Path Discovery & Validation (PD-VAL) Working Group

Minutes of the 08 December 2005 Meeting

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

A. AGENDA

1. Welcome & Opening Remarks/ Introductions
2. PD-VAL Current Activities and Update
   a) Validation Methodology & Criteria
   b) Overview of Vendor Test Results
      i. Tumbleweed
      ii. CoreStreet
      iii. Orion
      iv. True Pass
   c) Hosted Validation Requirements
   d) CML Performance Issues
3. Other Remarks
4. Adjourn

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Entrust (vendor)	Boeyen, Sharon	sharon.boeyen@entrust.com	Teleconference
CoreStreet, Ltd. (vendor)	Briley, Jr, James	jbriley@corestreet.com	Teleconference
Department of Commerce (NIST) PD-VAL Co-Chair	Cooper, David	david.cooper@nist.gov	301-975-3194
CoreStreet, Ltd. (vendor)	Dulude, Bob	bob@corestreet.com	Teleconference
Department of State	Edmonds, Deborah D.	EdmondsDD@STATE.GOV	Teleconference
Enspier	Fincher, Judy	Judith.fincher@enspier.com	Teleconference
SUN (vendor)	Freedman, Richard	Richard.Freedman@SUN.COM	Teleconference
Entrust (vendor)	Gopal, Gautam	Gautam.gopal@entrust.com	Teleconference
FPKI OA Program Manager/PD-VAL Chair	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	
Secretariat (Enspier Technologies)	Lazerowich, Steve	Steve.lazerowich@enspier.com	
Department of Defense	Mitchell, Deborah M.	dmmitc3@MISSI.NCSC.MIL	Teleconference
FICC support (FC Business Systems)	Petrick, Brant	brant.petrick@gsa.gov	202-208-4673
Department of State (Mount Airey Group)	Russell, William	russellwc@mountaireygroup.net	571-344-1671
Orion (vendor)	Shorter, Scott	sshorter@orionsec.com	Teleconference
National Institutes of Health	Silverman, Mark	mls@nih.gov	301-496-2317
Tumbleweed (vendor)	Smith, Ann		Teleconference
DOJ	Young, Siegfreid	Siegfreid.young@usdoj.gov	202-616-8989

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 9:35 a.m. with attendee introductions.

Ms. Jenkins indicated the next PD-VAL meeting would take place in February when the 2006 schedule has been determined.

Agenda Item 2

PD-VAL Current Activities and Update

a) Validation Methodology & Criteria– Ms. Cheryl Jenkins

Ms. Jenkins indicated that she expects the path discovery and validation process to be formalized and documented in a draft "criteria and methodology" document for review in the January 2006 timeframe.

b) Overview of Vendor Test Results

Mr. David Cooper, PD-VAL Co-Chair, provided an update on the status of the four products that have been tested:

Tumbleweed Communications: testing has been completed. The Tumbleweed product includes a validation server and at least one plug-in for Microsoft Outlook. Communication between the client and the validation server is accomplished using a draft version of the SCVP protocol. While the test results demonstrated that the validation server performs path discovery and validation correctly, there was concern about the user interface provided by the Microsoft Outlook plug-in. When using the plug-in, the user is presented with the correct information by a Tumbleweed pop-up, but the user is also presented with the results of Microsoft CAPI's validation of the certificate, which is sometimes incorrect. Proper training would be required to ensure that users would understand which information is correct and which information should be ignored. Mr. Cooper suggested agencies considering Tumbleweed's Microsoft Outlook plug-in arrange for in-house demos so the agencies may determine for themselves how much of a factor this might be.

During on the ensuing discussion, Mr. Mark Silverman asked how Tumbleweed's Microsoft Outlook plug-in would behave if a message arrived that had an invalid signature, but in which the signature was associated with a valid certificate. The concern was that the plug-in would present a pop-up indicating that the certificate was valid and that the only indication that the message signature was invalid would be the message presented by Microsoft Outlook. If this were the case, it would be unacceptable since users would be trained to ignore the message presented by Microsoft Outlook since that message is unreliable. Mr. Cooper agreed that this was a concern and indicated that testing should be undertaken to determine the Tumbleweed plug-ins actual behavior in this scenario. Mr. Cooper and Ms. Jenkins reiterated their confidence that Tumbleweed's validation authority is performing correctly, although additional testing in the lab may be required.

