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.

Webcullis from Orion Security Solutions is a plug-in for Microsoft's Internet Information Services (IIS) Web server that validates client's certificates when an SSL or TLS session is established that requires client-side authentication.

The PD-VAL WG tested Webcullis on September 7, 2005. The test results indicated that Webcullis is capable of performing path discovery and validation as required for use within the Federal PKI. While a few minor issues were encountered during testing, the PD-VAL WG does not believe these issues would prevent the effective use of Webcullis for validating certificates within the Federal PKI. A detailed synopsis of the test results is provided below.

Based on these findings, the PD-VAL WG recommends Webcullis as an acceptable Web server plug-in to be posted to the Qualified Validation List.

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

Webcullis incorporates the PKI Framework (PKIF) library, which is used to perform certification path discovery and validation. Using the naming scheme from the draft NIST Recommendation for X.509 Path Validation, PKIF is an Enterprise PVM with Policy Mapping, anyPolicy, Indirect CRLs, and Delta-CRLs. It has all of the capabilities of a Bridge-enabled PVM except the ability to process name constraints on email addresses. When the Webcullis plug-in was tested using the PKITS path validation test suite as specified in the NIST Recommendation, it passed all of the tests except 4.11.4. In the case of test 4.11.4, IIS rejected the certificate before passing it to Webcullis and so the certificate was rejected even though the certification path was valid.

Webcullis 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. In the case of the tests involving EE2 from section 4.2.4.3, it was necessary to add additional CA certificates to the list of trusted CAs in the Microsoft CAPI certificate store in order to prevent IIS from inappropriately rejecting the certificates before passing them to Webcullis for validation. This was considered acceptable since Webcullis does not rely on the Microsoft CAPI certificate store for making validation decisions and so adding these certificates to the certificate store cannot lead to certificates being accepted inappropriately.

The PD-VAL WG recommends the inclusion of Webcullis on the Qualified Validation List.