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

GSA NCR, 7th and D Streets, SW, Washington, DC
Room 5060

1. AGENDA

1. Welcome & Opening Remarks / Introductions
2. Directory Replication
3. Requirements for Test Environments
4. Implementation Guidance for Relying Parties (RPs) using the Common Policy Root
5. Signed E-Mail between CSPs and the OA
6. Other Topics
7. Adjourn Meeting

2. ATTENDANCE LIST

Organization	Name	Email	Telephone
Federal Entities			
DOJ	Morrison, Scott	Scott.k.morrison@usdoj.gov	202-616-9207
USPTO (contractor)	Jain, Amit	Amit.jain@gd-ns.com	Teleconference (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	Teleconference (202-203-5140)
DoD PKI PMO (BAE Systems)	Brown, Wendy	wendy.brown@baesystems.com	301-939-2706
DoD PKI PMO (Orion)	Chokhani, Santosh	CHOKHANI@Orionsec.com	703-917-0060 x 35
DHS (CygnaCom)	Shomo, Larry	shomol@saic-dc.com	Teleconference (703-338-6892)
DHS	Ambs, Matt	Matthew.ambs@associates.dhs.gov	Teleconference
NASA	Murakami, Kiku	??	Teleconference
FPKIA OA	Lins, Andrew	Andrew.lins@mitretek.org	703-610-1786
FPKIA OA (Mitretek)	Fisher, Dr. Jim	jlf@mitretek.org	Teleconference

Organization	Name	Email	Telephone
Non-Federal Entities			
Identrus	Cornaby, Travis	travis.cornaby@identrus.com	Teleconference
Wells Fargo	Koski, Ryan	koskira@wellsfargo.com	Teleconference
Isode	Kille, Steve	Steve.kille@isode.com	Teleconference (444-20-8783 2970)
Secretariat (Enspier)	Fincher, Judy	Judith.fincher@enspier.com	703-299-4709 (direct line) 703-795-8946 (cell)
ORC	Sloan, Brandy		Teleconference

3. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions—Ms. Cheryl Jenkins

This meeting took place at the GSA National Capital Region Building at 7th and D Streets, SW, Washington, DC. Ms. Cheryl Jenkins, Co-Chair, called the meeting to order at 10:05 a.m. with attendee introductions.

Agenda Item 2

Directory Replication—Andrew Lins

At the last FBCA-TWG (July 20, 2006), Ms. Jenkins presented the PowerPoint presentation, Proposed FPKIA Re-Design: Current Architecture and Proposed Changes, July 2006, and asked that cross-certified entities have their directory experts attend the FBCA-TWG meeting on August 25, 2006 to discuss the proposed changes to the architecture and FPKI OA Directory structure.

Andrew Lins reported that the FPKI OA Directory is unstable and that there have been problems querying the Directory. The proposed solution is to replicate entity data onto the FPKI Border Directory, using X.500/LDAP chaining and X.500 shadowing. The entities are the master and the FPKI Border Directory is the slave. Entities could push updates to the FPKI Directory.

For X.500 entities, the OA would set up nodes for entities to replicate their data onto. For LDAP types, another solution is needed and Dr. Jim Fisher has proposed a solution. The OA can run a spider to retrieve data that entities wish to replicate. The spider can then populate the FPKI Border Directory.

Wendy Brown: Shadowing can downgrade the Directory.

Deborah Edmonds: Schema issues are a concern. They have crashed our Directory, overwriting schema in our Directory.

Andrew Lins: Chaining through FPKI is crashing your Directory?

Deborah Edmonds: Something in which ever Directory the query went to did not match the same schema. The problem is with the collective attributes and the way in which things are being queried. Also there have been errors with the common name.

Andrew Lins: Isode M-Vault produces crashes when it doesn't understand certain object classes. Isode is working on a solution.[1]

Andrew Lins: We need to test the X.500 Directory. Can it support different object classes? We may have to specify certain object classes, but I think replication will solve some of these problems.

Andrew Lins: When testing the FBCA Directory with entities, we have to tell them to remove certain object classes.

Matthew Ambs: Do we have to replicate all that information over to the Border Directory?

Andrew Lins: It will be optional for entities to replicate CA certificates, CRLs, cross-certificate pairs, etc.

Santosh Chokhani: Can the Directory hold all these entities?

Santosh Chokhani: What product have you selected?

Andrew Lins: Both the FPKI OA and DoD are using the Isode M-Vault product.[2]

Cheryl Jenkins: We tested several products before purchasing M-Vault. We need to do some stress testing to look at performance once we load all the CRLs and certs. To Dr. Jim Fisher: What did we test for the ISODE Directory?

Dr. Jim Fisher: We tested simultaneous queries going after multiple search strings.

