Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 14 September 2004 Meeting

GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Approval Vote of Minutes from 10 August 2004
3) Status of Email Votes Since Last FPKIPA Meeting
4) Discussion Topic #1: Addressing Russ Davis Comments on E-Gov CA CP
5) Discussion Topic #2: FBCA CP Requirement for US Citizenship
6) Federal Identity Credentialing Committee (FICC) Report
7) FPKI Certificate Policy Working Group (CPWG) Report
8) FBCA Operational Authority (FBCA OA) Report
9) Other Topics
10) Meeting Adjourned / Next Meeting Plans

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	Breland, Mary Ann	maryann.breland@hq.doe.gov	301.903.7245
Dept of Justice	Burkhouse, Marty	martin.t.burkhouse@usdoj.gov	202.616.4574
Dept of State	Cao, Tin	caott@state.gov	202.203.5068
Dept of the Treasury	ABSENT		
GSA	Temoshok, David	david.temoshok@gsa.gov	202.208.7655
NASA	ABSENT		
OMB	ABSENT		
USDA/NFC	ABSENT		

OBSERVERS

Organization	Name	Email	Telephone
ACES	Duncan, Steve	stephen.duncan@gsa.gov	202.708.7626
Dept of Commerce (NIST)	Brown, Chris	chris.j.brown@nist.gov	301.975.4764
Dept of Defense	Mitchell, Debbie	dmmitc3@missi.ncsc.mil	410.854.4900
Dept of Energy (RSIS)	Whiting, Jacob	jacob.whiting@hq.doe.gov	301.903.4857
Dept of Justice	Morrison, Scott	scott.k.morrison@usdoj.gov	202.616.9207
Dept of the Interior	Davis, Russell	russell_davis@blm.gov	202.452.5054
Dept of the Treasury (eValid8)	Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681
E-Auth Lab (Enspier)	Russell, Arthur	arussell@enspier.com	202.208.1235
FICC	Petrick, Brant	brant.petrick@gsa.gov	202.208.4673
FICC	Spencer, Judith	judith.spencer@gsa.gov	202.208.6576
FICC support (Bearing Point)	Stipisic, Dario	dario.stipisic@bearingpoint.com	703.519.2534
FPKIA OA (Mitretek)	Tate, Darron	darron.tate@mitretek.org	703.610.1905
FPKIA OA Director (GSA)	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923
FPKIPA Secretary (IATAC)	Lentz, Mark	lentz_mark@bah.com	410.684.6520
GSA	Cornell, John	john.cornell@gsa.gov	202.501.1598
HEBCA	Faut, Nathan	nfaut@educause.edu	301.335.2656
HHS	Alterman, Peter	altermap@mail.nih.gov	301.252.8846
State of Illinois	Anderson, Mark	mark_anderson@cms.state.il.us	217.558.4859

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes
Mr. Tim Polk, NIST and FPKIPA Co-Chair, called the meeting to order at 9:35 a.m. with attendee introductions.

Regarding the 10 August 2004 FPKIPA meeting minutes, only editorial comments were mentioned and shared with IATAC prior to the meeting. Here is the voting record:

Approval vote for 10 August 2004 FPKIPA Meeting Minutes			
Voting members	**Vote (Motion – Commerce; 2nd – DoD)**		
	Yes	**No**	**Abstain**
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Justice	X		
Dept of State	X		
Dept of Treasury (proxy by FPKIPA Co-Chair)	X		
GSA	X		
NASA (proxy by FPKIPA Co-Chair)	X		
OMB (proxy by FPKIPA Co-Chair)	X		
USDA/NFC (proxy by FPKIPA Co-Chair)	X		

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting
There were not any email votes conducted since the last FPKIPA meeting on 10 August 2004. The Department of Labor (DoL) compliance audit letter was distributed to the FPKIPA voting members for review and vote but it was determined that it was missing some information so the vote request was cancelled until the DoL can resubmit an updated compliance audit letter.

Agenda Item 4

Discussion Topic #1: Addressing Russ Davis Comments on E-Gov CA CP
The comments raised by Mr. Russ Davis, Department of the Interior, Bureau of Land Management, at the 10 August FPKIPA meeting were resolved during discussions between Mr. Davis and NIST representatives prior to this meeting. The conclusion of the discussions were that organizations should meet the E-Gov CA CP requirements with smart cards that abide by GSC-IS new key sizes and hash algorithms should be able to be handled by GSC-IS cards in the future, since software updates will provide new, necessary functionality.

Agenda Item 5

Discussion Topic #2: FBCA CP Requirement for US Citizenship

Background
The Higher Education Bridge Certification Authority (HEBCA), by nature as a collection of educational institutions, hires foreign nationals. In fact, the current full time CA operator with HEBCA is a foreign national from Australia.

