

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 10 August 2004 Meeting GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Approval Vote of Minutes from 13 July 2004
- 3) Status of Email Votes Since Last FPKIPA Meeting
- 4) Discussion Topic: E-Governance CA CP, Section 2.4.2 – Dispute Resolution
- 5) DoD PKI Status Report on PKI Interoperability Requirements and Guidance Research
- 6) Federal Identity Credentialing Committee (FICC) Report
- 7) FPKI Certificate Policy Working Group (FPKI CPWG) Report
- 8) FBCA Operational Authority (FBCA OA) Report
- 9) Other Topics
- 10) Next Meeting Plans/Meeting Adjourned

B. ATTENDANCE LIST

VOTING MEMBERS

Organization	Name	Email	Telephone
Dept of Commerce (NIST)	Polk, Tim	tim.polk@nist.gov	301.975.3348
Dept of Defense	Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900
Dept of Energy	ABSENT		
Dept of Justice	Woods, Janice	janice.woods@usdoj.gov	202.616.9211
Dept of State	ABSENT		
Dept of the Treasury	Moldenhauer, Michelle (Chair)	michelle.moldenhauer@do.treas.gov	202.622.1110
GSA	Temoshok, David	david.temoshok@gsa.gov	202.208.7655
NASA	DeYoung, Tice	tdeyoung@hq.nasa.gov	202.358.2154
OMB	ABSENT		
USDA/NFC	Sharp, Kathy	kathy.sharp@usda.gov	504.426.0433

OBSERVERS

Organization	Name	Email	Telephone
ACES	ABSENT		
Dept of Defense	Mitchell, Debbie	dmmite3@missi.ncsc.mil	410.854.4900
Dept of the Interior/ Bureau of Land Management	Davis, Russell	russell_davis@blm.gov	202.452.5054
Dept of the Treasury (eValid8)	Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681
FBCA OA Director (GSA)	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923
FBCA OA (Mitretek)	Tate, Darron	darron.tate@mitretek.org	703.610.1905
FICC support (Bearing Point)	Stipisic, Dario	dario.stipisic@bearingpoint.com	703.519.2534
FICC	Petrick, Brant	brant.petrick@gsa.gov	202.208.4673
FICC	Spencer, Judith	judith.spencer@gsa.gov	202.208.6576
FPKIPA Secretary (IATAC)	Lentz, Mark	lentz_mark@bah.com	410.684.6520
GSA	Cornell, John	john.cornell@gsa.gov	202.501.1598
HHS	Alterman, Peter	altermap@mail.nih.gov	301.252..8846
NOAA	McDowell, Gene	eugene.c.mcdowell@noaa.gov	301.713.3333 x207
State of Illinois	ABSENT		
USDA/NFC	Goodwin, Linda	linda.goodwin@usda.gov	504.426.0424

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes:

Ms. Michelle Moldenhauer, FPKIPA Chair, called the meeting to order at 9:45 a.m. with attendee introductions.

Regarding the 13 July 2004 FPKIPA meeting minutes, only editorial comments were mentioned and shared with IATAC after the meeting. Here is the voting record:

Approval vote for 13 July 2004 FPKIPA Meeting Minutes			
Voting members	Vote (Motion – DoD; 2 nd – Commerce)		
	Yes	No	Abstain
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy (proxy by FPKIPA Chair)	X		
Dept of Justice	X		
Dept of State (proxy by FPKIPA Chair)	X		
Dept of Treasury	X		
GSA	X		
NASA	X		
OMB (proxy by FPKIPA Chair)	X		
USDA/NFC	X		

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting:

There were two email votes conducted since the last FPKIPA meeting on 13 July 2004 and the tabulated email vote records were distributed via email prior to the meeting (see Appendix A). The two items voted on via email and their results were:

- 1) 8 June 2004 FPKIPA Meeting Minutes (Vote Request – 07/14/04 / **Approved by a vote of 7 Yes votes and 3 absences out of 10 voting members – 07/27/04**)
- 2) E-Governance CA Certificate Policy – (Vote Request – 07/27/04 / **not sufficient votes collected for majority vote prior to 10 August FPKIPA meeting – 5 Yes votes and 5 absences out of 10 voting members**)

Since there weren't sufficient votes collected to produce a majority vote on the E-Governance CA Certificate Policy via email vote, the votes from the outstanding voting members will be requested at this meeting. Before the vote was taken there was discussion about comments from Mr. Russ Davis, Department of the Interior/Bureau of Land Management. The comments surrounded the issue of the policy requiring CAs to use signature keys of at least 2048 bit keys even though smart cards are not able to validate in hardware any signatures created by 2048 bit keys (See Appendix B). There was discussion about if signature validation is done within the smart card or in software on the computer hosting the smart card. The issue was not sufficiently addressed during the discussion so Mr. Tim Polk volunteered to have a smart card expert from NIST come to the 14 September 2004 FPKIPA meeting to address the comments from Mr. Davis.

