The Federal PKI Policy Authority tasked its Path Discovery and Validation Working Group (PD-VAL WG) to test products for accurate validation of certificates within the Federal PKI architecture, with the intent to qualify them as acceptable products for federal agencies' use.

The Tumbleweed Validation Authority (VA) is an SCVP server that performs both certification path discovery and validation. The VA was tested in conjunction with a client plug-in for Microsoft Outlook that was also provided by Tumbleweed.

The PD-VAL WG tested the VA product on June 28, 2005. When the VA was tested using the Microsoft Outlook plug-in, Microsoft Outlook reported the correct results for all of the path discovery tests, but path validation failed on many of the tests that involved segmented CRLs and delta-CRLs, but solutions to these problems were identified and the vendor provided an updated version of the VA product that incorporated the fixes to these problems on August 12, 2005. A detailed synopsis of the test results is provided below.

Based on these findings, the PD-VAL WG recommends the Tumbleweed Validation Authority as an acceptable validation solution to be posted to the Qualified Validation List. The PD-VAL WG also recommends the Microsoft Outlook plug-in when used in conjunction with the VA as an acceptable validation solution to be posted to the Qualified Validation List, but note that the information presented by user interface may be confusing for the typical user, and so encourage agencies that may be interested in deploying this plug-in to view a demonstration of the product in order to determine if its use would be appropriate within the agency.

Federal agencies are encouraged to weigh the findings and select a certificate validation solution from the Qualified Validation List based upon their specific requirements.

Detailed Technical Synopsis

The VA implements the functionality for a Bridge-Enabled Path Validation Module (PVM) as defined in the draft NIST Recommendation for X.509 Path Validation. The VA can also process delta-CRLs. When tests using the Public Key Interoperability Test Suite (PKITS) as specified in the NIST recommendation, the updated version of the VA passed all of the tests. The VA was also tested using the Directory, LDAP URI, and HTTP URI based tests from the Path Discovery Test Suite at both the Rudimentary and Basic levels and passed all of the tests.

The Microsoft Outlook plug-in that Tumbleweed provided also provided the correct information about certificate validity to the user. When the plug-in is installed and the user opens a message that is digitally signed, the plug-in attempts to validate the claimed signer's certificate and presents a series of pop-up messages that indicate the validity of each certificate in the certification path, with the final pop-up message indicating the validity of the claimed signer's certificate. However, the final pop-up window only indicates whether the certificate of the person who claimed to sign the certificate is valid, so the pop-up window may display an indication that the certificate is valid even if the signature on the email message itself is invalid. Since the certificate attached to a message does not provide any assurance of the identity of the signer unless the signature on the message is valid, users may not rely solely on the information provided by the pop-up windows to verify the integrity of a message. When the pop-up windows indicate

that the claimed signer's certificate is valid users will also need to examine certain information provided Microsoft Outlook.

When a message is digitally signed, Microsoft Outlook will display a ribbon that indicates whether the message has been properly signed. This ribbon will only indicate that the message is valid, if the signature on the message is valid and the Microsoft path validation software determines that the signer's certificate is valid. If both the pop-up created by the Tumbleweed plug-in and the ribbon displayed by Microsoft Outlook indicate that the message has been properly signed, then the signature on the message is valid. However, if Tumbleweed plug-in indicates that the claimed signer's certificate is valid but the ribbon displayed by Microsoft Outlook indicates that the message is invalid, then the user will need to click on the ribbon in order to determine the reason(s) that Microsoft Outlook is indicating that the signature on the message is invalid. If Microsoft Outlook indicates that the contents of the message were altered, then the signature on the message is invalid and so the signature on the message cannot be trusted. However, if Microsoft Outlook indicates that the contents of the message were not altered (i.e., the signature on the message is valid), and only indicates that the certificate cannot be validated, then the signature on the message is valid and Microsoft Outlook's error message can be ignored.

With the caveats noted above, the PD-VAL WG recommends the inclusion of the Tumbleweed VA and Microsoft Outlook plug-in on the Qualified Validation List.