Change Proposal: 2008-04 Option A (10/10) or 100% where a 75% majority vote was required.

Approval Vote to accept FBCA CP Change Proposal: 2008-04 (OPTION A) Limiting High Assurance to the Federal Government Entities Only			
Voting members	**Vote (Motion – DHS ; 2nd – Justice)**		
	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		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	ABSENT		
USPS	√		
USPTO	ABSENT		

Agenda Item 9

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

a. Discuss CPWG Mapping Report for VeriSign non-federal PKI SSP clone at Rudimentary, Basic, Medium and Medium Hardware (revised 2 Oct.)

The FPKIPA acknowledged receipt of the CPWG Mapping Report for VeriSign for Rudimentary, Basic, Medium and Medium Hardware. The FPKIPA did not have to vote because this report was not contentious. The CPWG did not map VeriSign at High, pending the results of this meeting. Now, that mapping will not be performed.

b. Review VeriSign WTCA Audit Letter and CPWG Response

John Cornell reviewed the VeriSign WTCA Audit Letter and found it failed on most criteria. He referred it back to VeriSign [to KPMG] and received a revised version on the morning of this meeting. This version, though improved, also failed. The FPKIPA did not vote because the CPWG cannot recommend acceptance.

c. Discuss CPWG Mapping Report for DoD ECA (one-way) at Medium and Medium Hardware (revised 2 Oct.)

The DoD ECA was successfully mapped at Medium and Medium Hardware following CPWG recommended changes that removed cross certification of the 1024-bit Root CA, and limited it to the 2048-bit CA. The CPWG report has been submitted, and no vote is required because this revised report was not contentious

d. Discuss FBCA CP Change Proposal: 2008-06 (CA validity period)

The FPKIPA could not vote on this change proposal because DoD had not formally accepted CPWG requested changes and due to DoD concerns regarding the requirement to audit configuration changes that appear to include all CA/RA systems.

A similar Change Proposal (CA Validity Period) for the Common Policy is under review by the CPWG. (See 9.f.)

e. Discuss /Vote FBCA CP Change Proposal: 2008-05 (Role-Based Certs), as revised 2 Oct.

At OMB's request, Tim Polk (NIST) prepared a Change Proposal which the CPWG reviewed to allow the issuance of role-based certs, i.e., certs issued to individuals—single or multiple—that are attributable to an official role, rather than that individual's actual identity.

At DoS request, this Change proposal was extended to provide the same capability under the Common Policy. Both are pending final revisions and acceptance. The FPKIPA did not vote at this meeting.

f. Discuss / Vote Common Policy Framework CP Change Proposal: 2008-03 (Role-Based Certs), revised 2 Oct.

The FPKIPA did not review this item at this meeting. (See 9.e.)

g. Discuss / Vote to cross-certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP

Wells Fargo was successfully mapped at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP, and its compliance audit has been accepted.

But, as a non-governmental entity, it must also undergo an Operational Parameters Review. Wells Fargo previously passed the Business Process Review (2006). The CPWG

is still conducting the Operational Parameters Review and expects to wrap it up at the 21 October 2008 meeting.

Wells Fargo is also drafting a refreshed MOA, according to Peri Drucker. NO interoperability testing is required because the directory has not changed, according to Wendy Brown.

h. Discuss / Vote on cross-certifying DoS at C4 and Rudimentary

The FPKIPA with minimal discussion unanimously approved the DoS request to be cross-certified at C4 and Rudimentary. (The vote in favor was 9/9 or 100%, where a 75% majority vote was required.

Approval Vote to Cross-Certify DoS at C4 and Rudimentary			
Voting members	**Vote (Motion – DHS; 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 - RECLUSE			
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	ABSENT		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	ABSENT		
USPS	√		
USPTO	ABSENT		

i. Discuss / Vote on DoS request to assert id-fpki-common-authentication

The DoS requested that the FPKIPA authorize the DoS to assert the id-fpki-common-authentication policy OID in its PIV certificates.

