Federal Public Key Infrastructure (FPKI)
Path Discovery & Validation (PD-VAL) Working Group
Minutes of the 14 April 2005 Meeting
NIST North, Gaithersburg, MD; Room 618

A. AGENDA

1) Opening Remarks / Introductions
2) Discussion on Meeting Minutes
3) Discussion on Action Items
4) Interim Validation Solution Update
5) Test Cases Update
6) Qualify Validation Process for Products and Services
7) Other Topics
8) Next Meeting Plans/Meeting Adjourned

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Defense	Mitchell, Deborah	dmmitc3@missi.ncsc.mil	Teleconference
Dept of Commerce (NIST)	Cooper, David	david.cooper@nist.gov	301.975.3194
Dept of State	Edmonds, Deborah	edmondsdd@state.gov	202.203.7984
Dept of State	Russell, William	russellwc@state.gov	202.203.5044
Enspier	Blanchard, Debb	dblanchard@enspier.com	Teleconference
Enspier	Silver, David	dsilver@enspier.com	Teleconference
FICC Support	Petrick, Brant	brant.petrick@gsa.gov	202.208.4673
FPKIA OA, Program Manager (GSA)	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923
MitreTek	Lins, Andrew	andrew.lins@mitretek.org	703.610.1786
NFC	Maldonado, Diana	diana.moldonado@nfc.gov	Teleconference
NFC	Sharp, Kathy	kathy.sharp@nfc.gov	Teleconference
NIH	Silverman, Mark	mls@nih.gov	301.496.2317
Orion Security Solutions	Shorter, Scott	sshorter@orioinsec.com	703.917.0600
PD-VAL Secretary (IATAC)	Clemons, Darryl	clemons_darryl@bah.com	410.684.7732
SRA	Tin2, Ganta	Tin2_ganta@sra.com	571.917.1490

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks:

The meeting was called to order at 9:46 a.m.

Ms. Cheryl Jenkins, GSA, began the meeting session by announcing that the meeting would be more or less a status meeting that would provide where we are and what we will be doing in the near future and that participation from both industry and government will be needed in completing the future work. Ms. Jenkins informed the group that the RFI was distributed to prospective vendors on 4 April and that the deadline for submitting responses to the RFI had been extended until 22 April. She stated that the RFI was deliberately written to favor no particular protocol. She mentioned that since the preferred protocol, Simple Certificate

Validation Protocol (SCVP), is not available to the Federal government at this time, functional validation requirements will be developed by which the vendors must meet prior to being selected to test their products in the E-Authentication Lab. Ms Jenkins stated that it is the responsibility of the Path Discovery and Validation Working Group (PD-VAL WG) to select the vendors based on their responses to the RFI. She stated that the goal is to have the vendor products and services selected and into the lab by the first week of June.

Agenda Item 2

Discussion on Meeting Minutes

The minutes from the previous meeting were reviewed, ratified, and approved for posting to the PD-VAL website by the PD-VAL members.

Agenda Item 3

Discussion on Action Items

The actions items were reviewed, ratified, and approved for posting to the PD-VAL website by PD-VAL members. Each open action item was reviewed and evaluated for a status change.

Agenda Item 4

Federal PKI Interim Validation Solution Update

Ms. Jenkins provided background knowledge on the future direction of CAM and the validation solution for those who were not present when this topic was discussed at a previous meeting. She stated that there are two activities that we are trying to achieve in the validation space:

1) Provide validation services and products to government entities, and

2) Support current customers using the CAM while gradually decommissioning the CAM

Prior to completely removing CAM, successfully tested validation services and products must be placed on the E-Authentication list. But until this happens, the CAM services will be available in parallel with the development of this list. Agencies will have the option of selecting one of the successfully tested products and/or services from the list.

Mr. Andrew Lins provided details on the current state of the CAM stress testing. Mr. Lins stated that presently the CAM (also known as the Interim Operating Capability Multi-Protocol Validation System) only does certificate trust list mode, it does not support path discovery and validation. The current effort is to ensure that the CAM version, CAM 4.0 RC8, that supports path discovery and validation can do this function without breaking any other systems. CAM 4.0 RC8 was tested in the production environment across the FPKI directory using the Common Policy CA as a trust anchor. A validation of the State of Illinois certificate was performed

initially and the test failed. The test was redone using a DST ACES certificate and the certificate was successfully validated, although there were some problems.

The test with the State of Illinois certificate CAM had problems calling CML, specifically the Storage and Retrieval Library (SRL). In order for CAM to validate any certificates after the problem calling the SRL occurred, the CAM had to be rebooted.

When the test was done using DST ACES certificates, CAM was successful in validating all of the certificates although under high loads CAM would lockup. CAM modifications were made that resolved this problem.

Another problem occurred if a revoked CA certificate was found in a path, CAM would incorrectly respond with "certificate revoked", rather than "No Path Found".