ACTION (088): Department of Commerce (NIST) will address the issue about verification of signatures from 2048 bit keys at the 14 September 2004 FPKIPA meeting

The outstanding 5 voting members were requested to vote on the E-Governance CA CP during this meeting, with the following vote results summarizing the email and meeting votes on this topic:

Approval vote for E-Governance CA CP			
Voting members	Vote		
	Yes	No	Abstain
Dept of the Commerce	X - email		
Dept of Defense	X - meeting		
Dept of Energy (proxy by FPKIPA Chair)	X - meeting		
Dept of Justice			X - meeting
Dept of State (proxy by FPKIPA Chair)	X - meeting		
Dept of Treasury	X - email		
GSA	X - email		
NASA	X - email		
OMB	X - email		
USDA/NFC	X - meeting		

Agenda Item 4

Discussion Topic: E-Governance CA CP, Section 2.4.2 – Dispute Resolution

During the 23 July 2004 CPWG meeting, the topic of how dispute resolution is addressed in the E-Governance CA CP was discussed and it was determined that the FPKIPA should discuss and decide if a policy change is necessary. The E-Governance CA CP currently states that the FPKIPA will resolve disputes between entities when conflicts arise as a result of the use of certificates issued under this policy. The recommended policy change would be for the E-Authentication PMO be given the primary responsibility for dispute resolution, since the E-Governance CA will be administered by the E-Authentication PMO.

After some limited discussion on this topic, the attendees agreed in principle to this CP change. A formal change proposal will be developed, forwarded to the FPKIPA mail list for review, and voted on either by email or at the next FPKIPA meeting.

ACTION (089): Dept of Commerce (NIST) will develop a E-Governance CA CP Change Proposal for Section 2.4.2 – Dispute Resolution to make the E-Authentication PMO the mitigating authority for disputes, rather than the FPKIPA, forward it to the FPKIPA mail list for review, and request a vote.

Agenda Item 5

DoD PKI Status Report on PKI Interoperability Requirements and Guidance Research

Ms. Debbie Mitchell, DoD PKI PMO, presented the information (see Appendix C) about the status of the work from a special working group under the DoD PKI PMO, the DoD Federal Bridge Interoperability Project Action Team. This group was formed to discuss, plan, and implement strategy for better positioning DoD for two-way interoperability with the FBCA. This group held their kickoff meeting on 27 April 2004. One of the documents the group envisioned developing was a Standard Operating Procedures document about interoperability with the FBCA, entitled something like, "How To Be an FBCA Cross-Certification Member". However, after some discussion, the group evolved their focus to develop a Risk Mitigation Assessment that included potential benefits to DoD, issues with interoperability with the FBCA, and recommendations to deal with issues associated with cross certification with the FBCA. The target date to achieve two-way cross-certification with the FBCA is December 2004. This will require getting paperwork to DoD management in August 2004.

The FPKIPA is very interested in the progress that this DoD working group is making in this area and would like to hear another status report and see any documentation on this subject that the group produces, in hopes that it will be beneficial to the FPKIPA and other cross-certification members and/or applicants.

Agenda Item 6

Federal Identity Credentialing Committee (FICC) Report:

Ms. Judith Spencer, FICC Chair, reported the following items:

At the last FICC meeting on 7 July, the primary discussion centered around the Identity Assurance Working Group (IAWG) recommendations for the minimum essential requirements and procedures for Federal agencies to follow for in-person identification of federal employees and contractors prior to issuance of a smart card identification badge. Comments on these recommendations were due on 6 August and very few comments were received. Following the appropriate handling of any comments, OPM will write and issue a guidance document for identity proofing requirements. The next IAWG meetings are scheduled for 11 and 25 August.

The Common PKI Policy and the Smart Card Guidance documents were recently approved within the FICC and have been forwarded to OMB for distribution. OMB was set to issue an OMB policy memo to state that these two policy documents will take effect as of May 2005. Now the memo is waiting on White House concurrence and has had to be rewritten based on the content of the 9/11 Commission Report.

The Interim Buy on smart cards is going forward. The Government Smart Card-Interoperability Specification (GSCis) does not address requirements for proximity cards/readers, because the specification is 18 months old. The E-Sign standard (Europe) includes details about proximity cards/readers. The American Transportation Authority (ATA), with the aid of Rob Butler, DoD, has developed a standard called RIS that includes requirements for proximity cards/readers. A meeting was recently held with the DoD Joint Interoperability Test Center (JITC) to request testing using the GSCis standards, middleware, and smart cards and they said they would conduct the testing, conditional on NIST assistance.

