Federal Public Key Infrastructure Policy Authority (FPKIPA)

FBCA Technical Working Group (FBCA-TWG)

Minutes

26 January 2006 Meeting

GSA, 2011 Crystal Drive (Crystal Park 1), Suite 911
Arlington VA 22202

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Meeting Objective
3) Modified Common Policy Certificate Profile
4) Replication & Strong Authentication Requirements for Directory Servers
5) Testing Environments
6) Business Operational Rules
7) OCSP Support in the FPKIA?
8) Next Steps
9) Adjourn Meeting

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Federal Entities			
DOE	Legere, Richard	Richard.Legere@HQ.DOE.GOV	301-903-9464
Treasury	Schminky, James	James.Schminky@DO.Treas.gov	Teleconference (202-622-2446)
Treasury	Kiel, Darren	Darren.kiel@do.treas.gov	202-622-9374
Treasury (eValid8)	Dilley, Brian	brian.dilley@evalid8corp.com	Teleconference (443-250-7681)
DOJ	Morrison, Scott	Scott.k.morrison@usdoj.gov	202-616-9207
DOJ	Young, Siegfreid	Siegfreid.f.young@usdoj.gov Or syoung@hpti.com	202-616-8989
DHS (CygnaCom)	Shomo, Larry	shomol@saic-dc.com	703-338-6892
DHS	Ambs, Matt	Matthew.ambs@associates.dhs.gov	
GPO	Hilderbrand, Jeff	JHildebrand@gpo.gov	202-512-0109
NFC/USDA	Collins, Louis	louis.collins@usda.gov	Teleconference 504-426-0434
NASA (Co-Chair)	DeYoung, Tice	Ticedeyoung@hq.nasa.gov	202-358-2154
NASA	Murakami, Kiku	kmurakami@mail.arc.nasa.gov	Teleconference 650-604-1591
USPTO	Purcell, Art	art.purcell@uspto.gov	571-272-5354
USPTO	Jain, Amit	Amit.jain@gd-ns.com	571-438-6309
GSA (Co-Chair)	Jenkins, Cheryl	Cheryl.jenkins@gsa.gov	571-259-9923
GSA	Spencer, Judith	Judith.spencer@gsa.gov	202-236-0328
FPKIA OA	Lins, Andrew	Andrew.lins@mitretek.org	703-610-1786
FPKI/FICC (FCBS)	Petrick, Brant	Brant.Petrick@gsa.gov	202-208-4673

NIST	Cooper, David	David.cooper@nist.gov	301-975-3194
Dept. of State (Dos)	Horowitz, Charles	horowitzce@state.gov	202-203-5167
Non-Federal Entities			
DST	Newman, Justin	Justin.newman@identrus.com	
Isode	Kille, Steve	Steve.kille@isode.com	444-20-8783 2970
Identrust	Cornay, Travis	travis.cornaby@identrus.com	Teleconference
ORC	Turissini, Dan	turissd@orc.com	703-245-8550
Wells Fargo	Koski, Ryan	koskira@wellsfargo.com	Teleconference
Wells Fargo	Pelton, Doug	peltond@wellsfargo.com	Teleconference
Secretariat (Enspier)	Fincher, Judy	Judith.fincher@enspier.com	703-299-4709
No Shows/or Added Later			
DoD PKI PMO	Hanko, Dave	djhanko@MISSI.NCSC.MIL	410-854-4900
NFC/USDA	Sharp, Kathy	Kathy.sharp@usda.gov	
NASA	Euler, Helen		
NASA	Vo, Jimmy		
Enspier	Lazerowich, Steve	Steve.lazerowich@enspier.com	703-299-3444
Identrus	Pinegar, Tim		
HEBCA	Rea, Scott	Scott.rea@dartmouth.edu	

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), Suite 911, Arlington, VA 22202. Ms. Cheryl Jenkins, Co-Chair, called the meeting to order at 10:10 a.m. with attendee introductions. Mr. Tice DeYoung. Co-Chair, co-hosted the meeting.

