

**Federal Bridge Certification Authority (FBCA)
Path Discovery & Validation (PD-VAL)
Working Group Meeting Overview
NIST North / Room 434
30 October 2003**

A. AGENDA

1. FBCA-aware Application Demo
 - a. Control Configuration
 - i. Infrastructure
 - ii. Desktop
 - b. Coordination of Agencies
2. Validation Systems and Tools
 - a. CAM
 - b. Intermediate Store
 - c. Spider
 - d. Entrust
 - e. RSA
3. Performance & Testing
 - a. Microsoft Updates
 - b. DigitalNet Updates
4. General Activities/Long Term
 - a. Uniformed expectations for PD-VAL
 - i. Enhance FPKI certificate, CRL, and repository profiles
 - ii. Path validation system requirements (“back-end requirements”)
 - iii. Logging/Auditing requirements
 - iv. Operational requirements
 - b. Desktop solutions and standards based DPD/DPV solutions
 - i. DPD/DPV requirements (“front-end requirements”)
 1. SCVP/XKMS profiles
 - ii. Vendor coordination [proposed “vendors – please do this” guide]
 - iii. [proposed] end-user “how-to” guide
5. Actions/Roundtable

B. MEETING ACTIVITY

Ms. Cheryl Jenkins, GSA and FBCA Operational Authority Administrator, called the meeting to order at 1:15 pm. She said that she would like future meetings to be 1-1.5 hours long, mainly composed of status reports on the technical work being done and progress on issues being solved.

Agenda Item 1

FBCA-aware Application Demo:

□ Control Configuration

➤ Infrastructure - Mr. Ken Stillson, Mitretek Systems (MTS), explained the status of the FBCA-aware Application Demo, keeping in mind the Goal 1 Architecture milestone of 31 December 2003.

The current status of the demo is being called, “Prototype Stand-in”. The following characteristics are currently evident with the demo system:

- A cross certificate has been established between the demo CA and the Higher Education Bridge Certification Authority (HEBCA).
- CAPI is working as expected. The AIA fields, as proposed/recommended by Microsoft, are correctly populated in the certificates being produced by the demo CA. CAPI works with WindowsXP.
- Testing has also been done with Windows2000 but additional testing has not been done to date with anything prior to Windows 2000 – partly due to time constraints to satisfy the Goal 1 Architecture milestones and partly due to direction to not test with older Windows versions at this time. Therefore, Windows XP will be the Operating System platform for this demo.
- The version of Outlook Email doesn’t effect path discovery processing - the different versions just provide different error messages.
- One current problem – Entrust doesn’t use SIA fields/extensions. This is not an immediate priority because the SIA extensions are not part of the Goal 1 Architecture. Mr. Mark Silverman asked for the parameters of the Goal 1 Architecture. One of the main differences between the demo and the production FBCA is the use of the AIA extensions.

Part of the demo is the use of Microsoft and Entrust relying party software, in all possible combinations (i.e. Microsoft to Microsoft, Microsoft to Entrust, Entrust to Microsoft, and Entrust to Entrust), can interoperate.

After some discussion about the demo testing, Ms. Jenkins asked for the following documents to be written by Ken Stillson, MTS:

- 1) Electronic Mail Demonstration Document - Goal 1 Architecture System Description document (e.g. description and configuration for the agencies participating in the demo.)
- 2) Electronic Mail Demonstration Report (i.e. lessons learned from the demo for entities to know how email works across the FBCA).

ACTION (007): Ken Stillson, Mitretek, will write two documents by 7 Nov 2003 – 1) Electronic Mail Demonstration and 2) Electronic Mail Demonstration Report.

