

# Federal Public Key Infrastructure Policy Authority (FPKIPA)

**Minutes of the 13 July 2004 Meeting**  
GSA; 1800 F Street; Room 5141B; Washington, DC

## A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Approval Vote on Minutes from 8 June 2004
- 3) Status of Email Votes Since Last FPKIPA Meeting
- 4) Discussion Topic: Use of PKCS-12
- 5) Federal Identity Credentialing Committee (FICC) Report
- 6) FPKI Certificate Policy Working Group (FPKI CPWG) Report
- 7) FBCA Operational Authority (FBCA OA) Report
- 8) Other Topics
- 9) Next Meeting Plans / Meeting Adjourned

## B. ATTENDANCE LIST

### VOTING MEMBER ORGANIZATIONS

Organization	Name	Email	Telephone
Dept of Commerce (NIST)	Polk, Tim (voter)	tim.polk@nist.gov	301.975.3348
Dept of Defense	Nolte, Gil (voter)	gc nolte@missi.ncsc.mil	410.854.4900
Dept of Energy	ABSENT		
Dept of Justice	Deeley, Kevin (voter #1)	kevin.deeley@usdoj.gov	202.353.2421
Dept of Justice	Woods, Janice (voter #2)	janice.woods@usdoj.gov	202.616.9211
Dept of State	ABSENT		
Dept of the Treasury	Moldenhauer, Michelle (voter) FPKIPA Chair	michelle.moldenhauer@do.treas.gov	202.622.1110
GSA	Temoshok, David (voter)	david.temoshok@gsa.gov	202.208.7655
NASA	DeYoung, Tice (voter)	tdeyoung@hq.nasa.gov	202.358.2154
OMB	ABSENT		
USDA/NFC	Sharp, Kathy (voter)	kathy.sharp@usda.gov	504.426.0433

### OBSERVERS

Organization	Name	Email	Telephone
ACES	ABSENT		
FICC support (BearingPoint)	Stipisic, Dario	dario.stipisic@bearingpoint.com	703.519.2534
FBCA OA (Mitretek)	Tate, Darron	darron.tate@mitretek.org	703.610.1905
FICC	Petrick, Brant	brant.petrick@gsa.gov	202.208.4673
FICC	Spencer, Judith	judith.spencer@gsa.gov	202.208.6576
Dept of Defense	Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900
Dept of the Treasury (eValid8)	Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681
USDA/NFC	Goodwin, Linda	linda.goodwin@usda.gov	504.426.0424
FPKIPA Secretary (IATAC)	Lentz, Mark	lentz_mark@bah.com	410.684.6520
State of Illinois	ABSENT		

## 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 9:35 a.m. with attendee introductions.

Regarding the 8 June 2004 FPKIPA meeting minutes, there was not sufficient time between the delivery of the minutes and this meeting for the voting members to have sufficient review time prior to this vote, so Department of the Treasury made a motion and DoD seconded the motion, to cast an email vote for the 8 June FPKIPA meeting minutes.

### Agenda Item 3

#### **Status of Email Votes Since Last FPKIPA Meeting:**

There were three email votes conducted since the last FPKIPA meeting on 8 June 2004 and the tabulated email vote records were distributed via email prior to the meeting (Appendix A). The three items voted on via email and their results were:

- 1) E-Governance CA Standard Operating Procedures (SOP) document approval - **Approved**
- 2) Common Policy Change Proposal 2004-01 - **Approved**
- 3) Question of whether to remove the requirement for US Citizenship for SSPs - **Denied**

### Agenda Item 4

#### **Discussion Topic: Use of PKCS-12**

Dr. Tice DeYoung, NASA, initiated this agenda item and distributed the discussion points/questions in an email message to the FPKIPA mail list prior to this meeting. (Appendix B)

The primary purpose of this discussion was to have the FPKIPA members share their experiences with PKCS-12 export and what PKI security and cross certification implications may exist.

After some brief discussion in the meeting, it was decided that this issue would be best handled in either a technical working group (e.g. FBCA TWG or FPKI CPWG) or with some of the PKI experienced personnel at NIST. To close out the discussion, it was recommended that NIST take responsibility for doing some analysis in the lab on this subject and make some recommendations to the FPKIPA at a future meeting.