Agenda Item 2

Meeting Objective—Ms. Cheryl Jenkins

Ms. Jenkins explained the reason for the meeting:

- There are interoperability issues that we must begin to address in order to be ready for the expanded use of PKI called for in FIPS-201.
- We have to begin to identify the problems and come up with solutions.

Ms. Jenkins noted that there are a number of operational and technical concerns within the Federal Public Key Infrastructure Architecture (FPKIA) and that the

purpose of this meeting was to forge synergy between the policy and technical side.

Agenda Item 3

Modified Common Policy Certificate Profile—Mr. Dan Turissini (ORC)

Ms. Jenkins asked Mr. Dan Turissini from ORC to discuss the issue he had raised about the requirement for a CA to have all of the OIDs present in its root certificate. Mr. Turissini said that it was not clear between the U.S> Federal PKI Common Policy Framework and the profiles what a CA was supposed to assert. He stated that stating "All the OIDs" could cause a conflict, e.g., Medium software where High hardware was intended.

Mr. Turissini maintained that agencies that are cross-certified with the FBCA want a standard approach when asserting OIDs. This applies to agency applications that process the OIDs.

Mr. David Cooper said that all of the OIDs had to be asserted throughout the entire path in order for a certificate to be verified.

Mr. Turissini then asked, "If you don't assert all of the OIDs, does that mean that you can't issue any not in the CA certificate?"

Mr. Cooper answered that yes, you do have to assert all of them. He added that if you don't, the end user certificates wouldn't work. If an end entity asserts High, the assumption is that a relying party looking for Medium would accept it.

Mr. Charles Horowitz (DoS) then stated that we should make it simple: have the clients assert all of the policies that they will accept, whether one or many. We shouldn't rely on the applications to do it for you because some of them aren't smart enough to know, he said. You should eliminate uncertainty and be precise, he said. Mr. Larry Shomo agreed: list all the OIDs in the cert.

Mr. Turissini then said that adding the additional OIDs indicated in the U.S. Federal PKI Common Policy Framework Change Proposal Number 2006-01 has major operational implications such as the card authentication OID, OCSP, to possibly having to re-do relying party applications to accept the new OIDs. This is a significant change to the operation of the CAs.

Ms. Jenkins said that agencies want better documentation for end-entity users. This applies to the Common Policy Certificate Authority and the application owners.

Ms. Jenkins then asked if a policy document for the U.S. Federal PKI Common Policy Framework would help: one that lays out what has to be done and how to do it. Such guidance for the Common Policy Certificate Authority should be posted on the web, she said.

ACTION: 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.

Re-Keying

Mr. Justin Newman (DST) stated that it is a technology issue with technical impacts caused by the Federal Public Key Infrastructure Policy Authority (FPKIPA). He stated that it will require a re-key in order to assert the new OIDs. He believes that the cost to the agencies and to private companies is "substantial."

Mr. Turissini then said that any change requiring more OIDs meant either a root CA re-key, or a resigning of the root CA and has implications all the way down to the end users, applications and relying parties. He did not want to have to re-key every six months due to new policy OIDs. He believed there would be significant technical issues with agencies too. It's a big cost driver, he stated.

Ms. Jenkins said that we would pass this information on to the FPKI Certificate Policy Working Group (CPWG) and the FPKIPA with the admonition that we need to figure out what to do about this.

ACTION: 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.

Agenda Item 4

Replication & Strong Authentication Requirements for Directory Servers—Mr. Steve Kille (Isode)

Mr. Steve Kille of the company Isode addressed the group on the topic of replication and strong authentication requirements for directory servers. Isode is a software product company that builds high performance email and directory server products using open standard protocols.

Mr. Kille urged the FPKIPA to add partial Directory Replication to the FPKIA and make it optional. This would be complimentary to chaining. It would also remove the single point of failure and improve performance and local access. He recommended the use of the Directory Information Shadowing Protocol (DISP) for partial replication.

