Minutes of the 9 September 2008 Meeting

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

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 12 August 2008 FPKIPA Minutes
3. Results of the e-vote on the Wells Fargo Audit Assertion Letter
4. Report on the Four Bridge Forum (4BF) AWG Meeting
5. FPKI Certificate Policy Working Group (CPWG) Report
    a. Discuss / Vote on FBCA CP Change Proposal: 2008-04
    b. Discuss CPWG Recommendation to Map DoD ECA (one-way) at Medium Hardware
6. FPKI Management Authority (FPKI MA) Report
7. Discuss Cross-Certification of Non-Federal Clones at High
8. Discuss / Vote on AAAE Application to Cross Certify with the Federal Bridge at Rudimentary, Basic, Medium (for devices) and Medium Hardware
9. Final Meeting Items
    a. Other Topics
    b. Proposed Agenda Items for the next FPKIPA meeting, 14 October 2008
        - Discuss / Vote on CPWG Recommendation to Map DoD ECA (one-way) at Medium Hardware
        - Review / Vote on CPWG Recommendation to Cross-Certify the DoS
        - Revised FBCA CP Change Proposal/"straw man." 2008-04 (cross-certification of non-federal clones at High)
        - Discuss / Vote on the AAAE Cross-Certification Application
        - FPKI MA Test Environment Proposal (to accommodate test OIDs)
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began without a quorum, (8/15 or 53.3%) where a two-thirds majority was required. DoD joined the teleconference one hour into the meeting, at 10:50 a.m., resulting in 9 of 15 members present, or 60% (still not a quorum). The meeting continued, but the FPKIPA was not able to conduct votes since there was no quorum.

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	O'Brien, Shawn	Teleconference
Department of Health & Human Services	Proxy to GSA	
Department of Homeland Security	Gallagher, Deborah	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark A.	
Department of Treasury	ABSENT	
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA -Alternate	Spencer, Judith	
NASA -Alternate	ABSENT	
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	ABSENT	

OBSERVERS

Organization	Name	Telephone
FPKI MA PM/GSA	Jenkins, Cheryl	Teleconference
GSA	Murdock, Rachael	
State of Illinois	Anderson, Mark	Teleconference
AAAE	Bishoff, Dallas	
IdenTrust	Wilson, Ben	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
IdenTrust	Schambach, Marco	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
GSA	Cornell, John	Teleconference
FPKI/FICC Support (Contractor--FC Business Systems LLC)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
FPKI PA Support/Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	
FPKI MA Technical Lead (Contractor, Protiviti Government Services)	Brown, Wendy	
eValid8	Dilley, Brian	
DHS (Contractor)	Shomo, Larry	Teleconference

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 9:44 a.m. and conducted introductions of those present in person and via teleconference.

Agenda Item 2

Discussion / Vote on 12 August 2008 FPKIPA Minutes—Judith Fincher

Ms. Fincher displayed the redline minutes on the screen and said that comments from David Sulser, Brant Petrick, Mark Stepongzi and Charles Froehlich had been incorporated. The FPKIPA did not vote on the minutes because there was no quorum. Ms. Fincher will issue the updated minutes for 12 August 2008 for an e-vote later this week.

Agenda Item 3

Results of the e-vote on the Wells Fargo Audit Assertion Letter—Judith Fincher

Ms. Fincher said that the e-vote to approve the Wells Fargo Audit Assertion Letter passed by 78.5%, or 11/14, where a 75% majority vote of votes cast was required. Those agencies voting, "Yes," were DOS, HHS, GSA, DHS, GPO, USPS, NASA, NRC, Justice, DEA CSOS, and Treasury. "No" votes were cast by DoD, SSA and Commerce. USPTO did not vote.