**ACTION (085): Mr. Tim Polk, NIST, will have some testing/evaluation of the PKCS-12 usage issue done and make a recommendation to the FPKIPA at a meeting in the near future.**

## **Agenda Item 5**

### **Federal Identity Credentialing Committee (FICC) Report:**

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

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 will soon be issuing an OMB policy memo that will state that these two policy documents will take effect as of May 2005. Part of the reason that OMB is waiting on distributing this memo and these two policy documents is to not confuse the federal community on this topic since the Homeland Security Council is said to be drafting a similar memo for distribution that states the importance of federal credentialing.

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. So far, the two organizations on the list are US Department of Agriculture/National Finance Center (USDA/NFC) and VeriSign.

At the last FICC meeting on 8 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 are due on 6 August. The next IAWG meeting is scheduled for 11 August. Following the appropriate handling of any comments, OPM will write a rule for identity proofing requirements.

The next Smart Card Working Group meeting is scheduled for 15 July starting at 1:00 p.m. in the GSA Building, 1800 F Street, room 1108 (POC: Tim Baldrige, NASA). One of the main topics of that meeting will be physical interoperability.

## **Agenda Item 6**

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

Mr. Tim Polk, CPWG Chair, led a discussion on one of the matters that had been voted on via email by the FPKIPA voting members since the last meeting – the question of whether to remove the requirement for US citizenship from the Common Policy to accommodate SSPs. The motion to remove the requirement for US citizenship for PKI SSPs was previously rejected by the FPKIPA voting members. At the request of the SSP community, Mr. Polk presented a new proposal removing the citizenship requirement for personnel filling the Operator role.

After some discussion, the attendees unanimously stated that the Common Policy should maintain the requirement for U.S. citizenship for all Trusted Roles at the PKI SSPs. Mr. Polk agreed to communicate this decision to the SSPs.

The next CPWG meeting is scheduled for 23 July at NIST North, room 618 starting at 09:30 a.m. The following meeting was originally scheduled for 2 Sept but that will be cancelled and new dates for future CPWG meetings will be decided at the 23 July meeting.

## Agenda Item 7

### FBCA Operational Authority (OA) Report:

#### Status of FBCA Certification & Accreditation (C&A)

Mr. Darron Tate reviewed the status of the FBCA Certification & Accreditation, stating the following highlights:

- The FBCA OA was granted Full Authority To Operate (FATO) on 1 July 2004, meeting its target goal. The DAA and numerous other people have since congratulated the FBCA OA on this accomplishment.
- There were 8 residual issues outstanding from the C&A of the FBCA OA and they are scheduled to all be addressed by the end of August 2004.

#### Status of FBCA/Applicant Cross-Certification Technical Testing:

Technical testing with Department of Homeland Security (DHS) is still waiting for the establishment of a border directory at DHS.

The only remaining cross certification criteria for Department of Labor (DoL) to complete is approval of their compliance audit letter. The CPWG hasn't approved of this letter yet but once it has it was recommended that the FPKIPA voting members be requested to review it and submit an email approval vote as soon as possible. Also, if that is done prior to the week before the 10 August FPKIPA meeting then it was recommended that the FPKIPA voting members also be requested to submit an email approval vote for cross certification of DoL.

**ACTION (086): CPWG review the Department of Labor (DoL) compliance audit letter and determine if it is sufficient and ready for requesting an FPKIPA approval vote.**

**ACTION (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.**

The FBCA OA reported that the ACES/ORC technical testing has successfully met all the interoperability testing requirements so it was recommended that the FPKIPA vote to approve the ACES/ORC Technical Testing. FPKIPA voted to approve the ACES/ORC Technical Testing, per the following voting record:

Approval vote for ACES/ORC Technical Testing			
Voting members	Vote (Motion – Commerce; 2 <sup>nd</sup> – DoD)		
	Yes	No	Abstain
Dept of 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 the Treasury	X		
GSA			X
NASA	X		
OMB (proxy by FPKIPA Chair)	X		
USDA/NFC	X		

**Status of CA Testing:**

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

**Agenda Item 8**

**Other Topics:**

**Action Item Review**

No changes to the Action Item list were necessary at this time.

**Status on FPKI Adhoc Working Group**

Dr. Tice DeYoung, NASA, reported that on 8 June the first meeting of this group was held in a Department of the Treasury facility and attended by representatives of Department of the Treasury, Department of State, NFC, Entrust, and NASA. The attendees were able to have a productive meeting and provide the Entrust representative, Gary Moore, with the technical information he needed to conduct further analysis of a current problem with path discovery and validation amongst FBCA cross-certification member organizations.

