Federal Public Key Infrastructure Policy Authority (FPKIPA)
FBCA Technical Working Group (FBCA-TWG)
Draft Minutes

8 February 2007

GSA NCR, 7th and D Streets, SW, Room 5700, Washington, DC
Room 5700 (Training Room)

1. AGENDA

1. Welcome & Opening Remarks / Introductions
2. Service Level Agreement (SLA)
3. Requirements for Test Environments
4. Monthly Scorecard
5. FPKI Architecture Re-Design
6. Relying Party Configuration Guidance
7. Closing Remarks
8. Adjourn Meeting

2. 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@jsdoj.gov	Teleconference 202-616-8989
GSA (Co-Chair)	Jenkins, Cheryl	Cheryl.jenkins@gsa.gov	571-259-9923
NIST (Co-Chair)	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		
DoD PKI PMO (Orion)	Chokhani, Santosh	Chokhani@Orionsec.com	703-917-0060 x 35
DHS PKI Operations Manager	Barcia, Gladys	Gladys.Garcia@associates.dhs.gov	202-261-9236
DHS (CygnaCom, Contractor)	Shomo, Larry	shomol@saic-dc.com	Teleconference (703-338-6892)
DoE	Legere, Richard	Richard.Legere@HQ.DOE.GOV	Teleconference 301-903-9464
Treasury (Hewlett-Packard, Contractor)	Kiel, Darren	Darren.keil@do.treas.gov	202-622-9374
Treasury (TCS TEDS Project Manager)	Morgan, Byron	Byron_K_Morgan@notes.tcs.treas.gov	Teleconference 703-747-0955
Treasury	Vaziri, Al		Teleconference
Nuclear Regulatory Commission	Sulser, David		
DoD (Tangible	Brundage, James	jbrundage@tangiblesoftware.com	

Organization	Name	Email	Telephone
Software, contractor)			
FPKI OA (Mitretek, Contractor)	Fisher, Dr. Jim	jlf@mitretek.org	703.610.2943
FPKI OA (Mitretek, Contractor)	Tate, Darron	darron.tate@mitretek.org	703-610-1905
Wells Fargo	Fontenot, Ward (Paul)	Ward.P.Fontenot@wellsfargo.com	Teleconference
Isode	Kille, Steve	Steve.kille@isode.com	Teleconference (444-20-8783 2970)
Secretariat (Enspier/Protiviti Government Services, contractor)	Fincher, Judy	Judith.fincher@enspier.com	703-299-4709 (direct line) 703-795-8946 (cell)
Enspier/Protiviti Government Services, contractor	Brown, Chris	Chris.Brown@enspier.com	(202) 208-1550
Enspier/Protiviti Government Services, contractor	King, Matt	Matt.King@enspier.com	410-271-5624
FPKI/FICC Support (General Dynamics Information Technology, Contractor)	Petrick, Brant	Brant.Petrick@gsa.gov	202-208-4673
A&N Associates, Inc.	Dzambasow, Yuriy	Yuriy@anassoc.com	410-859-5449 X. 107
Electrosoft, Inc. (Contractor)	Gupta, Sarbari	Sarbari@Electrosoft-inc.com	703-217-8475

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, in Room 5700. Ms. Cheryl Jenkins, Co-Chair, called the meeting to order at 9:30 a.m. with the attendee roll-call.

Agenda Item 2

Service Level Agreement (SLA)—Cheryl Jenkins

Ms. Jenkins said that she is working on the SLA for the FPKI OA. It is currently being scrubbed against the FBCA CP and MOAs. Currently, the MOAs are vague. For example, there is a requirement that you must contact someone "in a timely manner." What does this mean? Two months? It's left to the cross certified entity to determine the timeframes. The SLA will clean this up, she said.

Agenda Item 3

Requirements for Test Environments—Cheryl Jenkins

Ms. Jenkins said that the FBCA-TWG agreed on the requirements for test environments at the last meeting (25 August 2006). We asked agencies to set up test environments that mirror the production environment, she said.

ACTION: Cheryl Jenkins will send the latest version of the Test Guidelines for the OA Test Environment to the FBCA-TWG listserv.

Ms. Jenkins said that we are asking for 99% availability in the test environment. The last piece to be completed is the cost analysis for the test environment. This will help the Policy Authority determine when each cross-certified entity should stand up their test environment. If it costs a lot, it will probably be in your budget the year after next. If not, she estimates that test environments could be stood up within six to eight months.

