Federal Public Key Infrastructure Policy Authority (FPKIPA)
FBCA Technical Working Group (FBCA-TWG)
Minutes
20 July 2006 Meeting

GSA, 2011 Crystal Drive (Crystal Park 1), 11th Floor Conference Room
Arlington VA 22202

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) SSP Certificate Implementation Guidance
3) Requirements for Test Environment (RTE)
4) Proposed Changes to the FPKI Architecture
5) Bridge-Enabled Validation Solutions
6) Other Topics
   a. Score Card
   b. Next FBCA-TWG Meeting
7) Adjourn Meeting

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Federal Entities			
DOJ	Morrison, Scott	Scott.k.morrison@usdoj.gov	202-616-9207
DOJ	Young, Siegfreid	Siegfreid.f.young@usdoj.gov Or syoung@hpti.com	Teleconference 202-616-8989
USPTO	Purcell, Art	art.purcell@uspto.gov	571-272-5354
USPTO (contractor)	Jain, Amit	Amit.jain@gd-ns.com	571-438-6309
GSA (Co-Chair)	Jenkins, Cheryl	Cheryl.jenkins@gsa.gov	571-259-9923
FPKI/FICC (FC Business Systems)	Petrick, Brant	Brant.Petrick@gsa.gov	202-208-4673
NIST	Cooper, David	David.cooper@nist.gov	301-975-3194
Dept. of State (DoS)	Edmonds, Deborah D.	EdmondsDD@state.gov	202-203-5140
Dept. of State (DoS)	Head, Derrick	headdL@state.gov	202-203-5059
DoD PKI PMO (contractor)	Chokhani, Santosh	CHOKHANI@Orionsec.com	703-917-0060 x 35
DoD PKI PMO	Mitchell, Debbie	dmmitc3@missi.ncsc.mil	410-854-4900
DoD PKI PMO (contractor)	Nielsen, Rebecca	Nielsen_rebecca@bah.com	703-902-6985
USPTO/GD-NS (contractor)	McCain, Greg	Gregory.a.mccain@gdit.com	703-346-0196

Organization	Name	Email	Telephone
Non-Federal Entities			
DST/Identrus	Newman, Justin	Justin.newman@identrus.com	301-674-5282
DST/Identrus	Young, Kenny	Kenny.Young@identrus.com	240-447-7437
Secretariat (Enspier)	Fincher, Judy	Judith.fincher@enspier.com	703-299-4709 (direct line) 703-795-8946 (cell)
Enspier	Pinegar, Tim	Tim.pinegar@enspier.com	571-643-2944 (cell)

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions—Ms. Cheryl Jenkins
This meeting took place at the GSA/E-Authentication PMO Office (GSA, 2011 Crystal Drive (Crystal Park 1), 11th Floor Conference Room, Arlington, VA 22202. Ms. Cheryl Jenkins, Co-Chair, called the meeting to order at 9:40 a.m. with attendee introductions.

Agenda Item 2

SSP Certificate Implementation Guidance—Ms. Cheryl Jenkins (for Andrew Lins)

Ms. Jenkins explained that Andrew Lins was ill and could not make the presentations he was scheduled to deliver today.

Prior to the meeting, she distributed the paper, Implementation Guidance for the X.509 Certificate and Certificate Revolution List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program.

This paper is the product of an action item from the January 26, 2006 FBCA-TWG meeting. At that meeting it was agreed that the FBCA TWG needs to develop a guidance document on the U.S. Federal PKI Common Policy Framework Certificate Profile for the agencies and post it to the web site.

At the July 20 meeting Ms. Jenkins stated that she wanted to post this guidance on the FBCA web site as the product of the FBCA-TWG, once it receives the blessing of the FPKI Policy Authority (FPKIPA). She asked if there was a consensus of the meeting participants to accept the document, as written.

This question sparked a lengthy discussion as to the intended audience for the paper, e.g., the Relying Parties (RPs) —not the Certificate Authorities (CAs). Anyone using the Common Policy root as their Trust Anchor would use this guidance, according to Dave Cooper. Santosh Chokhani restated this: "The paper is intended for use by RP apps that use the Common Policy Root as their Trust Anchor."

Santosh Chokhani "If the CA is cross certified at Medium, and the end entity certificate asserts High, the path will not be valid for any policy."

