

Path Discovery & Validation (PD-VAL) Working Group

Minutes of the 15 September 2005 Meeting

NIST North Building, West Diamond Avenue, Gaithersburg MD 20878/ Room 618

A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Overview of Vendor Test Results
- 3) Report on Adobe Meetings
- 4) Vendor Update
- 5) GSA's Validation Demo Update
- 6) Other Topics
- 7) Adjourn Meeting

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Department of Commerce (NIST) /PD-VAL Co-Chair	Cooper, David	david.cooper@nist.gov	301-975-3194
Department of State (Mount Airey Group)	Russell, William	russellwc@mountaireygroup.net	571-344-1671
Department of Defense	Mitchell, Deborah M.	dmmittc3@MISSI.NCSC.MIL	Teleconference
GSA/OGP	Giles, April	april.giles@gsa.gov	Teleconference
FPKI OA Program Manager/PD-VAL Chair	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571-259-9923
FICC support (FC Business Systems)	Petrick, Brant	brant.petrick@gsa.gov	202-208-4673
Secretariat (Enspier Technologies)	Fincher, Judy	Judith.fischer@enspier.com	703-299-3444
FPKI OA (Mitretek)	Lins, Andrew	andrew.lins@mitretek.org	Teleconference
Tumbleweed (vendor)	Ebbets, Steve	Steve.Ebbets@TUMBLEWEED.COM	Teleconference
SRA	Ganta, Tin2	Tin2_ganta@sra.com	Teleconference
Department of State	Edmonds, Deborah D.	EdmondsDD@STATE.GOV	
Electrosoft Services	Gupta, Sarbari	sarbari@ELECTROSOFT-INC.COM	703-217-8475
Dartmouth	Rea, Scott	Scott.Rea@DARTMOUTH.EDU	Teleconference
CoreStreet, Ltd. (vendor)	Dulude, Bob	bob@corestreet.com]	Teleconference
CoreStreet, Ltd. (vendor)	Briley, Jr, James	jbriley@corestreet.com	301.318.5096
Interoperability Lab	Russell, Arthur	Arthur.russell@enspier.com	Teleconference
Tumbleweed (vendor)	Smith, Ann	Ann.Smith@TUMBLEWEED.COM	Teleconference
Orion (vendor)	Wallace, Carl	cwallace@orionsec.com	703-917-0060 Ext 28
LS3 (contractor)	Roberts, Steve A.	steve@LS3-INC.com	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions

Ms. Cheryl Jenkins

Ms. Cheryl Jenkins, FPKI OA Program Manager and PD-VAL Chair, called the meeting to order at 9:30 a.m. with attendee introductions.

Agenda Item 2

Overview of Vendor Test Results – Mr. David Cooper, NIST

The PD-VAL WG put out an RFI for COTS products that perform Path Discovery and Validation of certificates. There was a brief review of vendors who responded to the RFI and whose products are currently being tested in the E-Authentication Interoperability Lab:

- Tumbleweed Communications
- CoreStreet, Ltd.
- Orion Security Solutions
- Silanis.

Mr. Arthur Russell, the E-Authentication Initiative Contractor at the Interoperability Lab run by Enspier Technologies, and Mr. David Cooper described this testing.

CoreStreet, Ltd.

Mr. Russell stated that the CoreStreet testing is not complete. CoreStreet provided 3 products for testing:

- RTC Authority 5.0 build 22 Windows
- Validation Client 3.0 build 6 Windows
- Responder 5.0 build 22 Windows.

There was a setback due to past configuration procedures. The past configuration allowed a duplication of certificates and that caused a problem. Mr. Russell had to clean up the database and start anew. Testing was to resume today (9-15-05) and he planned to compile the results by COB.

Mr. David Cooper reported on the remaining vendors.

Tumbleweed Communications

Tumbleweed provided two products for testing:

- Desktop Validator 5.0 Windows
- Validation Authority 5.0 Windows.

We tested the Microsoft IIS plug-in. The Path Discovery test produced correct results when the Basic and Rudimentary tests were run. In a few cases, the validation server provided different results than the user. Tumbleweed provided a patch and it then passed the Path Validation test.

The Desktop Validator supports Microsoft Outlook 2000 and 2003.

Orion

Orion tested Webcullis version 1.0 and Security plug-in for IIS. It passed the Path Discovery tests and all but one of the 230 Path Validation tests. Two configurations were tested for Path Discovery: Rudimentary and Basic. A configuration problem was encountered which caused IIS to reject the cert before passing it to the plug in. Mr. Cooper noted that there were “no security implications.” “This is a configuration issue, not a trust issue,” he stated.

Orion’s web server plug-in supports both Apache and Microsoft IIS.

Silanis

The Silanis product (ApproveIt) was tested with Certificate Management Library (CML). The test results did not line up with CML, so Silanis is re-testing the product in their own lab and will get back to us.