The discussion then turned to the issue of cross-certification of Wells Fargo. Ms. Spencer said that the FPKIPA had accepted the mapping and had approved the audit letter. No interoperability testing is required since Wells had not changed products. Because the FPKIPA could not vote to cross certify Wells Fargo at Medium Hardware, et al., due to lack of a quorum, Ms. Spencer decided to conduct an e-vote, since Wells Fargo has been waiting in the queue for such a long time. The question of having a formal recommendation to cross certify from the CPWG was raised, and an attempt to clarify the need for such a document / action was made. Because the requirement could not be confirmed[1], it was determined that the CPWG would prepare a memo to circulate with the e-vote.

Agenda Item 4

Report on the Four Bridge Forum (4BF) AWG Meeting—John Cornell

[1] It was determined after the meeting that neither the Charter, By-laws, nor the Criteria and Methodology require a formal recommendation in the form of a memo. However, the CPWG is required, IAW the Criteria and Methodology to provide (1) a formal Certificate Policy Mapping Report; (2) an Auditor Letter of Compliance and Compliance Review Report; and, (3) an Operational Parameters Analysis Report; the FPKI MA is required, also IAW the Criteria and Methodology to provide a Technical Analysis Report to the FPKIPA Chair, who may then call for a vote. The documentation provided by the FPKI MA and CPWG and a record of the discussion and vote are kept in the Minutes of the FPKIPA meeting.

John Cornell reported on the August 21, 2008 meeting of the audit working groups of three members of the 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 the outcome of that meeting was that the meeting agreed on the content of the PKI Audit Guidelines document drafted by Vijay Takanti, as modified during the 4BF AWG meeting.

In addition, John Cornell and Vijay Takanti agreed to 'join' the FPKI "Audit Cook Book" and the CertiPath audit letter templates and attach the 'agreed upon joint expectation' to the PKI Guidelines document.

WebTrust for CAs (WTCA) was presented by Mark Lundin, chair of the WTCA Audit Task Force. He agreed to shepherd through changes to the WTCA documentation in response to 4BF requirements and concerns. The 4BF AWG will review the updated WebTrust model early next year and will determine then whether the revised WTCA assessment methodology meets the 4BF criteria.

The 4BF agreed that we need a 'Guidelines document' for CPS authors, which makes it clear the expectation of the Bridge PKI PA/PMA. DoD expressed concern on the 'depth of assessment' issue. Consequently, DoD is funding Santosh Chokhani to develop the first set of guidelines. DoD will develop the document, internally coordinate it, and then provide it to the 4BF community for review and comment.

Agenda Item 5

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

a. Discuss / Vote on FBCA CP Change Proposal: 2008-04
   The FPKIPA debated the merits of this change proposal. It was tabled after protracted discussion later during the meeting, and will be discussed at a future CPWG meeting. (See Agenda Item 7)

b. Discuss CPWG Recommendation to Map DoD ECA (one-way) at Medium Hardware

   The FPKIPA could not vote on the Mapping recommendation because DoD needs to fix "exception" language and get the approval of the CPWG at the 16 September 2008 CPWG meeting. It is not clear whether the DoD ECA falls under the same exemption as does the DoD Root CA, (e.g., continued internal use of 1024-bit certs after 12/31/2010). Vivian Shirley of the DoD PKI PMO (Contractor, Booz Allen) has been asked by the CPWG to quantify the impact of such use.

Agenda Item 6

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

1. Wendy Brown described the Change Proposal submitted prior to the meeting and asked the FPKIPA to vote to make the SIA extension optional. NIST concurs with this request. Since there were no objections and NIST cannot identify any existing users of this extension (not even Microsoft), the Secretariat will issue an e-vote later this week.

2. Although DoS has successfully completed interoperability testing of its CAs, the testing of its future directory infrastructure is incomplete pending FPKI MA receipt of a patch from their vendor to correct an interoperability issue. The patch has been received, and the FPKI MA is prepared to re-start directory testing. The FPKI MA recommends cross certification using the existing directory infrastructure. DoS is moving forward with a modification to their existing MOA.