Santosh Chokhani: "I do not agree with single assertion. They will fail legitimate Path Validation if you have a single OID. In an enterprise environment this is problematic; this gets more complicated in a cross-certified environment."

Santosh Chokhani expressed his concern that this guidance will not enable interoperability. He stated that he had expressed this point of view in an email to Tim Polk and Dave Cooper six months ago, but had not had a response.

Justin Newman proposed a scope statement: "The scope of this paper is to develop guidelines for application owners who are configuring applications to accept digital certs utilizing the Common Policy Root as their Trust Anchor— specifically, to discuss Common Policy OIDs, the applicable FBCA OIDs and applicable E-Authentication levels."

Dave Cooper said that this paper comes from the wrong direction. This paper is all about how CAs should issue certs, not about what RPs should do. This document is for CAs. It doesn't help the RPs. "There's nothing that tell you, for example, if I need E-auth Level 3, here's the OIDs I need to assert." This is complicated by the fact that some OIDs in the FBCA CP don't have a counterpart in the Common Policy. For example, there are no FBCA Basic and Rudimentary OIDs in the Common Policy. So, if you only accept Common Policy OIDs, they will only be asserted as the Medium Level and above. For SSPs using the Common Policy Root as their Trust Anchor, this document is telling them how to issue certs, not how to accept them.

Justin Newman said that the tables and outline are 80% there for RPs. But, the language surrounding those tables is directed toward CAs. It doesn't make sense from an RP perspective.

Ms. Jenkins summarized: We will red-line this document to take out the CA issuance language and address it to RPs only. The document will be from the RP point of view and will use E-auth levels to determine for each level which policies should be used. It will address policy only.

The meeting consensus was to refocus the paper to emphasize the role of RPs and give it another title: Implementation Guidance for Relying Parties (RPs) using the Common Policy Root: Acceptable Policies.

Ms. Jenkins stated that Dr. Fisher will be revising this document and that it will be reviewed again by the FBCA-TWG before it is sent up to the FPKIPA for approval.

ACTION: Cheryl Jenkins will publish the Implementation Guidance for Relying Parties (RPs) using the Common Policy Root: Acceptable Policies to the FBCA-TWG listserv prior to the August FBCA-TWG meeting.

Agenda Item 3

Requirements for Test Environment (RTE)—Cheryl Jenkins (for Andrew Lins)

Prior to the meeting, Ms. Jenkins distributed a paper, Test Environment Requirements. Ms. Jenkins led the discussion of this paper at the July 20 FBCA-TWG meeting in the absence of Andrew Lins.

After much discussion, the FBCA-TWG agreed to remove Item No. 1 and add a new requirement (No. 6) and to re-title the paper, Test Guidelines for the OA Test Environment.

Regarding removal of Item No. 1 and the addition of Item No. 6:
Setting up a mirror image test environment of the production environment was not acceptable to FBCA-TWG members, nor to the FPKIPA, whose members weighed in on this topic with Dr. Peter Alterman, Chair of the FPKIPA.

Cheryl Jenkins explained the rationale for No. 1. We can't have people testing test OIDs in the production environment. Therefore, we need the OA test lab to be a mirror of the production environment. We need a test environment to hammer out things. For example, Treasury is having problems with two applications (DHS and DoD) and needs a test environment.

Santosh Chokhani commented on the DoD environment. DoD has 20 CAs, he stated. DoD has a test infrastructure, but not all 20 CAs are represented. We don't need CA's in the test environment. In the test environment each cross-certified PKI should make available certs and CRLs for testing and OCSP responders.

Rebecca Nielsen: We need to ask what are the artifacts of the CAs.

Justin Newman: You don't need the exact same CA in the test environment.

Justin Newman: Nos. 4 and 5 are required, but that you may need only representative CAs (No. 3). Regarding No. 2, he agreed that the profiles need to mesh.

Rebecca Nielsen: We use test systems as the final test before it is put into production. The Directories need to be similar versions. They interact with things the CA produces. We need a set of those things. For example, the DN structure should look the same. The DNs need not be identical—just the same structure.

Cheryl Jenkins: Some DNs worked fine in the lab, but didn't work in the production environment.

Cheryl Jenkins: If we were to get rid of Requirement No. 1, would that lower costs and resource requirements tremendously?

Santosh Chokhani: For DoD, that is a big cost item.

Dave Cooper wanted to know about the DoD's huge CRLs.