Tumbleweed partners with ORC to provide hosted validation services. Agencies should approach ORC for more information and pricing.

CoreStreet, Ltd.: Testing is complete. CoreStreet's offering consists of a delegated path discovery server, PathBuilder 1.0, and a client that uses the information provided by the server to perform path validation. While the client/server combination is capable of performing path discovery and validation as required in the Federal PKI, there is one limitation that results from the way that CoreStreet processes revocation information. Rather than sending CRLs to the client for processing, the CoreStreet server uses CRLs to generate pre-signed OCSP responses, which are sent to clients as necessary to determine the status of certificates. This method has some advantages in terms of efficiency and will work correctly in most cases, however there can be a problem when it is necessary to provide status information for a certificate that is issued by a CA that only generates segmented CRLs. Since determining the certificate status for such a CA would require obtaining a copy of every CRL segment issued by the CA, and since there is no way for the OCSP response generator to verify that it has obtained every such CRL segment, the OCSP response generator must either refrain from creating OCSP responses for CAs that do not issue full CRLs or create OCSP responses for such CAs and accept the risk that it may provide incorrect status information for some certificates. CoreStreet has made their OCSP generator configurable so that it can work either way and the PD-VAL WG recommends configuring the server so that status information is only provided for CAs that issue full CRLs. This should not cause significant problems in practice since most CAs that are part of the Federal PKI issue full CRLs and if there are any CAs that do not issue full CRLs, those CAs could be easily reconfigured so that they do issue full CRLs.

Mr. Mark Silverman asked how the server would respond if presented with a certificate that was issued by a CA that was previously unknown to the server. Mr. Cooper responded that information about every CA in the PKI needs to be manually configured into the server and that the client would not be able to validate certificates issued by a CA that was not included in this configuration information. Mr. Bob Dulude of CoreStreet clarified that the CoreStreet product indicates the status of such a certificate as "unknown" and does not indicate the certificate is invalid. Mr. Dulude also indicated that a spider/crawler capability maybe added in the future to address this potential issue.

CoreStreet partners with CyberTrust to offer the delegated path discovery server as a hosted service. Pricing and availability off the GSA Schedule is in process.

Orion Security Solutions: Mr. Cooper indicated there are no recent technical updates to report on Orion's WebCullis product. There are, however software licensing issues that require resolution. WebCullis is based on the PKIF toolkit and DoD provided funding for some of this work. It is available as open source software. As a result, the software license itself is available at no cost to agencies. Support, however, has not yet been addressed and there is risk that agencies may modify the code resulting in multiple, divergent versions of the software.

Ms. Jenkins has spoken with Dr. Santosh Chokhani and Orion has agreed to do configuration management to avoid the above potential problem. Orion will publish the software on the open source software web site. The issue of how Orion is funded to provide configuration management remains open and DoD is involved in those discussions. It is possible that a solution may be arrived at by January 2006.

Mr. Scott Shorter (Orion) indicated that version 2 of PKIF is under development and will provide the capability to run on Unix platforms. This new version will be included in the above referenced licensing and support discussions.

Mr. Cooper emphasized that WebCullis uses a fat-client architecture.

Entrust: The initial round of testing of the TruePass product has been completed and issues have been uncovered. Entrust is actively investigating these issues and next steps will be determined based on their review. Ms. Jenkins urged Entrust to resolve the issues as soon as possible after the holidays, because Treasury, an e-Authentication PKI customer needs this product to work with their PKI application as a prerequisite to joining the E-Authentication Federation.

Ms. Jenkins was asked if the Entrust validation service will be tested and she is amenable to this testing going forward.

c) Hosted Validation Requirements – Ms. Cheryl Jenkins

Ms. Jenkins provided high-level guidance on how the criteria and methodology document will define acceptance criteria for agencies wishing to use these PD-Val products.