An issue has arisen related to whether or not a C&A has to be performed for the test node—in the test environment. Some DAAs say it's up to the owner of that operational system. Others say that if it's part of the operational system, it has to be part of the C&A.

Santosh Chokhani said that if the test environment was completely separate, e.g., had its own T-1 line, there would be no need for a C&A.

Agenda Item 4

Monthly Scorecard—Cheryl Jenkins

Ms. Jenkins said that statistical information collected on each cross-certified entity is displayed visually in a "scorecard". We got behind in November and December and decided to wait for the next version of the Scorecard—due on February 15, 2007. She reviewed the list of ten cross-certified entities that had either technical or policy issues. A description of the issue appears in the column opposite the name of the entity. You need to address your issues, she said.

If you need your Scorecard before February 15, let me know and we will send you the December Scorecard.

Agenda Item 5

FPKI Architecture Re-Design—Dr. James Fisher

Jim Fisher, Ph.D., the FPKI OA Technical Lead, gave a slide presentation on the proposed re-design of the FPKI Architecture. This presentation, "FPKI Architecture Re-Design," February 8, 2007, was distributed to the FBCA-TWG listserv prior to the meeting.

Background
The background is that the current ATO for the architecture expires 6/30/07 and a technology refresh is planned, since warrantee/service agreements for much of the equipment in the current infrastructure is not obtainable. His presentation covered the consolidation of the Certification Authority (CA) hardware and a description of the X.500/LDAP directory infrastructure, with both near-term and long-term architectural changes.

Certification Authority (CA) Changes
The proposed CA changes consist of:

1) Consolidation of the FBCA, C4CA, FCPF CA and eGovernance CAs to run on the same computer.
2) A proposed new Domain Name (DN) structure of the CAs to better reflect the FPKIA hierarchy and provide internal consistency.

Ms. Jenkins said that she has submitted a change proposal to the Policy Authority on the DN level at which we will cross-certify new entities. We need a single reference, she said. In the spring, she will create a directory schema which will promote interoperability of directories of cross-certified entities. Currently, cross-certified entities have widely-varying directory structures.

To support the CA changes, Dr. Fisher explained, it will be necessary to transition the current architecture to the new architecture. Both will run in parallel for a short period of time. You can't just turn off the switch, he said.

Santosh Chokhani took exception to Dr. Fisher's proposal to either:

1) maintain two sets of cross-certificates and two sets of chaining agreements, or alternatively,
2) allow entities to transition without dual cross certificates by issuing cross certificates between the current and new architectures.

There are just three things you need to do, he said:

1) Revoke the certs
2) Issue new CRLs
3) Destroy that key.

Dave Cooper agreed it was easy to shut down the Bridge and that it had been designed to do so. Just issue new certs to the cross-certified entities and shut down the Bridge, he said. But, he raised a concern about entities that are using the current ones as trust anchors. He didn't know how that would work.

X.500 Directory and Directory Chaining

Dr. Fisher said that clients need to get used to the idea of referrals, instead of Directory Chaining. While directory chaining has some advantages, such as mitigating Denial of Service (DOS) attacks, it also has some disadvantages:

1) Single point of failure
2) Requires directory interoperability.

He said that DHS currently requires access to their directory only through chaining through the FPKIA Directory to reduce DOS attacks. Gladys Garcia pointed out that this is a budget issue, not a policy issue. DHS wants to put an external directory out on the Internet, she said.

He described directory interoperability problems of the current system and other chaining issues:

1) He spent five hours with Treasury, trying to sort out how to handle X.500 syntax. This was due to the fact that the Siemens directory used by Treasury does not handle an LDAP filter "objectClass-*" supported by the Isode directory.
2) Chaining to DHS was down for two days, possibly due to a firewall issue.

Dr. Fisher then discussed some ways of mitigating Directory Chaining risks. Two of the options he discussed were:

1) Administrative filtering in X.500 software itself to filter out expensive searches. This is not yet implemented, but Steve Kille (Isode) said that Isode can put in administrative filtering.
2) Use of referrals, with no Directory Chaining involved.

