Entrust TruePass Technical Synopsis

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.

TruePass 8.0 SP1 from Entrust is a web-based security solution that can use certificate validation to authenticate clients. TruePass consists of a Web server plug-in, which is responsible for validating clients' certificates, and a client Java applet, which is downloaded by the client when the client connects to the server.

On behalf of the PD-Val WG, the E-Authentication Lab completed testing of TruePass on March 20, 2006. The test results indicated that TruePass is capable of performing path discovery and validation as required for use within the Federal PKI. A detailed synopsis of the test results is provided below.

Based on these findings, the PD-Val WG recommends TruePass 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

TruePass was tested while running on top of Microsoft Internet Information Services (IIS) 5.0. Using the naming scheme from the draft NIST Recommendation for X.509 Path Validation, TruePass is a Bridge-enabled PVM. When TruePass was tested using the PKITS path validation test suite as specified in the NIST Recommendation, it passed all of the tests.

TruePass was also tested using the Directory based tests from the Path Discovery Test Suite at both the Rudimentary and Basic levels and passed all of the tests.

Most of the tests were performed by loading the PKCS #12 files provided as part of the test suites into MS CAPI. In this configuration, however, the client Java applet will only allow the client to use a certificate if the certificate can be validated using CAPI. In order to test the TruePass server's handling of all of the test cases, including tests in which the client's certificate is invalid, some of the tests were run by first converting the corresponding PKCS #12 file to Entrust's EPF format. When EPF files are used by the client, the client Java applet does not attempt to validate the certificate before allowing its use by the client.

The PD-Val WG recommends the inclusion of TruePass on the Qualified Validation List.