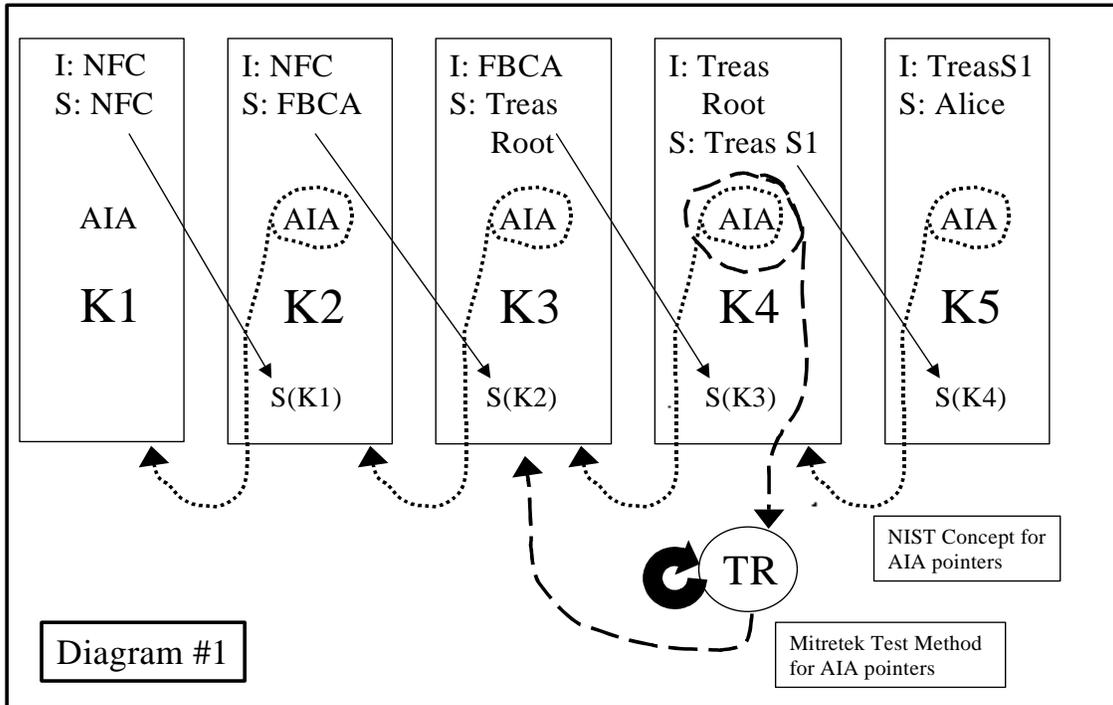
- Desktop – Software certificate users will have an easier time getting updated certificates that incorporate the AIA fields than DoD users with CAC cards (hardware tokens).
- Coordination of Agencies – USDA/NFC has recently agreed to be the other test partner. Department of the Treasury is already committed as a demo partner.

ACTION (008): The FBCA OA will coordinate with the Department of the Treasury and USDA/NFC about any future responsibilities or contributions for the Electronic Mail demonstration.

In other existing interagency interoperability efforts, Mr. Brian Dilley, eValid8 Corporation and Department of the Treasury representative to the PD-VAL, informed the attendees that Treasury, USDA/NFC, and Office of the Federal Registry (OFR) have only exchanged electronically signed documents to date, but will be expanding their testing soon. Mr. Stillson suggested that intermediate CAs and user certificates will need to have AIA fields to insure total interoperability. Mr. Dilley said that it won't be until Entrust CA, Version 7.0, that they will have the capability to populate the AIA field in certificates. Mr. Stillson thought that AIA fields must exist in intermediate CA certificates for CAPI and thus any signature or encryption functions to work.

This AIA field discussion led to diagramming some example certificates and each group describing what they believed was the correct function/purpose of the AIA field, resulting in Diagram #1. Mr. Stillson, Mitretek, in his demo testing, thought that the AIA field of intermediate CA's points to that certificate's issuer self-signed certificate which in turn points to the cross-certificates issued to the self-signed CA. For example, in Diagram #1, the Treasury Subordinate CA #1 (Treas S1) subscriber certificate was issued by the Treasury Root CA (Treas Root). So, the AIA field in the Treas S1 subscriber certificate points to the Treas Root self-signed certificate which points to the Treas Root subscriber certificate. NIST offered another perspective on how the AIA field works as a pointer. Mr. Polk and Mr. David Cooper thought that the AIA field is a more direct pointer because the AIA field in a subscriber certificate points to its issuer's subscriber certificate. For example, in Diagram #1, the AIA field in Alice's subscriber certificate points to its issuer's subscriber certificate, Treas S1. Mr. Stillson said he would alter his FBCA demo testing to validate the NIST concept of AIA fields and report his findings to this working group.

ACTION (009): Mr. Ken Stillson will test the NIST concept of AIA fields and report his findings to the PD-VAL working group at the next meeting.



Legend for Diagram #1:

I = Issuer

S = Subscriber

K# = Key Number

TR = Treasury Root self-signed certificate

S(K#) = Digital Signature of Subscriber certificate with Key # from Issuer

Agenda Item 2

Validation Systems and Tools:

- ❑ CAM – no updates reported on this topic at this meeting
- ❑ **Intermediate Store** – no updates reported on this topic at this meeting. This is a useful utility for testing when there are no AIA fields in the certificates, but any further enhancements are on hold now. The Intermediate Store is not necessary as part of the demo to meet the Goal 1 Architecture milestones.