ACTION: Ms. Cheryl Jenkins and Mr. David Cooper will put together a synopsis (written report) of the Interoperability Lab’s testing status and results as of 9/15/05.

Ms. Cheryl Jenkins reported that the Designated Approving Authority (DAA) has been identified for those vendors wanting to host validation products. Ms. Jenkins advocates that vendors will not have to go through the entire certification and accreditation. ‘Delta’ requirements may be all that is needed to get on board.”

Entrust

Ms. Jenkins also noted that Entrust has submitted four products to the lab, consisting of:

- Product
- Tool kit
- Application.

We need to get a lab evaluation agreement in place before the Enspier begins testing in the E-Authentication Program Management’s Lab, she stated.

Agenda Item 3

Report on Adobe Meetings – Mr. David Cooper, NIST

Mr. Cooper has been in touch with Adobe since the Public Key Infrastructure Research and Development Workshop in April 2005 and more recently, when Adobe made a presentation at the Certificate Policy Working Group (CPWG) meeting on August 24.

Both Acrobat and the free Reader (V7.0) have a document signing capability which would be useful for private citizens interacting with government, i.e., they could download a tax form that has been digitally signed.

The Federal PKI Policy Authority (FPKIPA) is interested in its capability and is looking into a two-way cross-certification with Adobe: However, it may be a one-way certificate to the FBCA. The FPKIPA needs to analyze whether a cross-certification with Adobe is in the best interest of the federal government.

The challenge is that Adobe currently has path validation capability, but they don't perform path discovery.

Mr. William Russell reported that the Department of State had recently done a demo using the USPTO digital signature (a project with Adobe) and it failed because the signing cert had expired. The Department of State cert is only valid for three years.

Ms. Cheryl Jenkins noted that PD-VAL is planning to put the Adobe products into the E-Authentication PMO's lab to test it against the Path Discovery and Validation test suites. She noted that the CPWG is currently mapping the Adobe X.509 CP (RFC 2527) to that of the FBCA CP (RFC 3647).

Agenda Item 4

Vendors Update – Mr. Steve Ebbets (Tumbleweed) & Mr. Carl Wallace (Orion)

Tumbleweed (Mr. Steve Ebbets)

Mr. Ebbets reported that two products were tested in the interoperability lab:

- A client plug in for signed email (Path Discovery and Validation)
- A validation server.

Tumbleweed is teaming with ORC to offer a hosted validation service. ORC will stand up a validation server with a OCSP/SCVP responder and the VA server; it works as a standalone or as a server.

Mr. Ebbets noted there are three additional products to test:

- Apache/Netscape plug in (server validator)
- IIS plug in
- Tool kit: C++ and Java are under development. There is no firm date, but either before the end of this year or beginning of next year.

Orion (Mr. Carl Wallace, for Scott Shorter)

Mr. Wallace reported that Webcullis IIS plug in was tested and that it does Path Discovery and Path Validation beyond what IIS can perform. He also noted that the Apache version of Webcullis is ready for testing (on Linux and Unix platforms).

ACTION: Art Russell is to contact Scott Shorter of Orion to get the Apache version of Webcullis into the E-Authentication interoperability lab.

Agenda Item 5

GSA's Validation Demo Update – Ms. April Giles, GSA

Ms April Giles of the GSA/OGP, who is leading this effort, reported that she is currently waiting on the contract to go through and had no additional information on the demo at this time.

Ms. Cheryl Jenkins noted that this will be a limited funded contract where only a few products will be picked up and funded. “We are working with the lab to determine the best interests of the government,” she said.

Agenda Item 6

Other Topics

Ms. Deborah Mitchell reported that the DoD is trying to lock down the web server environment so that will be a consistent way to validate certs and processes in a bridge environment.

ACTION: Ms. Deborah Mitchell will check with DoD on the use of Orion GOTS product(s) by other federal agencies.

Ms. Jenkins reminded participants that meeting minutes will be posted to the web site: www.cio.gov/FBCA (under Working Groups, PD-VAL, Minutes).

The sales Point of Contact for Orion is Mr. Scott Shorter and for Tumbleweed, Ms. Ann Smith.

Agenda Item 7

The meeting was adjourned at 10:20 a.m.

PD-VAL Current Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
1	Put together a synopsis (written report) of Interoperability Lab testing status and results as of 9/15/05.	Cheryl Jenkins, David Cooper	Sept. 15, 2005	Oct. 13, 2005	Open
2	Contact Scott Shorter of Orion to get the Apache version of Webcullis into the interoperability lab.	Arthur Russell	Sept. 15, 2005	Sept. 30, 2005	Open
3	Check with DoD on the use of Orion GOTS product(s) by other federal agencies.	Deborah Mitchell	Sept. 15, 2005	Sept. 30, 2005	Open
4	Provide comment on the 11 August Minutes.	Cheryl Jenkins	Sept. 15, 2005	Sept. 16, 2005	Open