Santosh Chokhani: I'm OK with 2, 3, 4, but No. 5 should be "equivalent to the "test policy OIDs," not "production policy OIDs."

Justin Newman: Should everyone use test OIDs?

Santosh Chokhani: DoD doesn't have sufficient test OIDs.

Dave Cooper: For every policy OID, we can assign a test OID. Then everything would work the same as in the production environment.

Cheryl Jenkins: We need buy-in from the Policy Authority members as to whether they will use test OIDs.

Cheryl Jenkins explained where E-Auth is headed: You must have a PD-Val product to validate a cert or we won't test with you. The first question we ask is, What is your validation product? We need to know it works correctly with the FPKI and Federation architecture.

Justin Newman: Whatever validation mechanisms are exposed or identified in production should be exposed in the test environment.

Cheryl Jenkins: What do we need to do to make that happen?

Justin Newman proposed adding Requirement No. 6: "Certificate revocation information must be made available in the test environment, using the same validation mechanism as in the production environment."

The FBCA-TWG agreed to this change.

Cheryl Jenkins: How quickly can we get this up?

Justin Newman: This is a first step. If the Policy Authority approves this test policy, is this an all or nothing thing?

Cheryl Jenkins: I met with the Policy Authority Chair (Dr. Peter Alterman) to discuss this testing proposal. He couldn't live with No. 1, based on feedback he had received from FPKIPA members. He agreed we should be able to stand up something similar and be able to do good testing.

Cheryl Jenkins: We will re-write the testing proposal and eliminate No. 1, keep Nos. 2, 3, 4 5, and add No. 6 (as Justin Newman proposed).

Scott Morrison: There will be some costs at DOJ to get this up. We will have to stand up a test Border Directory. If the Policy Authority makes this a requirement, that will justify us going forward.

Cheryl Jenkins: If it doesn't have warranties, we don't care, but we need a SLA between the OA and all cross-certified agencies regarding their test environments.

ACTION: Justin Newman will provide an SLA template for the OA to use.

There then ensued a discussion regarding the availability of the directory for the test environment. It was agreed to use 80% availability during "normal business hours" or an equivalent of two months per year.

Rebecca Nielsen: We will also need notification for scheduled down times.

Someone asked how availability would be measured, but this was not addressed directly.

Debbie Mitchell: If the Bridge isn't up, no one can do anything in the test environment.

Cheryl Jenkins: Availability for the FBCA and cross-certified entities is 90%. We will set the bar high and make adjustments if needed.

The FBCA-TWG then discussed the potential need for a C&A for the test environment.

Debbie Mitchell. A Border Directory is expensive in terms of labor required and the C&A process.

Cheryl Jenkins questioned whether a C&A would be required for a test environment.

Scott Morrison stated that the DOJ Border Directory would be located within the DMZ, along with the other boxes. This is an "operational environment" and as such would require a C&A.

Cheryl Jenkins: This C&A requirement is the kind of thing that will prohibit us from moving forward.

ACTION: Cheryl Jenkins will talk with the CIOs of the federal cross-certified agencies to determine if a C&A would be required for the OA test environment.

Cheryl Jenkins: A non-operational box doesn't need a C&A. Some DAAs may not think this is an issue. The issue is: how to deploy a test environment and maintain your accreditation.

Cheryl Jenkins: The agencies need to review the revised OA test requirements and determine the operational impacts and costs. She needs this feedback before the Policy Authority reviews the revised draft of the OA test requirements, entitled: Test Guidelines for the OA Test Environment.

ACTION: Federal Bridge cross-certified agencies need to review the revised OA test requirements document, Test Guidelines for the OA Test Environment, and determine the operational impacts and costs. This feedback is required before the next FBCA-TWG meeting in August 2006.

Cheryl Jenkins: Show me how you would implement the test environment at nominal costs.

Agenda Item 4

Proposed Changes to the FPKI Architecture—Cheryl Jenkins (for Andrew Lins)

Prior to the meeting, Ms. Jenkins distributed a PowerPoint presentation, Proposed FPKIA Re-Design: Current Architecture and Proposed Changes, July 2006. In Andrew Lins' absence, Ms. Jenkins reported on the proposed changes. The changed architecture has its origins in a proposal from Scott Rea of HEBCA and guidance from Rich Guida.