[1] After the meeting, Isode (Steve Kille) provided this information: M-Vault will correctly handle unknown object classes and other schema in peer DSAs. There is no need for members to adjust schema.

[2] Isode M-Vault is a LDAP (Lightweight Directory Access Protocol) directory server.

Wanda Brown: Did you test during shadowing?

Andrew Lins: There was no shadowing tested with the current product.

Cheryl Jenkins: We need buy-in from the cross-certified entities to the Replication concept.

Dr. Jim Fisher: We don't anticipate everyone will be hitting the replication directory at the same time.

Santosh Chokhani: DoD will publish CRLs and certs only to the Border Directory.

Deborah Edmonds: Our internal systems replicate at the Department of State.

Cheryl Jenkins: I'm hearing that nobody has a problem with the concept of Directory Replication, but that we need a schema and test plan to get buy-in. Is any entity interested in replicating their subscriber certificates? e.g., all users?

Deborah Edmonds: We don't want everything published.

Dave Cooper. There is a dichotomy. Some entities, for privacy reasons, don't want to publish subscriber information on the Border Directory. Other agencies want to put subscriber information on the Border Directory to support encrypted e-mail.

Several members agreed that encrypted e-mail is a very important application that agencies want.

Matt Ambs: You can set up separate areas for e-mail searches.

Deborah Edmonds: You don't have a way to direct queries to a particular part of the Directory.

Dave Cooper: If a substantial number of people want to do encrypted e-mail, we will have to use indexing to make sure the queries go quickly.

Steve Kille: It would be better to distribute the search, making use of the Directory hierarchy, using a two-state search (1) e-mail domain (2) constrained to the sub-tree.

Santosh Chokhani: Can you create an index so that a search on e-mail is efficient?

Steve Kille: Yes, you can. It will scale and you will get good security for a single server. You can also do distributed search over multiple servers.

Cheryl Jenkins: Steve Kille (Isode) will be involved in the test plan to make sure we get more efficient searches.

Wendy Brown: Steve Kille is also working with DoD on the speed (performance) and CRL (size) issues.[3]

Cheryl Jenkins: To recap, we need to develop a Directory Schema and a test plan to ensure that we can roll out the new directory properly. Or, if it doesn't prove to be more efficient, we may not use it.

Dave Cooper: In summary, there are two issues: reliability and efficiency. With chaining, can we still get information if the Directory is down?

ACTION: Cheryl Jenkins will talk to Steve Kille during the week of Sept. 11-15, 2006, to discuss developing a Directory Schema and test plan.

Cheryl Jenkins: The FPKI is lacking SLAs to ensure that folks are up 99.5% of the time—a FBCA uptime requirement. When are you going to get your systems up to that level?

Agenda Item 3
Requirements for Test Environment (RTE)—Andrew Lins

At its last meeting the FBCA-TWG agreed that cross-certified entities 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 was required before the August 25, 2006 FBCA-TWG meeting.

To date, Ms. Jenkins has not received that input.

At the last FBCA-TWG meeting (July 20, 2006), the meeting consensus was to refocus the paper to emphasize the role of Replying Parties and give it another title: Implementation Guidance for Relying Parties (RPs) using the Common Policy Root: Acceptable Policies.

This revised paper was circulated for review prior to the August 25, 2006 FBCA-TWG meeting. It was presented at the meeting by Andrew Lins.

It was agreed that we need a test environment in place in order to test the new Directory Architecture. You can't talk about Replication without a test environment.

[3] Isode (Steve Kille) provided this information after the meeting: With CRLs greater than 10 Mbytes, care needs to be taken. Some directory client and server code does not handle very large CRLs well. Isode M-Vault default configuration should be changed where there is a need to hold master or shadow copies of large CRLs.

Dave Cooper: You need to do infrastructure testing, as well as application testing.

Scott Morrison: If the test environment is put into the DMZ, a formal C&A process will be required.

Santosh Chokhani: A bigger concern, now, is to get the test environment up.

Cheryl Jenkins: We'll have to have a test lab (for audit).

Cheryl Jenkins: Does the revised document capture the seven (7) requirements we agreed on at the last FBCA-TWG meeting? If so, then we need milestones as to when we could deploy it.

The FBCA-TWG worked through the list of seven requirements and agreed:

1: Add: "The test CA's name must not be the same as the production environment."

4. Do we need end-entity certs? If we do this in the production environment, then we will have to do it in the test environment. Else, it should be put on a web site for public access.

Santosh Chokhani: Would we put DIR (o=usgovt) tree on the web? Or, an informal list?

6. Andrew Lins is to incorporate Dave Cooper's list of Policy OIDS for use in the test environment (email attachment of August 12, 2006).Thus, this document will become a "living document," as new OIDs are added.