The Federal Government's position on requiring U.S. citizens for PKI Trusted Roles is:
1) When the PKI is located on US soil, it is expected that the PKI Authorities/Trusted Roles will be filled by U.S. citizens.
2) When the PKI is on foreign soil, it is expected that the PKI Authorities/Trusted Roles will be filled by citizens of that country (e.g. Canada, UK, Australia, etc.)

Discussion
Dr. Peter Alterman made the following points:
1) Bridges, such as HEBCA, are autonomous piers and thus have different issues to address than independent PKIs.

2) Bridges other than HEBCA also have foreign national participants (e.g. Pharmaceutical bridge, Aerospace bridge, etc.)

3) U.S. Citizenship is not a well-justified requirement for PKI Authorities/Trusted Roles. The other issues mentioned in the FBCA CP, Section 5.3.1 – loyalty, trustworthiness, and integrity – are the more important parts of the requirement.

In dealing with this issue, the requirements for personnel only specify the 4 Trusted Roles, not the Subscribers who receive certificates.

The Department of Defense (DoD) has voiced the strongest opposition to allowing non-U.S. citizens in Trusted Roles. If the FBCA CP is changed to allow non-U.S. citizens to serve in Trusted Roles, then if the DoD has the proper technical capability to do proper bridge certification path discovery and validation for email, web access, and other applications, the DoD would have the freedom within the FBCA model to exclude communications for their subscribers with any PKI or Bridge that is not using U.S. citizens in Trusted Roles.

Requiring U.S. Citizenship will not allow the bridge to operate as freely as technically possible, and may cause PKIs to go to extreme, independent measures to cross-certify with other bridges. For example, if Georgia Tech, whose PKI employs foreign nationals in Trusted Roles and whose personnel perform DoD research, would potentially not be allowed to communicate to DoD PKI subscribers via trust relationships established by the FBCA, if the DoD PKI excludes communications with Georgia Tech PKI subscribers. For the Georgia Tech PKI subscribers to communicate with DoD PKI subscribers, they would have to get certificates issued directly from the DoD PKI or the Georgia Tech PKI would have to cross-certify directly with the DoD PKI.

The question was asked if background checks are done by any of the HEBCA members, to provide some credibility for loyalty, trustworthiness, and integrity. Currently, 3 university members of HEBCA do background checks, consisting of a residence check, criminal check, and credit check. These checks were not considered sufficient checks for the worst-case scenario of a foreign national in a Trusted Role, a foreign exchange student from Iraq who will be going back to Iraq after his graduate/research is over. Similarly, the point was made that U.S. citizenship doesn't guarantee trustworthiness or loyalty to the U.S., because someone like Timothy McVey, who blew up the Federal building in Oklahoma City a few years ago, was a U.S. citizen.

ACTION (091): Peter Alterman, HHS; Tim Polk, NIST; and Judy Spencer, GSA will collaborate on a white paper to summarize the background, discussion points and options to address the U.S. citizenship requirement for Trusted Roles in the FBCA CP, Section 5.3.1. This will be discussed at the next CPWG meeting on 8 October 2004.

Agenda Item 6

Federal Identity Credentialing Committee (FICC) Report
Ms. Judith Spencer, FICC Chair, reported the following items:

Homeland Security Presidential Directive – 12 (HSPD-12) was signed by President Bush on 27 August 2004. NIST has the lead to develop a standard to be implemented by Federal agencies for use by Federal employees and their contractors. The FICC will work with NIST to develop this standard, to be called FIPS 201, and also to help NIST during the implementation/enforcement stages.

Here is the current timetable for the different phases of the standard:

12 Sept 04	Meeting of FICC principals – NIST to present plans for the standard
21 Sept 04	FICC meeting - NIST to present plans for the standard to FICC members
06 Oct 04	Invitation only meeting – NIST to answer questions about this standard
07 Oct 04	Public forum meeting – NIST to answer questions about this standard
08 Nov 04	NIST will publish first public draft of FIPS 201 standard. It will have a 45-day comment period with comments due on 23 Dec
31 Jan 05	FIPS 201 finished
28 Feb 05	FIPS 201 signed and effective
24 June 05	Target date for FIPS 201 Implementation Plans to fit into FY07 budgets or FY06 pass backs to agencies around Nov 2004.

The Interim Aggregate Buy for smart cards is going forward this month. The cost is down to under $10 per smart card. The Aggregate Buy scheduled for December will have more requirements for contactless smart cards.

Ms. Spencer reported that all FICC goals in the FY04 plan have been completed except for the identity assurance part.

