Federal Public Key Infrastructure (FPKI)
Path Discovery & Validation (PD-VAL) Working Group
Minutes of the 12 May 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) Vendor RFI Update
5) Interim Validation Solution Update
6) Test Cases Update
7) Validation Report
8) Other Topics
9) Next Meeting Plans/Meeting Adjourned

B.   ATTENDANCE LIST

Organization	Name	Email	Telephone
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	Teleconference
Enspier	Simonetti, David	david.simonetti@enspier.com	Teleconference
FICC Support	Petrick, Brant	brant.petrick@gsa.gov	Teleconference
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
Sun Microsystems	Elley, Yassir	yassir.Elley@sun.com	Teleconference
Orion Security Solutions	Shorter, Scott	sshorter@orionsec.com	Teleconference
USDA/NFC	Morgan, Shiela	shiela.morgan@usda.gov	Teleconference
ElectroSoft	Gupta, Sarbari	sarbari@electrosoft-inc.com	703.918.4905

C.   MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks:

The meeting was called to order at 9:40 a.m.

Ms. Cheryl Jenkins, GSA, began the meeting session by announcing that this meeting was a status meeting that would provide where we are in the RFI process and what we will be doing in the near future to qualify validation products and services for federal agency use.

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

Vendor RFI Update

Ms. Jenkins stated that the process to qualify validation products and services was not used to qualify validation products and services for testing. She stated that the group reviewed all of the responses in relationship to the requirements to determine qualification.

She shared with the group that four (4) vendors (i.e., Gemini Security, Tumbleweed, Operational Research Consultants, and CoreStreet) had been invited into the E-Authentication Lab for testing. There are also four (4) other vendors that may qualify upon receiving clarification about their product or upon receiving a product name for those that submitted responses for a toolkit.

After testing, the lab will provide a status report of the testing to the PD-VAL WG for review and comments. Vendors will be notified of the PD-VAL WG comments and a meeting will be scheduled with them to resolve any residual issues (if any).

Action Item 31: Provide a template of the recommendation letter to qualify products and services to the PD-VAL WG for review and comments.

Agenda Item 5

Federal PKI Interim Validation Solution Update

Ms. Jenkins reiterated from last meeting that prior to completely removing CAM services, successfully tested validation services and products must be placed on the E-Authentication Validation 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 the CAM 4.0RC9, featuring path discovery and policy OID filtering, was tested with ACES and FPKI/Illinois Directory using LDAP chaining and referrals to determine if the past problems would be resolved. The 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 and their compatibility with CAM.

Agenda Item 6

Test Cases Update

Mr. Cooper discussed the Path Discovery Test suite. He stated NIST has not yet been able to generate the test data that is described in section 5 of the document, but hopes to be able to do so soon. If any errors are discovered when the test data is generated, then the appropriate changes will be made to section 5, but he does not anticipate the need to make any significant changes before the tests are used by the E-Authentication Lab.

Mr. Cooper stated that the Department of Defense (specifically NSA) has provided eight (8) hours of contractual support to NIST to resolve the 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.

Ms. Jenkins requested that the test suites be delivered to the E-Authentication Lab on June 1, 2005; as the path discovery test will be followed by the path validation testing.

He said once the test data has been generated, he will be posting a document along with the test data on the NIST Web site and will allow people to review and comment on the document. Changes made to the test suite based on these comments will be incorporated into the final version of the test suite, but may not be incorporated in the version that will be used by the E-Authentication lab in June.

He also mentioned that the draft NIST Recommendation for X.509 Path Validation includes a test plan for path validation modules (PVMs) that, at a minimum, implement all of the functionality required for an Enterprise PVM. The document includes an appendix that lists all of the tests in PKITS and indicates whether the test should be run and provides a hint about the expected outcome of the test. The set of tests to run and the outcomes depend on the particular functionality implemented by a PVM.

Action Item 32: Provide path validation test plan to the PD-VAL WG for review and comments.

Agenda Item 7

Validation Report

A program written by Mr. Cooper that generates a customized version of the table in the appendix of the NIST Recommendation was projected for the in-person attendees. After providing the program with information about the functionality implemented by a PVM, the program generates an HTML file with a table listing every test in PKITS and indicating the expected result of running each test with the PVM. The top of the HTML file lists the inputs that were used to generate the table, with functionality that is not implemented by the PVM marked using strike through text. The table has one row for each test and each row lists the test name, the expected result for the test, and includes an empty column for writing the actual test results.

Mr. Cooper proposed that the E-Authentication Lab should use this table to report its test results. In order to simplify reviewing the results, the lab could either delete any row from the table where the actual result corresponded to the expected result or could provide the entire table but

with the rows in which discrepancies occurred highlighted.

Ms. Sarbari Gupta suggested adding a new column for the lab to add notes or comments from the testing and it was agreed that any comments about a test result could be either be included in a new column or in the column that includes the test results.

Action Item 33: Provide test suite and program to the PD-VAL WG for review and comments.

<div align="center">

Agenda Item 8

</div>

Other Topics

<div align="center">

Agenda Item 9

</div>

Next Meeting Plans / Meeting Adjourned:

The next PD-VAL Meeting is scheduled for 14 July 2005 from 09:30 a.m. - 12:00 p.m. at the NIST North facility, Room 618, Gaithersburg, MD. An interim meeting, which will be limited to government employees, contractors with no conflict of interest, and contractors supporting a federal agency's PKI, will be held in June to review the test results from the E-Authentication lab. The meeting adjourned at 10:55 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	02 May	**Closed**
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	02 May	**Closed**
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	05 May	**Closed**
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	**Closed**