ACTION: Cheryl Jenkins is to discuss with Judy Spencer the issue of who governs o=us govt branch.

ACTION REMINDER: Justin Newman was to send an SLA example for the Test Environment Requirements to Cheryl Jenkins. Open Action Item.

Cheryl Jenkins: The budgets are already in for FY 07, but what are your test environment milestones for FY07? FY08?

ACTION: Cheryl Jenkins or Dr. Peter Alterman will contact the government Program Managers when the Test Environment Requirements document is revised, as per today's editing instructions, to determine the timeframe in which we can implement the test environment. Cheryl Jenkins will check with Dr. Alterman to determine who should send out this message.

The FBCA-TWG again discussed the ramifications of auditing the test environment. Cheryl Jenkins noted that we may have to do a "delta" accreditation and risk assessment.

Cheryl Jenkins: What's it going to cost and what will be needed on a yearly basis? The cost components and requirements are:

- Server
- Directory Software license
- C&A (delta accreditation)
- Risk assessment (800-53)
- CA license (for test CA)
- Test Border Directory IP address.

Andrew Lins: The level of effort on software patches to the test box (on-line directory) is about two hours per week.

Cheryl Jenkins: People want to know the man hours required to deploy and maintain the new directory.

Wendy Brown: How long will the testing of Replication take?

Santosh Chokhani: We need to focus on Objects and Directories.

Cheryl Jenkins: The initial effort is development.

Scott Morrison: And, we need to issue test certs.

ACTION: Cheryl Jenkins and the FPKI OA/Mitretek will develop a Test Environment Implementation Plan.

Agenda Item 4

Implementation Guidance for Relying Parties (RPs) using the Common Policy Root—Dr. Jim Fisher

The 20 July 2006 FBCA-TWG meeting consensus was to refocus the SSP paper discussed at that meeting to emphasize the role of Relying Parties (RPs) and give it another title: Implementation Guidance for Relying Parties (RPs) using the Common Policy Root: Acceptable Policies.

Dr. Jim Fisher revised the document and presented at the 25 August 2006 meeting. Dave Cooper also revised the document to include FBCA OIDs, but sent it only to the FPKI OA/Mitretek. These two documents need to be combined.

ACTION: Dr. Jim Fisher is to edit the Implementation Guidance for Relying Parties, etc., to blend the Dave Cooper and Mitretek versions and distribute to the FBCA-TWG at its next meeting.

Agenda Item 5

Signed E-Mail between CSPs and the OA—Andrew Lins

Andrew Lins distributed a hard-copy document, FPKIA Certificate Exchange: Proposed E-Mail Capabilities, at the meeting. The presentation described the existing courier-based communications between the OA and the cross-certified entities and proposed four options, including obtaining credentials from a commercial vendor.

After limited discussion, the FBCA-TWG chose the second option:

"Issue digital signature credentials to the FPKI OA from one of the 3 FPKI cross-certified CAs. This option utilizes the FPKI Infrastructure and allows entities to chose either PD-Val or trust list mode capable applications."

This option was judged to be the cheapest and most doable.

The scope of this initiative is the entire life cycle of a certificate between the OA and cross-certified entity.

Agenda Item 6

Other Topics

a) FBCA-TWG Meetings

The next FBCA-TWG meeting will be scheduled for September, 2006.

Agenda Item 7

Adjourn Meeting

The meeting was adjourned at 11:55 a.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
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	25 August 2006	Open
010	Cheryl Jenkins will talk to Steve Kille during the week of Sept. 11-15, 2006, to discuss developing a Directory Schema and test plan.	Cheryl Jenkins, Andrew Lins, Steve Kille	25 August 2006	11-15 Sept. 2006	Open
011	Cheryl Jenkins is to discuss with Judy Spencer the issue of who governs o=us govt branch?	Cheryl Jenkins, Judy Spencer	25 August 2006	15 Sept. 2006	Open
012	Cheryl Jenkins or Dr. Peter Alterman will contact the government Program Managers when the Test Environment Requirements document is revised, as per today's editing instructions, to determine the timeframe in which we can implement the test environment. Cheryl Jenkins will check with Dr. Alterman to determine who should send out this message.	Cheryl Jenkins, Peter Alterman	25 August 2006	12 Sept. 2006	Open
013	Cheryl Jenkins and the FPKI OA/Mitretek will develop an Test Environment Implementation Plan.	Cheryl Jenkins, FPKI OA/Mitretek	25 August 2006	15 Sept. 2006	Open
014	Dr. Jim Fisher is to edit the Implementation Guidance for Relying Parties, etc., to blend the Dave Cooper and Mitretek versions and distribute to the FBCA-TWG at its next meeting.	Dr. Jim Fisher/ Mitretek	25 August 2006	15 Sept. 2006	Open