Dave Cooper wanted to know the timeframe for implementation of the new architecture. Why re-issue certs with the SIA extension (a current activity) if the architecture will be changing and new cross-certs will be required?

Ms. Jenkins responded that the current cert re-issuance process (for the SIA extension activity) is appropriate since the timeframe for the new architecture is 1Q07. She expects to get the ATO in June 2007 and to re-issue the cross certs in the August 2007 timeframe.

Ms. Jenkins described the three key changes to re-design and streamline the FPKI Architecture:

- Directory Consolidation of the LDAP and DSP directories into one directory
- CA Consolidation—the current Bridge membrane architecture has four separate CA boxes. New products permit running multiple CAs on one box.
- DN information for CAs will be changed to better represent FPKI.

Ms. Jenkins described an issue that will be referred to the FPKIPA. NIST wrote a recommendation to the E-Auth PMO (page 5 of the PowerPoint presentation) that directory replication would be used to replace chaining. Ms. Jenkins will recommend this approach to the FPKIPA and pointed out that the FPKIPA MOA template will need to be modified.

ACTION: Each FBCA-TWG representative of cross-certified entities should meet with his/her directory experts to review the proposed new architecture and these directory experts should attend the August FBCA-TWG where these three proposed changes and directory replication will be discussed.

Agenda Item 5

Bridge-Enabled Validation Solutions—Ms. Cheryl Jenkins (for Andrew Lins)

This topic was not discussed in depth due to the absence of its champion, Dr. Tice DeYoung, who wants to see the Federal PKI Architecture have a validation solution within it and a centralized OCSP Responder, Ms. Jenkins reported.

This topic will be put on the August FBCA-TWG agenda.

Justin Newman wanted the FBCA-TWG to have a legal discussion on having the government respond on behalf of commercial entities.

Agenda Item 6

Other Topics

a) Score Card—Cheryl Jenkins

Ms. Jenkins proposed that she post Score Card (Red, Yellow, Green) information on the performance of cross-certified entities on the public web site to encourage Program Managers to take more responsibility for compliance with OA requirements. The MOA language is too vague to enforce compliance with OA operations, she said. People don't want to be reviewed negatively.

Justin Newman and Rebecca Nielsen objected to posting the Score Card on the public web site, arguing that it should be used as an internal tracking mechanism and should be included in the OA's Monthly Statistical Report.

ACTION: Ms. Jenkins agreed to include the Score Card in the next Monthly Statistical Report and try it for a couple of months to see how it works.

b) FBCA-TWG Meetings

The next FBCA-TWG meeting will be scheduled for August. Ms. Jenkins will invite the Co-Chair, Tice DeYoung, to report on Bridge-Enabled Validation Solutions.

Agenda Item 7

Adjourn Meeting

The meeting was adjourned at 12:12 p.m.

Action Item List

No.	Action Statement	POC	Start Date	Target Date	Status
003	The FBCA-TWG needs to issue to the listserv strategies, approaches to mitigate the costs of re-keying, and schedule an additional meeting on this issue to resolve it.	FBCA-TWB	1-26-06	March 06	Open
004	Each FBCA-TWG representative of cross-certified entities should meet with his/her directory experts to review the proposed new architecture and these directory experts should attend the August FBCA-TWG where these three proposed changes and	FBCA-TWG	7-21-06	August 06	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	directory replication will be discussed.				
005	Cheryl Jenkins will publish the Implementation Guidance for Relying Parties (RPs) using the Common Policy Root: Acceptable Policies to the FBCA-TWG listserv prior to the August FBCA-TWG meeting.	Cheryl Jenkins	7-21-06	August 06	Open
006	Ms. Jenkins agreed to include the Score Card in the next Monthly Statistical Report and try it for a couple of months to see how it works.	Cheryl Jenkins	7-21-906	Oct. 2006	Open
007	Justin Newman will provide an SLA template for the OA to use.	Justin Newman	7-21-06	7-28-06	Open
008	Cheryl Jenkins will talk with the CIOs of the federal cross-certified agencies to determine if a C&A would be required for the OA test environment.	Cheryl Jenkins	7-21-06	August 2006	Open
009	Federal Bridge cross-certified agencies need to review the revised OA test requirements document, Test Guidelines for the OA Test Environment, and determine the operational impacts and costs. This feedback is required before the next FBCA-TWG meeting in August 2006.	FBCA Cross-Certified entities	7-21-06	August 2006	Open