The Shared Service Providers (SSP) Subcommittee publicized the Certified Providers List (CPL) for PKI Service Providers on the Federal Identity Credentialing Committee (FICC) web site (<http://www.cio.gov/ficc/cpl.htm>) starting on 6 July. Since the 13 July FPKIPA meeting, Betrusted has successfully passed the SSP criteria and joined the US Department of Agriculture/National Finance Center (USDA/NFC) and VeriSign as the only three organizations on the SSP CPL.

A new working group, the Bridge to Bridge Working Group, met for the first time during the week of 2 August 2004. It was attended by representatives of the Higher Education Bridge Certification Authority (HEBCA), the Pharmaceutical Bridge (“Safebridge”), and the Aerospace Bridge (“Certipath”). Deb Blanchard, Enspier, is providing administrative support for this working group. This group should facilitate more expeditious handling the bridge to bridge interoperability and policy issues facing the FBCA.

Agenda Item 7

FPKI Certificate Policy Working Group (CPWG) Report:

Mr. Tim Polk, CPWG Chair, reported that the CPWG met on 23 July 2004 and addressed comments received on the E-Governance CA CP.

The next CPWG meetings are scheduled for 30 August (replacing a previously scheduled meeting on 2 September), 17 September, and 7 October --- all at NIST North, room 618 starting at 09:30 a.m. The HEBCA CP mapping at the Basic, Medium, and High assurance levels and FBCA CP Change Proposals will be the primary subjects of the 30 August meeting. The agenda for the 17 September and 7 October meetings hasn't been finalized yet, but the Government Printing Office (GPO) and Wells Fargo will be sending their CPs in for mapping soon so they may be topics for these upcoming CPWG meetings.

Agenda Item 8

FBCA Operational Authority (OA) Report:

Status of FBCA Certification & Accreditation (C&A)

Ms. Cheryl Jenkins, FBCA OA Director, reviewed the status of the FBCA Certification & Accreditation, stating the following highlights:

- The FBCA OA has contracted with KPMG to conduct CP/CPS compliance audits for all the CPSs associated with the FBCA CP, Common Policy CP, and the E-Governance CA CP, starting on 8 September 2004.

Status of FBCA/Applicant Cross-Certification Technical Testing:

ACES/AT&T is ready to submit their system for interoperability testing and wants to participate in a teleconference soon with the FBCA OA to coordinate the process and schedule for testing.

The DoD ECA system is scheduled to start interoperability testing on 16 August 2004.

Status of CA Testing:

The FBCA OA didn't have any new information for this portion of their report for this month.

Agenda Item 9

Other Topics:

Action Item Review

Action Items 075 and 078 were closed based on activities in this meeting.

Discussion about Action Item 004 determined that part of it has already been accomplished, so it will be closed and a new action item will be opened for the remaining unfinished work regarding criteria for compliance audits and C&A.

Discussion about Action Item 076 determined that the original intent of the action item is unclear so IATAC will research what Action Item 068 was, since it was referenced in the text of Action Item 076. The Action Item records show the following text for Action Item 068:

068	Compose the Microsoft approval letter for the FPKIPA Chair to sign.	Cheryl Jenkins, GSA	18 Nov 2003	19 Dec 2003	Open
-----	---	---------------------	-------------	-------------	-------------

Agenda Item 10

Next Meeting Plans / Meeting Adjourned:

The next FPKI PA Meeting is scheduled for 14 September 2004 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141B, Washington, DC.

The meeting adjourned at 11:30 a.m.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
004	Define the audit criteria (Web Methods, SAS70, PAG) that will be used to conduct C&A sessions for the FBCA and FBCA OA. 14 January 2003 – This delta report of what is covered by each C&A technique has been deferred until the completion of the FBCA Criteria and Methodology documents.	Tice DeYoung, NASA	08 April 2002 Updated – 14 Jan 2003 Updated – 13 May 2003	13 Jan 2004 FPKIPA meeting	Closed, 10 Aug 2004 FPKIPA meeting
043	Establish policy to reflect the changing interoperability needs of the multiple membrane members, and forward requested changes to Mr. John Cornell for review before sending out to the working group members.	Tim Polk, NIST	13 May 2003	13 Jan 2004 FPKIPA meeting	Open
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	Open
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
061	Incorporate the new FBCA CP Change Proposals (2003-01 through 2003-05) into the FBCA CP, dated 10 September 2002, and forward the resulting FBCA CP to the FPKIPA webmaster for posting to the Federal PKI web sites.	IATAC	9 Sept 2003	31 Dec 2003	Open
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	Open
075	Develop, approve, and forward to the FPKIPA an E-Gov Certificate Policy for Assurance Levels 1 & 2 by 1 October 2004.	FBCA CPWG	9 Mar 2004	1 Oct 2004	Closed, 10 Aug FPKIPA meeting