**Agenda Item 9**

**Next Meeting Plans / Meeting Adjourned:**

The next FPKI PA Meeting is scheduled for 10 August 2004 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141B, Washington, DC.

The meeting adjourned at 11:15 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	<b>Open</b> – reassigned to GSA/FTS, Cheryl Jenkins (as of 14 Jan 2003) and Tice DeYoung (13 May 2003)
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	<b>Open</b>
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	<b>Open</b>
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	<b>Open</b>
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	<b>Open</b>
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	<b>Open</b>
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	<b>Open</b>
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	<b>Open</b>

<b>No.</b>	<b>Action Statement</b>	<b>POC</b>	<b>Start Date</b>	<b>Target Date</b>	<b>Status</b>
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	<b>Open</b>
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	<b>Open</b>
081	Brief the status of the establishment of a new FPKI working group for technical/business issues at the 13 July FPKIPA meeting.	Dr. Tice DeYoung, NASA	8 June 2004	13 July 2004 FPKIPA meeting	<b>Closed, 13 July</b>
084	Review the Treasury CP and determine if it allows the practice of changing the reason code in a certificate after that particular certificate has been revoked.	Dept of the Treasury	8 June 2004	10 August 2004 FPKIPA meeting	<b>Closed, 28 July email</b>
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	<b>Open</b>
086	Review the Department of Labor (DoL) compliance audit letter and determine if it is sufficient and ready for requesting an FPKIPA approval vote.	FBCA CPWG	13 July 2004	16 July 2004	<b>Closed, 13 July FPKIPA meeting</b>
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	<b>Open</b>

## Appendix A:

### FPKIPA Email Voting Record (8 June – 12 July 2004)

<b>ORG</b>	<b>E-Gov SOP</b>  [6/9/04]	<b>Voting Member</b>	<b>Common Policy Change Proposal, 2004-01</b>  [6/9/04]	<b>Voting Member</b>	<b>US Citizenship for SSPs</b>  [6/30/04]	<b>Voting Member</b>
<i>Treasury</i>	Y 7/9/04	Moldenhauer			N 7/7/04	Moldenhauer
<i>Commerce</i>	Y 7/8/04	Polk	Y 6/9/04	Polk		
<i>Justice</i>	Y 6/9/04	Burkhous	Y 6/9/04	Burkhous	N 7/6/04	Burkhous
<i>DoD</i>					N 7/7/04	Nolte
<i>GSA</i>	Y 6/9/04	Temoshok			Y 7/7/04	Temoskok
<i>OMB</i>	Y 6/9/04	Thornton	Y 6/9/04	Thornton	Y 7/6/04	Thornton
<i>NASA</i>			Y 6/9/04	DeYoung	N 7/6/04	DeYoung
<i>NFC</i>	Y 7/9/04	Sharp	Y 6/9/04	Sharp	N 7/7/04	Sharp
<i>State</i>						
<i>Energy</i>						

## **Appendix B:**

### **FPKIPA Issue: Use of PKCS-12**

**13 July 2004**

This is the informal poll on PKCS-12 export that was originally provided via email on 21 June 2004 to the Federal PKI Policy Authority members. The purpose is to determine which, if any, agencies are allowing PKCS-12 export and what implications permitting this export have on the security of their PKI and their cross-certification with the FBCA. The questions are numbered, but not prioritized. This poll will help NASA decide what to do about this increasingly important issue:

- (1) Does your agency allow PKCS-12? \_\_\_\_\_  
(If the answer is Yes, please skip the next question).
- (2) If not, was it a technology and/or a policy decision and why?
  - A. Technical reason:
  - B. Policy reason:(Skip to (5))
- (3) If so, how are you handling the exported keys?
  - (A) Centrally managing
  - (B) Distribute management to users
- (4) If so, do you use a special group and/or OID to indicate you are allowing PKCS-12 export?
- (5) Does your agency think that allowing the exporting of PKI keys using the PKCS-12 mechanism could increase the possibility of key compromise or reduce the overall security policy of your PKI?
- (6) Does permitting PKCS-12 export jeopardize an agency's cross-certification with the FBCA?