If an approved product is currently in use in an accredited environment, the agency will be required to undergo an independent review of the product's configuration to ensure it conforms to the configuration used to test the product and perform a verification test in the agency's environment. The independent reviewer must inform the Designated Approving Authority and the PD-VAL WG of this effort.

If an agency wishes to add an approved product to their current accredited environment, the agency must undergo a risk assessment and an independent reviewer must inform the Designated Approving Authority and the PD-VAL WG of this effort. Templates of this letter, and other appropriate letter templates, will be made available via the PD-VAL web site. Ms. Jenkins indicated these letter templates have now been approved by the CIO's office.

d) CML Performance Issues

Mr. William Russell spoke to this issue. The State Department has uncovered fairly severe scalability issues (i.e., it takes approximately 17 hours to run the test suite 20 times) during testing of the CML library written by BAE Systems. Mr. Tom Horvath of BAE Systems has confirmed the problem but BAE has indicated they are not currently funded to correct the problem.

Mr. Cooper inquired if State has also run a second set of path discovery tests and Mr. Russell said they have not done so at this time. The issue of whether or not PD-VAL WG should also investigate scalability testing was raised and the sense of the group is that such testing would be appropriate.

Mr. Russell indicated additional testing would be performed in an environment more reflective of the real world.

Ms. Jenkins and Mr. Cooper agreed that scalability testing is important but equally important is the approach taken. This point will require further discussion.

Issues with CML may impact the TrustEnabler product, which is on the approved product list.

There was discussion regarding the availability of the PKIF v2 software (February 2006) and whether that might provide a suitable alternative to CML. Ms. Jenkins and Ms. Debbie Mitchell of DoD will discuss this off-line and formulate a position regarding what is in the best interest of the government.

Agenda Item 3

Other Topics

The next meeting will be in February 2006.

Agenda Item 4

Adjourn Meeting

The meeting was adjourned at 10:35 a.m.

Following the formal adjournment of the meeting, those attendees at NIST continued the discussions as follows:

A. Ms. Jenkins expressed interest in being able to provide information on agency requirements and applications to the PD-VAL vendors. Mr. Lazerowich briefly described the "vendor fair" that the E-Authentication Program Office sponsored last Spring for approved SAML vendors and suggested something comparable could easily be arranged for this purpose. The group seemed favorably disposed towards investigating this option in more detail.
B. There was considerable discussion and interest amongst the remaining attendees regarding SAML product capabilities, especially as they might relate to SAML 2.0 which provides support for PKI to protect the integrity and confidentiality of data in SAML assertions.
C. Ms. Jenkins indicated that Ms. Mary Mitchell (GSA Office of Government-wide Programs) is making sure that the PD-VAL WG has proper visibility within GSA and with other Government entities.

PD-VAL Current Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
001	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	Feb. 06, 2006	**Open**
002	Contact Scott Shorter of Orion to get the Apache version of Webcullis into the interoperability lab.	Andrew Lins	Sept. 15, 2005	Feb. 03. 2006	**Open**
003	Check with DoD on the use of Orion GOTS product(s) by other federal agencies.	Deborah Mitchell	Sept. 15, 2005	Sept. 30, 2005	**Closed**
005	Schedule a technical meeting with Entrust (Alan McPhee) with David Cooper and Cheryl Jenkins	Cheryl Jenkins	Oct. 13, 2005	Nov. 17, 2005	**Closed**
006	Mr. Bob Dulude (CoreStreet) is to provide the pricing information he submitted previously again.	Bob Dulude, CoreStreet	Oct. 13, 2005	Dec. 31, 2005	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
007	Ms. Jenkins will hold a discussion about True Pass with Entrust before the end of the year and another in January. Ms. Jenkins will get the due date where Treasury must go live with the True Pass product.	Cheryl Jenkins	December 8, 2005	December 22, 2005	**Open**
008	Ms Jenkins and Ms. Mitchell agreed to speak regarding the support approach for the PKIF library	Cheryl Jenkins	December 8, 2005	January 31, 2005	**Open**