

**Federal Bridge Certification Authority (FBCA)
Path Discovery & Validation (PD-VAL)
Working Group Meeting Overview
NIST North / Room 660**

20 November 2003

A. AGENDA

1. Introductions and Opening Comments Cheryl Jenkins

2. Lab Report Ken Stillson, Andrew Lins
 - a. Draft Report
 - b. Testing Status

3. FBCA-Aware Application Demo

4. Validation Systems and Tools
 - a. CAM
 - b. Intermediate Store
 - c. Spider
 - d. Entrust
 - e. RSA

5. Performance and Testing
 - a. Microsoft Tim Polk
 - b. DigitalNet Ken Stillson
 - c. Testing Status

6. General Discussion

B. MEETING ACTIVITY

Ms. Cheryl Jenkins, GSA and FBCA Operational Authority Program Manager, called the meeting to order at 2:15 pm.

Agenda Item 1

Introductions and Opening Comments:

Ms. Jenkins started by saying that the group should be working to get the demonstration goals completed before the holidays, and that the group needed to figure out how the goals fit into the FBCA mid- to long-term goals.

Agenda Item 2

Lab Report:

Ms. Jenkins then turned over the meeting to Mr. Ken Stillson and Mr. Andrew Lins, Mitretek, for a report on the testing activities for Electronic-Email Exchange Demonstration (EED).

The first goal of the EED testing has been to validate the functionality required for a formal email exchange demonstration. A report, *E-Mail Exchange Demonstration (EED) Technical Guidance*, has been created containing the historical notes and status of the testing efforts thus far. This document should be distributed to the working group and get comments back within the following week. Those comments are needed before we can go back to Entrust or the other vendors.

ACTION (013): Mitretek will send a softcopy of the report to the mail list and request comments by 26 November 2003.

ACTION (014): The PD-VAL members will review the *E-Mail Exchange Demonstration (EED) Technical Guidance* and submit comments by 26 November 2003.

ACTION (015): Mitretek will update the report by COB the Monday after Thanksgiving based on comments.

The only successful tests have been from Microsoft to Microsoft, and Entrust to Microsoft with Microsoft acting as the relying party. The testers thought that Entrust should have worked very easily, due to the maturity of their products. However, Entrust products did not perform as expected. Email signed by Microsoft cannot be validated by an Entrust-enabled client; the client says that the signature is not trusted.

Testing is ongoing, but they have not been able to determine the cause of the problems as of yet. One conclusion is that the properties of a certificate seem to matter very much. The end-user validation software from Entrust is not behaving as expected, and the testing steps performed are documented in the draft report, above.

Agenda Item 3

FBCA-Aware Application Demo:

Ms. Jenkins then asked what affect the testing status has on the ability to demo something by the end of December. Mr. Stillson and Mr. Lins responded that this is still a work in progress, and they don't have enough information yet to say when it will be functional. However, they believe that they will be able to sort out the details – hopefully; the incompatibility issue is a small,

overlooked detail. They don't believe it is a problem with the certificate contents, but rather something went wrong with the Entrust configuration. Also, several changes were made to the infrastructure (e.g. directory service) during the testing. The testers may not have gotten something set correctly with the replication agreements, or something similar to that.

It will likely be hard for partners to re-issue certificates that align with the adjusted certificate structure set forth in the technical guidance document. The profile changes will cause significant impact to the vendors, who cannot deal with these certificates yet.

Ms. Jenkins noted that when the trust anchors' certificate profile is changed, a new document signing ceremony will be required for all the cross certified PKI members, with all the attendant staffing (time/people) impacts. It may require coordination of 2-3 hours of several peoples' time. Ms. Jenkins stressed the importance of making sure any reissue of cross certificates address the 100% solution to any known problems, so this won't have to be repeated in the foreseeable future. The CA's self-signed certificate would not have to be reissued, but all subordinate certificates would be impacted.

There followed much back-and-forth discussion as to whether a key generation signing ceremony is really required when changing a certificate, if you're not changing a key. There was no clear consensus on this issue.

ACTION (016): Ms. Jenkins will arrange a teleconference with the team and government customers to discuss the level of effort required for the email demonstration, identify a proposed demonstration date, and discuss the need for a resigning ceremony.

Agenda Item 4

Validation Systems and Tools:

Status of validation systems and tools is as follows:

CAM: no longer included in demo configuration.

Intermediate Store: no updated status to report

Spider: no updated status to report

Entrust: Trying to work out licensing issues between Mitretek and Entrust and therefore Mitretek doesn't have the software yet. This is a concern if we are proposing a COTS solution.

RSA: Mr. Bret Michaels, RSA Director of Federal Services, states that Keon Validation Authority (KVA) doesn't do path validation but informally committed to providing path validation by 4 January 2004 and will provide product for evaluation.

ACTION (017): Mr. Stillson will discuss the Entrust situation off-line to determine resolution of the issues and to figure out how to get Entrust personnel engaged in the lab to resolve the problems.