Dr. Fisher then proposed the FBCA-TWG consider sun-setting directory chaining and go directly to referrals. He discussed issues related to sun-setting directory chaining, including:

1) The primary Isode directory returns referrals when chaining is down and there are no known reports of complaints of client software problems.
2) Directory chaining alone is sufficient if all of the following are true:
    i. The Client software supports URI-formatted DNs in CDP and AIA fields; DSP, LDAP, HTTP redirects, following referrals; trying all CDP/AIA entries until success.
    ii. There are no DSP-only software clients
    iii. Certificates are constructed such that CDP, AIA fields contain LDAP URIs. FPKIA profile requires LDAP URIs (with hostnames); DN-only entries are optional.

iv. All entity directory infrastructures are directly accessible.

Dr. Fisher then discussed some recommendations to mitigate existing directory chaining problems. Long-term, he said, the solution was to replace chaining with referrals and make sure PD-Val can handle referrals.

Steve Kille (Isode) was not in agreement with a strategy to go directly from directory chaining to referrals. We need to test to find out which is the best option and at present, he said, there is not enough information to decide.

To address the problem of remote administration, Dr. Fisher noted the need for rapid response remotely and proposed the use of software, KVM-over-IP, to support remote viewing/access of boot & BIOS screens, etc. A disadvantage of the current two-site operation is that any change to the FBCA requires people to go on site to fix it.

Jim Brundage (Tangible Software, a DoD contractor) commented that DoD uses KVM and has had problems. Their goal is to shut down all remote access and go to a VPN solution instead.

ACTION: Jim Brundage will provide a DoD White Paper describing the issues behind their decision to drop KVM-over-IP and go to a VPN solution.

Dr. Fisher proposed a phased directory implementation using multiple, geographically disbursed, ISP-diverse, simultaneously operational directory systems. He said that the proposed directory architecture is agnostic as to chaining vs. referrals vs. partial tree replication.

He recommended a minimum of three sites, with one 400 miles away. Current operations have access to two geographically disbursed locations (Fairfax, VA and Washington, DC), with network access provided by two different ISPs. He recommended that both currently occupied sites be simultaneously active and that the new OA contractor be allowed to choose additional sites.

Cheryl Jenkins said that she needs to justify the cost of an additional site(s).
She disagreed with the bullet on page 14 of the presentation that stated that the new OA contractor had already established on-site facility agreements, etc. There will be no decisions about other sites until the new OA contractor team takes over.

Dr. Fisher then presented a slide (page 15) depicting the proposed new FPKI architecture. The highlights of this “macro view” included:

1. Geographically disbursed sites
2. All sites are always live, publicly accessible, up-to-date

3. Proper native master/shadow directory replication via DISP (not pushy scripts)
4. Chaining agreements do not automatically replicate to each remote site
5. Only shadows can access the master directory
6. Open public access to LDAP (Shadows) and HTTP
7. IP-filtered DSP access to X.500 shadows
8. HTTP servers periodically pulls CRLs & certs from nearest X.500 Directory; periodically recreates p7c file
9. At each site, firewall dynamically load balances between X.500 directories, and between HTTP servers
10. Public is directed to different sites via round-robin DNS; can load-balance between sites.

He then presented the detailed view of the proposed new architecture, showing which components were replicated at some satellite sites and which were replicated at all satellite sites. This depiction assumed the use of KVM-over-IP.

At the end of his presentation, Dr. Fisher opened the floor for other questions. David Sulser (NRC) wanted to know if we can learn anything from the DNS community related to recursive behavior or referrals.

Dr. Fisher said that three of the 12 DNS roots were under DOS attacks and that two had fared well. The DNS community deploys shadow directories and has a master/slave directory structure. To protect against attacks, you need an ISP to help, he said.

Jim Brundage took exception to this description of the DNS community. That's not how DNS works, he said. There is no master/slave relationship in DNS. [David Sulser commented that Mr. Brundage used to work for VeriSign and did this everyday.]

Jim Brundage wanted to know if Dr. Fisher had the specs for the hardware for the new architecture, given that the ATO was expiring at the end of June.

Cheryl Jenkins said that the equipment specifications would not be done until an independent reviewer has signed off on the new architecture and until she had the consensus of all the cross-certified entities.