   The DOS has satisfied all remaining hurdles to Cross-Certification. Charles Froehlich, Co-Chair of the CPWG, is drafting a template cross-certification recommendation for consideration by the CPWG, as a revised procedure, which would be considered for incorporation into the soon-to-be-revised Crits and Methods. This template will support e-voting on both the Wells Fargo and DoS cross certification issues.[2]

1- Ms. Brown reported that DoD ECA has requested interoperability testing with their new 2048-bit CA (but not the 1024-bit CA).
2- Ms. Brown said the FPKI MA is drafting a White Paper on the FPKI MA's plans to add support for SHA 256; however, they intend to continue to sign with SHA-1 until the deadline.
3- She said the FPKI MA is putting together a list of equipment for this FY for the re-design effort.
4- The FPKI MA met with Judy Spencer and Adobe about Adobe's plan to establish an Adobe Approved Trust List (AATL), and their desire to re-populate it with the Common Policy Root certificate. Adobe would like this AATL to be restricted only to trusting signatures issued with Medium Hardware or High assurance levels. However, the Common Policy Root certificate contains additional policy OIDs. Therefore, Adobe needs to investigate how they will implement the AATL support to filter on specific policies as well as the root certificates in the AATL.
5- Ms. Brown said the FPKI MA is developing a plan to support a more robust testing environment with the Redesign, given the reluctance, so far, for the affiliates to fully-support the proposed test environment.

Agenda Item 7

Discuss Cross-Certification of Non-Federal Clones at High—David Sulser

Two commercial SSPs (VeriSign and Verizon Business) want to come in at the "High" Assurance level, and the CPWG has begun the mapping for the requested LOAs. The issue is do we want SSPs to issue cross certs with the Bridge at High?

[2] The template will summarize the previously issued reports identified in the Criteria and Methodology document—Certificate Policy Mapping Report, Auditor Letter of Compliance and Compliance Review Report, Operational Parameters Analysis Report, and Technical Analysis Report.

David Sulser introduced prepared remarks into the record to address the issue of Commercial High Assurance PKI Providers:

1. "A State, local, or tribal government is entitled under Federal Bridge policy to operate a High Assurance PKI and apply for cross-certification with the Bridge. Once a need is identified, where should they turn for a solution?

2. A number of State government offices have shown a desire to interoperate with the Federal PKI hierarchy and policies by contracting with approved vendors for SSP-like services.

3. Commercial SSPs are authorized to operate Common High PKIs on behalf of Federal agencies.

4. By seeking cross-certification at the intermediate policy CA level, along the lines of the SSP model, vendors hope to offer better value to their subordinate CA customers, including Federal agencies issuing non-PIV certificates by relieving those customers of the burden of individual cross-certification.

5. Government-side policy direction as expressed in OMB M-04-04 is for organizations to rely on proven, tested commercial PKI providers with shared infrastructure, rather than implementing and operating all required infrastructure internally, e.g., state and local governments.

6. Commercial SSPs operate infrastructure that is tested by GSA security certification processes and monitored under FISMA reporting procedures.

7. When a State, local or tribal government identifies a need for a High Assurance PKI, would the Policy Authority prefer they implement entirely in-house and then apply for cross-certification with the Bridge, or seek the services of a cross-certified SSP clone provider?"

In the discussion that followed, members struggled with the pros and cons of opening the FPKIPA to cross-certification with non-Federal entities at High Assurance. Currently, the High Assurance policy is reserved for government (federal, state, local, and tribal) use. This was done when the Commercial Best Practices matrices were introduced, Ms. Spencer said.

Charles Froehlich: In a co-mingled environment, such as the non-federal PKI clone service from VeriSign or Verizon Business, what kind of guarantees are in place to ensure that High Assurance certs will only go to government employees and their contractors. Our mapping tables do not address this consideration now.

Brian Dilley: There are policy differences between Federal and commercial offerings. You are headed down a "slippery slope" when the two are co-housed.

ACTION: The CPWG will evaluate documentation and talk with VeriSign and Verizon Business to see how they would delimit boundaries and guarantee that certs will only go to government.