Agenda Item 7

FPKI Certificate Policy Working Group (CPWG) Report
Mr. Tim Polk, CPWG Chair, presented the following change proposals for discussion/vote:

1) FBCA CP, Change Proposal 2003-01
2) FBCA CP, Change Proposal 2003-02
3) FBCA CP, Change Proposal 2004-02
4) E-Gov CA CP, Change Proposal 2004-01

Change Proposals 1), 2), and 4) above were approved with 3) being tabled until the week of 20 September for email vote so that the cross-certification members can see if there are any implementation issues for them as a result of approving that change proposal. The following vote records were recorded for change proposals 1), 2), and 4) above:

Approval vote for FBCA CP, Change Proposal 2003-01			
Voting members	**Vote (Motion – Commerce; 2nd – DoD)**		
	Yes	**No**	**Abstain**
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Justice	X		
Dept of State	X		
Dept of Treasury (proxy by FPKIPA Co-Chair)	X		
GSA	X		
NASA (proxy by FPKIPA Co-Chair)	X		
OMB (proxy by FPKIPA Co-Chair)	X		
USDA/NFC (proxy by FPKIPA Co-Chair)	X		

Approval vote for FBCA CP, Change Proposal 2003-02			
Voting members	**Vote (Motion – GSA; 2nd – Justice)**		
	Yes	**No**	**Abstain**
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Justice	X		
Dept of State	X		
Dept of Treasury (proxy by FPKIPA Co-Chair)	X		
GSA	X		
NASA (proxy by FPKIPA Co-Chair)	X		
OMB (proxy by FPKIPA Co-Chair)	X		
USDA/NFC (proxy by FPKIPA Co-Chair)	X		

Approval vote for E-Gov CA CP, Change Proposal 2004-01			
Voting members	**Vote (Motion – Commerce; 2nd – Justice)**		
	Yes	**No**	**Abstain**
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Justice	X		
Dept of State	X		
Dept of Treasury (proxy by FPKIPA Co-Chair)	X		
GSA	X		
NASA (proxy by FPKIPA Co-Chair)	X		
OMB (proxy by FPKIPA Co-Chair)	X		
USDA/NFC (proxy by FPKIPA Co-Chair)	X		

ACTION (092): IATAC will distribute FBCA CP Change Proposal 2004-02 to the FPKIPA voting members for review and email vote during the week of 20 September 2004.

The next CPWG meetings are scheduled for 17 September, and 8 October --- both at NIST North, room 618 starting at 09:30 a.m. The HEBCA CP mapping at the Basic, Medium, and High assurance levels, International issues with the FBCA CP, and another E-Gov CA CP Change Proposal will be the primary topics of the 17 September meeting. The agenda for the 8

October meetings hasn't been finalized yet, but the mapping analysis of the Government Printing Office (GPO) and Wells Fargo CPs will probably be done and may be the topics for that CPWG meeting.

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 term "FBCA OA" is being replaced in documentation with "FPKI Architecture OA (FPKIA OA)", effective immediately.
- The FPKIA OA met with KPMG on 8 September to discuss plans for performing CP/CPS audits. This will be audit of all the CAs under the management of the FPKIA OA – FBCA, Common Policy CA, and the E-Gov CA. KPMG will provide a compliance audit letter based on these audits on 8 October.

Status of FBCA/Applicant Cross-Certification Technical Testing:

Interoperability testing with the Patent & Trademark Office (PTO) is completed.

Testing with the DoD ECA system has begun.

Testing with ACES/AT&T is going well. Cross-certification certificates have been exchanged and directory testing is currently ongoing.

Status of CA Testing:

ACES/DST is on the E-Authentication trust list but not with the same certificate that was used to cross-certify with the FBCA. They are now using a different CA.

Any new SSP vendors will not be able to be tested and issue certificates until after the FPKIA OA audit is completed on 8 October.

A draft RFP is in development to award a contract for the commercial management of the FPKIA OA. The final RFP should be released in early CY2005.

Agenda Item 9

Other Topics

Dr. Peter Alterman, HHS, reported that HHS has done some evaluation testing of CoreStreet products and they found them to successfully demonstrate SCVP path discovery and path validation functionality.

Mr. David Temoshok, GSA, recommended that the topic of annual compliance audits be an agenda item for the 12 October FPKIPA meeting. The main question to discuss would be what

process should the FPKIPA implement for the FBCA cross-certification members to enforce and/or track compliance of this FISMA requirement.

Agenda Item 10

Meeting Adjourned / Next Meeting Plans
The meeting adjourned at 11:50 a.m.

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

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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	**Closed, 27 Sept 2004**
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**
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**

No.	Action Statement	POC	Start Date	Target Date	Status
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	**Closed, 14 Sept FPKIPA meeting**
089	Develop an 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	**Closed, 14 Sept FPKIPA meeting**
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 Oct 2004 FPKIPA meeting	**Open**
091	Collaborate on a white paper to summarize the background, discussion points and options to address the U.S. citizenship requirement for Trusted Roles in the FBCA CP, Section 5.3.1. This will be discussed at the next CPWG meeting on 8 October 2004.	Peter Alterman, NIH; Tim Polk, NIST; and Judy Spencer, GSA	14 Sept 2004	5 Oct 2004	**Closed, 1 Oct 2004**
092	Send FBCA CP Change Proposal 2004-02 to the FPKIPA voting members for review and email vote during the week of 20 September 2004.	IATAC	14 Sept 2004	22 Sept 2004	**Closed, 21 Sept 2004**