Ms. Jenkins then asked Dr. Fisher if he needed any more information from the FBCA-TWG participants in order to finalize the architectural plan. He identified the following:

1) Will CAs and CRLs be on separable branches of the directory tree? [This will drive what gets replicated and what gets chained, he said.]
2) Are current RP clients sufficiently capable?
3) Any legacy or non-compliant certificates?
4) Any DSP/DAP applications requiring chaining?

Ms. Jenkins encouraged all agencies represented at the FBCA-TWG to comment on the proposed new architecture and to respond to these questions posed by Dr. Fisher.

He also pointed out that the architecture needs one DSA for each to-level node (currently: c=US; dc=gov).

Ms. Jenkins thanked Dr. Fisher for his presentation.

Agenda Item 6

Relying Party Configuration Guidance—Dave Cooper

Prior to the FBCA-TWG meeting on 8 February 2007, Dave Cooper submitted a guidance paper, "Implementation Guidance for Relying Parties Using the Common Policy Root." This document was distributed to the FBCA-TWG listserv prior to the meeting. The purpose of this paper is to provide guidance for selecting a set of acceptable policy object identifiers (OIDs) when the Common Policy Root CA is used as a trust anchor.

Background
Many PKI applications have a requirement to only accept certificates that were issued in conformance with certain policy requirements. This may be accomplished by configuring the application to only accept certificates that validate with respect to a certain set of OIDs. The guidance in this document is based on the set of certificate policies and policy mappings that are currently asserted in certificates issued by the Common Policy Root CA.

Mr. Cooper noted that this paper will be modified in the future to add the OIDS for the certificates policies that were defined within the past year, e.g., Common Policy High and FBCA Medium Hardware, FBCA Medium CBP, FBCA Medium Hardware CBP. The OIDs for these policies will be added when new cross-certificates are issued by the Common Policy Root CA to the FBCA.

Dr. Santosh Chokhani expressed his view that this guidance only provides a 90% solution. He maintained that you need to map every asserted OID to have cross certified domains express all lower policies also. Mapping one-to-one won't work, he said. You should mandate that when you assert a policy, that you assert all

lower policies, as well. The alternative is to assert all higher policies, he said. Government doesn't recognize the problem. For example, if Medium Hardware is asserted (only) and the RP wants to assert Medium, it won't work, he said. A one to many mapping is required.

Dave Cooper said that we only map what the applicant wants us to map, e.g., Medium HW (theirs) to Medium (ours). Dr. Chokhani's mapping recommendation (above) should be guidance to cross-certified members, not to RPs. It would be in appropriate for us to map OIDs where they have not been requested (and reviewed by the CPWG).

Dr. Alterman, who joined the meeting at the end, expressed his view that this Relying Party guidance should be posted to the FBCA website.

ACTION: Cheryl Jenkins will post the "Implementation Guidance for Relying Parties Using the Common Policy Root" to the FBCA website for use by Relying Parties (RPs).

Note: Not discussed at the meeting was another section of the paper which addresses the use of policy OIDS with certain E-Authentication levels, e.g., E-Authentication levels 3 and 4. This will assist agencies with applications that need to filter certificates based on the E-Authentication level.

Agenda Item 7

Closing Remarks—Cheryl Jenkins

Cheryl Jenkins noted that a List of Principal CA (PCA) Distinguished Names (DNs) cross certified with the FBCA has been posted to the FBCA website, with a link to it from the FPKIPA website. This was done in response to a suggestion by one of the FBCA-TWG members, Dr. Santosh Chokhani.

A "Hint List" will also be added to the PD-VAL website next week to assist agencies with setting up their validation services. The Hint List is provided free of charge.

Agenda Item 8

Adjourn Meeting

The meeting was adjourned at 11:15 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

No.	Action Statement	POC	Start Date	Target Date	Status
015	Cheryl Jenkins will send the latest version of the Test Guidelines for the OA Test Environment to the FBCA-TWG listserv	Cheryl Jenkins	8 Feb. 2007	16 Feb. 2007	Open
016	Jim Brundage will provide a DoD White Paper describing the issues behind their decision to drop KVM-over-IP and go to a VPN solution.	Jim Brundage	8 Feb. 2007	9 March 2007	Open
017	Cheryl Jenkins will post the "Implementation Guidance for Relying Parties Using the Common Policy Root" to the FBCA website for use by Relying Parties (RPs).	Cheryl Jenkins	8 Feb. 2007	16 Feb. 2007	Closed