Mr. Kille also urged the FPKIPA to allow "strong authentication," i.e., authentication based on X.509, as soon as possible. This would make the directory more secure and resilient and simplify server to server communications. "We should eat our own dog food," he commented, adding that security at present is "incredibly poor."

ACTION: Mr. Kille will post his presentation to the Isode web site and notify Ms. Cheryl Jenkins of the URL. He provided this URL after the meeting: www.isode.com/fbca.html

In the ensuing discussion, some members were not sure replication was the right solution. Mr. Sigfreid Young (USDOJ) suggested "clustering" as an alternative to replication.

No decisions regarding replication and/or strong authentication were made at this meeting.

Agenda Item 5

Testing Environments—Ms. Cheryl Jenkins, Mr. Andrew Lins

Ms. Jenkins and Mr. Andrew Lins described the requirement for a testing environment that closely mirrors the production FPKIA. Discussion then ensued about the need to ensure that CAs cross-certified with the FBCA not make changes to either the version of the software, their certificate repositories, or other things that would cause the directory chaining to break.

Mr. Lins urged agencies to work directly with him in standing up consistent test environments. Many had prototype test environments that have been abandoned. Mr. Dan Turissini would like a Test Road Map.

As we roll out HSPD-12 we need a test environment that mimics the FPKIA, according to Ms. Jenkins.

ACTION: Ms. Cheryl Jenkins will send out the test requirements document to the FBCA-TWG listserv to obtain feedback on where each agency is vis-à-vis standing up PKI test environments.

Ms. Jenkins stated that she would not test products that haven't passed the NIST PD-Val test suite.

Mr. Larry Shomo suggested we define what it is we want to test.

Several members expressed an interest in sending encrypted emails across the Federal Bridge, a capability that is not currently supported.

Agenda Item 6

Business Operational Rules—Ms. Cheryl Jenkins

Ms. Jenkins stressed the need for timeliness, accuracy and accountability in the business operations of the FPKI-Operational Authority (OA). There are problems with inaccurate information in the certificates. She raised the issue of how well aligned we are with Program Management and asked if the FPKIPA needs to have Service Level Agreements (SLA's) put in place for agency operators. Agency infrastructure changes will require notifying the FPKIPA and the FPKI-Operational Authority (OA).

Agenda Item 7

OCSP Support in the FPKIA? —Dr. Tice DeYoung

Dr. Tice DeYoung developed a PowerPoint slide presentation on the Online Certificate Status Protocol (OCSP) which was discussed by the FBCA-TWG at this meeting.

Background
OCSP is one of two common schemes for maintaining the security of a server and other network resources. The other, older method, which OCSP has superseded in some scenarios, is known as Certificate Revocation List (CRL). The CRL method is currently used by the Federal Bridge.

OCSP overcomes the chief limitation of CRL: the fact that updates must be frequently dowloaded to keep the list current at the client end. When a user attempts to access a server, OCSP sends a request for certificate status information. The server sends back a response of "current", "expired," or "unknown." The protocol specifies the syntax for communication between the server (which contains the certificate status) and the client application (which is informed of that status). OCSP allows users with expired certificates a grace period, so they can access servers for a limited time before renewing.

Centralized or Distributed?
Dr. DeYoung put forth a strawman argument that a centralized OCSP server is needed for the FPKI and that by 2008 it will be required. He said that we need to have a central FBCSA OCSP repository where everyone would go to determine if a certificate was valid.

Ms. Judith Spencer noted that that meant that every entity cross-certified with the FBCA would have to make its information available for download and that the

FBCA would have to download and store all of the data, something that the FPKI OA wasn't prepared to do. This means that every member of the Federal Bridge would have to provide full CRLs for every application if OCSP is implemented.

This sparked a lot of discussion about whether or not this was necessary, or the wise thing to do.

Some members questioned whether the OCSP was necessary for the FPKIA and whether the functionality could be distributed, possibly to lower costs and reduce latency (lag), and be co-located with the CAs.