After some modifications CAM 4.0 RC8 was promoted to RC9 and the following issues were resolved:

- CAM lockup error under high loads
- CAM returning wrong error code when a revoked CA certificate was found in the path (i.e., the path should no longer be found), and
- Other minor fixes

The test was redone using CAM 4.0 RC9, using a simulated environment of the FPKI directory and the Illinois certificates/CRLs stored in a single OpenLDAP directory. The test was a success with no returned errors.

The initial test was repeated with the production FPKI directory and the State of Illinois. The certificate validation process failed. CAM reported many unknown errors on several attempts. As before, after a short period of testing, CAM was unable to start SRL without rebooting CAM.

Mr. Lins stated that from evidence from the test, it seems that the problems stems from issues with the directories.

Action Item 27: Test CAM with FPKI/Illinois Directory using LDAP Chaining or Referrals

Action Item 28: Test ACES with new CAM version to determine if the past problems are resolved

Agenda Item 5

Test Cases Update

Mr. David Cooper began the discussion by explaining the latest situation with the test cases. Mr. Cooper stated that he believes that the path discovery validation test cases are complete. The delay is stemming from problems involved in compiling a program that takes text descriptions of the certificates and CRLs from the test suite and generates certificates and CRLs from them. Once the program is compiled and is running properly then the testing can began. Mr. Cooper

felt quite confident that the test cases data was correct even though he had not tested them but he would be more certain once certificates and CRLs are generated and could be tested using some path discovery and validation software.

Mr. Cooper also mentioned that the Basic level test cases were more difficult than expected. Mr. Cooper wanted to ensure that path discovery modules that could pass the Basic level tests would be capable of building certification paths across the entire FPKI, as it current exists. After downloading certificates and CRLs from the FPKI directory, it turned out that the FPKI architecture was more complex than he first expected. This complexity is reflected in the test cases at the Basic level.

Action Item 29: Estimate a timeframe to develop a Test Plan using PKITS and the path discovery test suite

Agenda Item 6

Qualify Validation Process for Products and Services

Ms. Jenkins facilitated a group discussion to develop a process to qualify validation products and services. She stated that the group must find an approach whereby we can present to the agencies or entities the evaluation findings. She provided two action items that the process must be based upon:

1) Qualify Test
    a.) Threshold (mandatory requirements)
    b.) Package after qualifying
        i) Lab Agreements
        ii) Non-disclosure Agreements
2) Qualify for Validation List

The group developed the following process to qualify a product or HVS:

1) PD-VAL Receives RFI from the vendors
2) RFI is evaluated
3) RFI is provided with a score
4) Based on the total number of score, determine a threshold
5) Determine which vendor will be tested based upon the thresholds
6) After testing, lab provides a status
7) Status is sent to PD-VAL WG for review and comments
8) Vendors are notified of the PD-VAL WG's comments and a meeting is scheduled with them to resolve any residual issues (if any).
9) PD-VAL WG makes a recommendation on the product and/or service to the E-Authentication Program Executive based on the final outcome of the meeting.
10) The Program Executive will determine products and/or services that will be added to the trust list.

The group discussion also resulted in two separate draft Baseline Requirements tables that may be used to facilitate the aforementioned process:

Product Baseline							
	Reqmts	Vendor Initial	Score	Lab	Status	PD-VAL WG	Final
1							
2							
3							
4							
Options:							
Synopses:							
Totals:							

HVS Baseline							
	Reqmts	Vendor Initial	Score	Lab	Status	PD-VAL WG	Final
1							
2							
3							
4							
Options:							
Synopses:							
Totals:							

Action Item 30: Develop baseline requirements for the Trust List & PD-VAL for Hosted Validation Services (HVS) and Products

Agenda Item 7

Other Topics

No other additional topics were discussed.

Agenda Item 8

Next Meeting Plans / Meeting Adjourned:

The next PD-VAL Meeting is scheduled for 12 May 2005 from 09:30 a.m. - 12:00 p.m. at the NIST North facility, Room 618, Gaithersburg, MD. The meeting adjourned at 11:59 am.

D. PD-VAL CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
FY05-27	Test CAM with FPKI/Illinois Directory using LDAP Chaining or Referrals	Andrew Lins, Mitretek	14 April PD-VAL meeting	TBD	**Open**
FY05-28	Test ACES DST with new CAM version to determine if the past problems are resolved	Andrew Lins, Mitretek	14 April PD-VAL meeting	22 April PD-VAL	**Open**
FY05-29	Estimate a timeframe to develop a Test Plan using PKIX and the path discovery test suite	David Silver, Enspier	14 April PD-VAL meeting	22 April PD-VAL	**Open**
FY05-30	Develop baseline requirements for the Trust List & PD-VAL for HVS and Products	Cheryl Jenkins, GSA	14 April PD-VAL meeting	29 April PD-VAL	**Open**