Ms. Spencer said that FIPS 201 required Federal agencies to put PIV authentication credential on the PIV cards, under the Common Policy id-fpki-common-authentication OID. We need to allow legacy agencies such as DoS to use the Common Authentication OID in their certs.

Ms. Spencer said that no vote is required because this is already permitted—except for DoD which cannot get to 18 hour CRLs.

The FPKIPA in December 2007 provided guidance on implementing HSPD-12 using Legacy PKI certificates. (See the Memorandum at the end of these minutes and/or on the FPKIPA web site, http://www.cio.gov/fpkipa/drilldown_fpkipa.cfm?action=memos_studies_papers.) The Memorandum is the one entitled: 12.07.07 - Implementing HSPD-12 using Legacy PKI Certificates.

This guidance states that Federal Legacy PKIs may assert id-fpki-common-authentication policy OID in its PIV certificates provided they were cross certified at Medium Hardware or Higher and provided that they adhere to other stipulations that affect certificate issuance:

- "Identity proofing requirements (FIPS 201 Section 2)
- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.
- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)
- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP)* Program [SSP-PROF] (FIPS 201 Section 5.4.2.1).
- Requirement not to post PIV Authentication certificates to a public directory. (FIPS 201 Section 5.4.5.1)
- Requirement to make directory information available via LDAP and HTTP. (FIPS 201 Section 5.4.5.1"

Since no vote was required, the FPKIPA authorized the DoS to assert the id-fpki-common-authentication policy OID in its PIV certificates by acclamation--not a formal vote). But, we need to chain back to the hierarchical root in Common, Ms. Spencer said, and NIST needs to tell us how to solve this. Terry McBride noted that this should not be a problem, technically.

Agenda Item 10

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

Wendy Brown said we now have a new directory product and a load balancing capability that should increase directory stability at the primary site. It will be tested in the lab over several weeks and deployed early November 2008.

The FPKI MA has stood up a second Common Policy CA to help Shared Service Providers with key rollover issues; and it is now available. The second CA is a peer to the current Common Policy CA and they are cross-certified with each other. This should be transparent to the outside community. This is a "shadow" CA with a path to the Common Policy root.

We have started on the re-design and the big equipment buy was completed by the end of the FY. Most of the equipment will ship by October 21, 2008, and the remainder in early November. We should be ready to deploy in March, 2009, she said.

The FPKI MA feasibility study on SHA-256 shows that most agencies are not ready to implement it, so we will hold off signing with SHA-256 for the present. Until 1Q FY10, we will run in parallel, taking steps toward the re-design.

Agenda Item 11

Discuss Forum of the 4 Bridges (4BF) Revised Audit Cook Book—John Cornell

John Cornell provided an update of an action resulting from the August 21, 2008 meeting of the audit working group, Forum of the Four Bridges (4BF). Mr. Cornell, the GSA/FPKIPA attorney, represented the FPKIPA. HEBCA was not in attendance. Vijay Takanti represented CertiPath and Jon Schoonmaker represented SAFE.

Mr. Cornell said that one outcome of that meeting was the creation of a joint CertiPath/FPKIPA "Audit Cook Book". Ms. Fincher displayed the document on the screen. It is also posted to the FPKIPA website.

John Cornell is drafting a FBCA CP Change Proposal for the November FPKIPA meeting, reflecting changes made to the Cook Book.

Agenda Item 12

Final Meeting Items

1) Proposed Agenda Items for the next FPKIPA meeting, 12 November 2008
   a. Results of e-vote to Cross-Certify Wells Fargo at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
   b. FBCA CP Change Proposal (Cook Book issues)—John Cornell

2) IdM Initiative
   Judith Spencer reported on efforts by the OMB, FICC and OGP to centralize all identity management initiatives under one authority. The FPKIPA web site will be transitioned to www.idmanagement.gov. One of the impacts of FIPS 201 and HSPD-12 is the re-birth of PKI, since digital certificates are required on the PIV card.