Mr. David Cooper responded that anyone who wants to can do OCSP now. Mr. Cooper said that FIPS 201 requires PIV authentication certs and an OCSP responder, but that no profile has been written for OCSP yet.

Mr. Justin Newman (DST) said it is assumed that within one or two years everybody will have an OCSP server interface. He stated that he feared the creation of a centralized OCSP repository because of the risk that someone else could assert his certificates and that the higher initial costs of a distributed OCSP system might be offset by lower [administrative] costs, in the long run.

Moreover, if you have a centralized OCSP responder, the rest of the world might not trust it. For that reason, we would still need agency CRL repositories.

Ms. Jenkins thought that distributed repositories would serve as an interim solution until OCSP becomes widely available and Ms. Judith Spencer asked the TWG to consider pursuing an architectural model that has distributed OCSP.

It was noted that CoreStreet uses an OCSP responder in their product.

Role of CRL's in the Trust Path

Discussion centered on whether or not CRL's are fundamental to OCSP responders. It was pointed out that CRL's are not used in Europe. Mr. Larry Shomo (DHS) reported that Verisign captures info directly from the CAs, not from the CRLs.

Ms. Judith Spencer noted that initially ACES did not have CRLs and that these were added later.

Mr. Dan Turissini stated that you could do both CRLs and OCSP in the same environment.

The drawback to using OCSP responders centers around the fact that you can't control Relying Parties. Ms. Spencer stated: you can't control who hits a border directory. Our directories are outward facing, she explained. You can chain back to anybody who is authenticated by the FBCA.

Ms. Jenkins wanted to know the agencies' opinion on centralized versus distributed repositories, before we go charging down a particular path. What are agencies using internally to validate certificates? Entrust is working with Treasury to solve these issues.

No actions items resulted from this discussion.

Transmission of Sensitive Information Across the Federal Bridge
A side discussion was held about how cross-certified members currently are sending sensitive email information across the Bridge. Currently, members have to send signed emails to each other to establish a link and then send encrypted messages.

Ms. Judith Spencer stated that this is a hole in the FPKIA which we are working diligently to fix. She noted that she had had discussions with Mr. Gary Moore of CygnaCom about the PD-Val capabilities of Entrust. CygnaCom is working with Entrust and the US Treasury to solve this problem.

ACTION: Mr. Charles Horowitz (DoS/Cygnacom) asked members to send him signed emails, so he can help Entrust validate testing procedures/suites.

Agenda Item 8

Next Steps

FBCA-TWG Meetings
The next FBCA-TWG meeting will be scheduled for March.

FBCA-TWG Listserv
The FBCA-TWG listserv is being updated with the names of people who participated in this meeting.

ACTION: Ms. Jenkins asked everyone to make sure they were the right person or have the right person send their contact information to Ms. Judy Fincher.

Agenda Item No. 9

Adjourn Meeting

The meeting was adjourned at 12:18 p.m.

Action Item List

No.	Action Statement	POC	Start Date	Target Date	Status
001	Mr. Kille will post his presentation to the Isode web site and notify Ms. Cheryl Jenkins of the URL He provided this URL after the meeting: www.isode.com/fbca.html	Steve Kille	1-26-06	2-6-06	**Closed**
002	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.	FBCA-TWG	1-26-06	March 06	**Open**
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	Ms. Cheryl Jenkins will send out the test requirements document to the FBCA-TWG listserv to obtain feedback on where each agency is vis-à-vis standing up PKI test environments	Cheryl Jenkins	1-26-06	March 06	**Open**
005	Mr. Charles Horowitz (DoS/Cygnacom) asked members to send him signed emails, so he can help Entrust validate testing procedures/suites	FBCA-TWG members	1-26-06	1-31-06	**Open**
006	Ms. Jenkins asked everyone to make sure they were the right person or have the right person send their contact information to Ms. Judy Fincher.	FBCA-TWG members	1-26-06	March 06	**Open**