Judith Spencer said that an SSP can run at High to support Federal agencies, e.g., VeriSign at NRC. Alternatively, we could limit "high" just to the Federal PKI environment. We need a

compelling reason why the states need High. We could limit them to Medium Hardware and address High when a state or local entity really needs it, she said.

There may be some confusion as to what an entity means by "high." FPKI High and FPKI Medium Hardware are both equivalent to E-Auth Level 4, she said. FRAC needs Medium Hardware, for example. At least one of our cross-certified Bridge partners is opposed to letting our non-federal clones issue at FPKI High. However, if we cannot allow non-federal clones to issue at High, we cannot provide High to the states. It is an "all or nothing" thing.

Charles Froehlich noted that it is very likely that state, local, and tribal governments would shy away from High Assurance once they realized the onerous requirements associated with it, such as having to renew certificates in-person every three years, vice every nine with Medium Hardware.

There is also some indication that FRAC wants FPKI High, according to Brian Dilley.

ACTION: Deborah Gallagher will check with DHS to verify the FRAC requirement.

Judith Spencer: The Federal Bridge "High" is an animal of our own making. It only applies in context to its relationship with Bridge. Who will we enter into relationship at Federal High? We could cross certify non-federal clones at Medium Hardware while they might be operating at Medium Hardware or High. There is also the question of cross certifying allied and coalition partners at High Assurance.

David Sulser: Another approach is to require non-federal SSP PKI clones to identify all their "high" customers and enforce that separation through policy.

Shawn O'Brien joined the call at this point and stated that DoD (Debbie Mitchell) wishes to prepare "talking points" on this issue, to be distributed to the FPKIPA listserv.

Judith Spencer: Ms. Spencer reported on the Committee for National Security Systems (CNSS) PKI WG, previously referred to as the "classified PKI WG." The CNSS has recommended a hierarchical architecture. NSA would fund and operate the C-PKI root under which all other entities – initially DoD, DoJ (FBI), and DoS would subordinate, except DoD and FBI who have their own classified PKIs—until they can transition to the CNSS model.

There is already an intelligence community or Intel PKI in place. The CNSS addresses the gap between the unclassified FPKI Bridge and the highly classified Intel system.

Agenda Item 8

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

The Security Biometric Clearing Network (SBCN) submitted an application 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. TSA is the sponsoring organization. The SBCN was represented at this meeting by Dallas Bishoff, the compliance auditor. The SBCN wants to issue ACIS cards to airport workers, including

pilots, and to be interoperable with FRAC. (ACIS is the Airport Credentialing Interface Specification). FRAC represents the emergency responders.

The AAAE is the industry trade association supported by DAON, a biometric company founded in Ireland. SBCN is a joint venture company composed of DAON and AAAE. It operates the CA to provide the PKI infrastructure for the Registered Traveler program, which uses digitally signed certificates on the smart cards it issues.

The FPKIPA asked the SBCN to provide a contact at the TSA to validate this request. The FPKIPA also requested that SBCN (Mr. Patrick Osborne) provide a justification for cross-certification at all four assurance levels. TSA has a draft ACIS spec and it is unclear how many levels will be specified.

The FPKIPA anticipates being able to vote on this application at the 14 October meeting, provided the requested information is provided in a satisfactory manner.

Agenda Item 9

Final Meeting Items

a. Other Topics
   1) Proposed Agenda Items for the next FPKIPA meeting, 14 October 2008
      1. Discuss / Vote on CPWG Recommendation to Map DoD ECA (one-way) at Medium Hardware
      2. Review / Vote on CPWG Recommendation to Cross-Certify the DoS
      3. Revised FBCA CP Change Proposal/"straw man": 2008-04 (cross-certification of non-federal clones at High)
      4. Discuss / Vote on the AAAE Cross-Certification Application
      5. FPKI MA Test Environment Proposal (to accommodate test OIDs)

Action Item 10

Adjourn Meeting

Ms. Spencer adjourned the meeting at 11:37 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

No.	Action Statement	POC	Start Date	Target Date	Status
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
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