Agenda Item 5

Performance and Testing:

Microsoft: Mr. Tim Polk, NIST, reported that the name constraint issue has been resolved. There are some issues with Microsoft's approach, which chains on keys rather than use domain names, but they should not be showstoppers. It can be used, but it will require a lot of care. The issues appear to be in the details, but we can probably work around them. Will provide a follow-up update at the next PD-VAL meeting

Mr. Polk also will address the mail question, specifically the use of the Microsoft CAPI and still interoperate with the FBCA, at the next PD-VAL meeting.

DigitalNet: no report

Agenda Item 6

General Discussion:

Ms. Jenkins asked Mr. Stillson to send out the draft requirements document to the list that describes the XKMS and SCVP framework.

C. LIST OF ATTENDEES:

NAME	Email	Telephone	Organization
Brown, Chris	chris.j.brown@nist.gov	301.975.4764	NIST
Cooper, David	david.cooper@nist.gov	301.975.3194	NIST
Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681	eValid8
Horvath, Tom	tom.horvath@digitalnet.com	301.939.2728	DigitalNet
Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923	GSA
Johnson, Bob	johnson_robert@bah.com	410.684.6455	IATAC
Koziana, Kathy	kathleen.koziana@do.treas.gov	202.854.4900	Treasury PKI
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
Lins, Andrew	andrew.lins@mitretek.org	703.610.1905	MTS
Louden, Chris	clouden@enspier.com	703.299.3444	Enspier, Inc
Mitchell, Debbie	dmmitc3@missi.ncsc.mil	410.854.4900	DoD PKI PMO
Polk, Tim	tim.polk@nist.gov	301.975.3348	NIST
Silverman, Mark	mls@nih.gov	301.496.2317	NIH
Stillson, Ken	stillson@mitretek.org	703.610.2965	MTS
Tate, Darren	darron.tate@mitretek.org	703.610.1905	MTS
Weiser, Russ	rweiser@identrus.com	801.326.5421	Identrus

D. CURRENT ACTION ITEMS LIST

No.	ACTION STATEMENT	POC	Start Date	Due Date	Status
001	Coordinate efforts for agencies to participate in an e-mail signing demonstration	Brian Dilley, eValid8 Cheryl Jenkins, GSA		30 Oct 2003	Open
002	Test Goal #1 (Signed-E-Mail)	Ken Stillson, Mitretek		30 Oct 2003	Open
003	Provide Microsoft Summary Report from NIST Test Suite finding	David Cooper, NIST Tim Polk, NIST		30 Oct 2003	Open
004	Get LDAP IP Address	Andrew Lins, Mitretek		30 Oct 2003	Open
005	Use DigitalNet Test Suite as a starting point to define a FBCA-aware PD-VAL test suite	Ken Stillson, Mitretek		30 Oct 2003	Open
006	Re-post Test Results	Ken Stillson, Mitretek		30 Oct 2003	Closed
007	Write two documents by 7 Nov 2003 – 1) FBCA Demo – Goal 1 Architecture System Description document, and 2) FBCA System Differences document.	Ken Stillson, Mitretek	30 Oct 2003	07 Nov 2003	Closed
008	Coordinate with both Department of the Treasury and USDA/NFC about any future responsibilities or contributions for the FBCA demo testing.	Andrew Lins, Mitretek Ken Stillson, Mitretek	30 Oct 2003	20 Nov 2003	Open
009	Test the NIST concept of AIA fields and report his findings to the PD-VAL working group.	Ken Stillson, Mitretek	30 Oct 2003	20 Nov 2003	Closed
010	Request evaluation copies of the next version of the RSA and Entrust CAs for testing.	Andrew Lins, Mitretek	30 Oct 2003	20 Nov 2003	Closed
011	Re-distribute the path discovery system requirements (“back-end requirements”) document out to the PD-VAL list serve for review and comment by 7 Nov 2003.	Ken Stillson, Mitretek	30 Oct 2003	07 Nov 2003	Closed
012	Re-distribute the logging/auditing requirements document out to the PD-VAL list serve for review and comment.	Ken Stillson, Mitretek	30 Oct 2003	07 Nov 2003	Closed

013	Send softcopy of "FBCA OA E-Mail Exchange Demonstration (EED) Project 2003, Technical Guidance" report to email list for review and request comments by 26 Nov 2003.	Ken Stillson, Mitretek	20 Nov 2003	21 Nov 2003	Closed
014	Review "FBCA OA E-Mail Exchange Demonstration (EED) Project 2003, Technical Guidance" and submit comment to Mitretek by 26 Nov 2003.	All	20 Nov 2003	26 Nov 2003	Closed
015	Integrate comments received wrt technical guidance report and re-issue report.	Ken Stillson, Mitretek	20 Nov 2003	01 Dec 2003	Open
016	Arrange a teleconference with the team and government customers to discuss the level of effort required for the email demonstration, identify a proposed demonstration date, and discuss the need for a resigning ceremony.	Cheryl Jenkins, GSA	20 Nov 2003	26 Nov 2003	Open
017	Discuss the Entrust situation off-line to determine resolution of the issues and to figure out how to get Entrust personnel engaged in the lab to resolve the problems.	Ken Stillson, Mitretek	20 Nov 2003	01 Dec 2003	Open