Ms. Jenkins wonders if the Intermediate Store works with Windows98 or Windows95 but she hasn't tasked Mitretek to do any work in this area to date and doesn't foresee assigning this work in the future because Microsoft isn't supporting Windows98 or Windows95 after 31 December 2003.

- **Spider** – no updates from Mark Silverman at this time, further work is on hold until CAM issues are resolved.
- **Entrust** – It has been determined in testing is that it doesn't use or recognize SIA fields.
- **RSA** – Ken Stillson, Mitretek, is expecting a telephone call from an RSA VP before any more progress can be made.

Ms. Jenkins stated that she would work with the vendors to get the evaluation copies into the lab.

ACTION (010): Mitretek will request evaluation copies of the next version of the RSA and Entrust CAs for testing.

Ms. Jenkins informed the attendees that Mr. Dave Fillingham, NSA and Chair of the DoD PKI Technical Working Group (TWG), is also conducting a pilot now and is aware of the CAM and performance issues. Mr. Fillingham has contracted with various technical personnel from DigitalNet and Gemini Security – namely Mr. Rich Nicholas, Mr. Jon Pawling, and Mr. Peter Hess – to be involved in the DoD PKI – FBCA interoperability pilot. Ms. Jenkins would like Mr. Stillson to start getting involved with this pilot as well, to contribute lessons learned from e-mail exchange across the FBCA.

Agenda Item 3

Performance & Testing

- Microsoft Updates – Microsoft tested their software against the NIST test suite and the results were not sent to NIST for review. NIST is awaiting these results to determine which path this group should pursue to ensure FBCA interoperability with Microsoft products.

The FBCA OA shared that the Microsoft cross-certification was not approved. Ms. Jenkins expressed that she would like a teleconference to take place between Microsoft; Ms. Michelle Moldenhauer, Treasury and Chair of the Federal PKI Policy Authority; Mr. Tim Polk, NIST and Chair of the Federal PKI Certificate Policy Working Group; and others to discuss the status of Microsoft testing and products with the FBCA.

- DigitalNet Updates – Mr. Stillson reported that there have been improvements but there are integration issues between CAM and the new CML that are interfering with testing. The source of the interference is not clear – the CAM, CML, or something else. He believes that there is only a few more hours of work left to finish this portion of the work. Ms. Jenkins authorized Mr. Stillson an one week time period to coordinate the completion of this work with DigitalNet.

Agenda Item 4

General Activities/Long Term

- Uniformed expectations for PD-VAL
 - Enhance FPKI certificate, CRL, and repository profiles – no updates reported on this topic at this meeting.
 - Path discovery system requirements (“back-end requirements”) – Mr. Stillson sent out version 0.4 of the “back-end requirements” with an expectation of getting comments by 7 Nov. He’ll send them out again to make sure everyone received them.

ACTION (011): Mr. Ken Stillson, Mitretek, will 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.

- Logging/Auditing requirements – Mr. Stillson had previously distributed the logging/auditing requirements paper but he will send it out again and request comments.

ACTION (012): Mr. Ken Stillson, Mitretek, will re-distribute the logging/auditing requirements document out to the PD-VAL list serve for review and comment.

- Operational requirements – no updates reported on this topic at this meeting
- Desktop solutions and standards based DPD/DPV solutions – all of the efforts under this agenda item are on hold while the Goal 1 Architecture effort is underway.

Agenda Item 5

Actions/Roundtable

Mr. Silverman asked if the current FBCA cross-certified members (i.e. Treasury, NASA, USDA/NFC, and DoD) are aware of the AIA field implementation. NIST representatives said that they can’t enforce the use or incorporation of AIA fields by these currently cross certified PKI members. However, based on our experience with these member PKIs, it is anticipated that they will maintain consistent in their PKI implementations with any technical developments in the FBCA.

Next PD-VAL meeting – the next meeting is scheduled for Thursday, 20 Nov from 2:00-3:30pm at the NIST North facility.

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
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
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

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	Done
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	Done
005	Use DigitalNet Test Suite as a starting point to define a FBCA-aware PD-VAL test suite	Ken Stillson, Mitretek		30 Oct 2003	Done
006	Re-post Test Results	Ken Stillson, Mitretek		30 Oct 2003	Done
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	Done

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	Done
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	request done; s/w pending
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	Done
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	Done