No.	Action Statement	POC	Start Date	Target Date	Status
076	Check the accuracy of the dates and contact information in the Microsoft agreement (Action Item #68) and then distribute it to the FPKIPA and the CPWG.	FBCA OA	9 Mar 2004	13 Apr 2004 FPKIPA meeting	Open
078	Present a briefing at the 10 August FPKIPA meeting on the status of their PKI interoperability requirements and guidance research.	DoD PAT	11 May 2004	10 Aug 2004 FPKIPA meeting	Closed, 10 Aug FPKIPA meeting
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	Open
087	Once the FPKIPA approves the Department of Labor (DoL) compliance audit letter, request the FPKIPA voting members to submit their approval votes for cross certification of DoL.	IATAC	13 July 2004	10 August 2004 FPKIPA meeting	Open
088	Address the issue about verification of signatures from 2048 bit keys at the 14 September 2004 FPKIPA meeting	Dept of Commerce (NIST)	10 Aug 2004	14 Sept 2004 FPKIPA meeting	Open
089	Develop a E-Governance CA CP Change Proposal for Section 2.4.2 – Dispute Resolution to make the E-Authentication PMO the mitigating authority for disputes, rather than the FPKIPA, forward it to the FPKIPA mail list for review, and request a vote.	Dept of Commerce (NIST)	10 Aug 2004	14 Sept 2004 FPKIPA meeting	Open
090	Define the criteria for FBCA compliance audits and C&A, based on NIST Standards (800-26 and 800-53).	Tice DeYoung, NASA	10 Aug 2004	12 October 2004 FPKIPA meeting	Open

Appendix A:

FPKIPA Email Voting Record (13 July – 9 August 2004)

ORG	8 June 2004 FPKIPA minutes [Requested 07/14/04] [Approved 07/27/04]	Voting Member	E-Gov CA CP [Requested 6/9/04] [Not sufficient votes cast via email]	Voting Member		
<i>Commerce</i>	Y 07/26/04	Polk	Y 07/28/04	Polk		
<i>Defense</i>	Y 07/15/04	Hanko				
<i>Energy</i>						
<i>Justice</i>	Y 07/14/04	Deeley				
<i>State</i>						
<i>Treasury</i>	Y 07/27/04	Moldenhauer	Y 07/30/04	Moldenhauer		
<i>GSA</i>			Y 07/28/04	Temoshok		
<i>NASA</i>	Y 07/14/04	DeYoung	Y 07/30/04	DeYoung		
<i>OMB</i>	Y 07/26/04	Thornton	Y 07/27/04	Thornton		
<i>USDA/NFC</i>	Y 07/26/04	Sharp				

Appendix B:

From: X.509 Certificate Policy for the E-Governance Certification Authorities

6.1.5 Key Sizes and Signature Algorithms

...

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bit keys.

So how will the smartcard validate a 2048-bit signature?



From: X.509 Certificate Policy for the Common Policy Framework

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

Distinguished names based on Internet domain component names shall be in the following directory information trees:

*dc=gov, dc=org0, [dc=org1],...[dc=orgN]
dc=mil, dc=org0, [dc=org1],...[dc=orgN]*

From: X.509 Certificate Policy for the E-Governance Certification Authorities

3.1.1 Types of Names

Names assigned to E-Governance CAs shall be in the following form:

- *C=US, o=U.S. Government, ou=GSA, ou=e-Gov, cn=CAname*

The common name should be descriptive and must include the authentication level supported by the CA.

CSP subscriber names assigned by E-Governance CAs shall be in the following form:

- *C=US, o=Organization, [ou=major unit], [ou=minor unit], cn=CSP name*

Appendix C:



DoD Federal Bridge Interoperability Project Action Team

Debbie Mitchell

DoD PKI PMO

dmmittc3@missi.ncsc.mil



Background – Establishing the Process Action Team and Initial Progress

- Need to Better Position DoD for Two-Way Interoperability with the Federal Bridge
- Kick off Meeting April 27, 2004
 - Voluntary Membership
 - Information Sharing
 - Charter
 - Open Discussion



Results of Follow-on Meetings

- Refined Charter
- Developed “Risk Mitigation Assessment”
 - Executive Summary
 - Background Information
 - Potential Benefits to DoD
 - Issues With Interoperating with the FBCA
 - Recommendations to Deal with Issues
 - Conclusion



Where Are We?

- Risk Mitigation Assessment
 - Process Action Team Coordinated, Reviewed, Finalized
 - Gil Nolte Provided to DoD CIOs
 - Presently Being Reviewed by DoD PKI Business Working Group (BWG)
 - Plans to brief Identity Management Senior Coordinating Group upon BWG Concurrence
- Future Direction
 - Potential for Re-occurring Group
 - Need to Address External Interoperability Beyond the Federal Community