   Judith Spencer said that the newly released report by the National Science and Technology Council (NSTC) describes the new direction of Identity Management for the Federal Government. The FPKIPA will continue in its current function, but she recommended everyone read the report. The link to the NSTC Identity Management Task Force Report is:
   <http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf>

   According to Ms. Spencer, e-Auth, FPKIPA, and FICC will all come under this new organization and will have a Charter (already in draft) for the IdM Segment Architecture. The E-Auth PMO and Fed PKI is transitioning and transforming themselves. OGP will lead the government-wide effort to make Federal Identity Management a reality, she said.

   The CIO Council has stood up the Security Identity Management Committee (SIMC), led by Navy (Rob Carey) and Justice (name?)

   FICC will broaden its scope to look at IdM as a whole. FPKIPA will have a larger role to play in that structure, she said.

3) 2009 Meeting Schedule
There are several meetings next year, which closely precede or follow Federal holidays. The FPKIPA discussed possible solutions, such as moving the meeting dates and encouraging all members to issue an enduring proxy, in case they cannot attend a meeting.

ACTION: 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.

Action Item 13

Adjourn Meeting
Ms. Spencer adjourned the meeting at 11:27 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
315	Dr. Alterman and John Cornell will incorporate language into the FPKIPA audit Cook Book. This language was provided by Noel Nazario of KPMG and says that if customers set up the terms of their Web Trust audits appropriately, the Web Trust audit would satisfy all our requirements.	Dr. Alterman, John Cornell	9 Oct. 2007	13 Nov. 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
329	Cheryl Jenkins and Dr. Peter Alterman will reach out to Wells Fargo to determine what should be in the Directory and what the next steps are.	Cheryl Jenkins, Dr. Peter Alterman	11 March 2008	21 March 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

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
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
372	The CPWG will talk with VeriSign and Verizon Business to see how they would delimit boundaries and guarantee that certs will only go to government.	CPWG	9 Sept. 2008	14 Oct. 2008	Open
373	Deborah Gallagher will check with DHS to verify the FRAC requirement.	Deborah Gallagher	9 Sept. 2008	14 Oct. 2008	Open
374	PGS (Terry McBride) will draft the LOA for Ms. Spencer's signature to issue a cert to DoS at Basic, Medium, Medium Hardware and High.	Terry McBride	14 October 2008	12 Nov. 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

MEMORANDUM FOR FEDERAL AGENCY LEGACY PKIs

SUBJECT: Implementing HSPD-12 using Legacy PKI certificates

[DATE: 10/7/07]

Section 5.4.4 of FIPS 201 states: "Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)"
In order to facilitate Federal Legacy PKI compliance with this requirement, the Common Policy has been modified to include provisions that exclusively pertain to the Federal Legacy PKIs. By adding language pertaining to naming conventions and off-line root CAs, the main obstacles to compliance with the Common Policy by Federal Legacy PKI agencies have been removed. This should enable the Federal Legacy PKI agencies to express Common Policy OIDs in the PIV Authentication Certificates, as is required to meet the requirements of FIPS 201 (additional certificates for signing and key management can continue to only assert agency OIDs). However, those agencies planning to take advantage of this new language must ensure that they implement their certificates in a manner consistent with other provisions in the Common Policy. A Federal Legacy PKI will be deemed to be issuing PIV Authentication certificates in conformance with the Common Policy if it issues those certificates in accordance with the requirements of a certificate policy that has been mapped to the FBCA CP at the Medium Hardware or High assurance level and in accordance with the following additional provisions that affect certificate issuance:

- Identity proofing requirements (FIPS 201 Section 2)
- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.
- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)
- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP)* Program [SSP-PROF] (FIPS 201 Section 5.4.2.1).

- Requirement not to post PIV Authentication certificates to a public directory. (FIPS 201 Section 5.4.5.1)

- Requirement to make directory information available via LDAP and HTTP. (FIPS 201 Section 5.4.5.1

Peter Alterman, Ph.D.
Chair