Entrust Authority Security Toolkit for the Java Platform 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.

The Entrust Authority Security Toolkit for the Java Platform 7.1 sp1 with patch 104143 is a Java based toolkit with interfaces that supply encryption, authentication and digital signature capabilities using X.509 certificates.

On behalf of the PD-Val WG, the FPKI Architecture Lab completed testing of the Entrust Authority Security Toolkit for the Java Platform on April 17, 2006. The test results indicate that the toolkit 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 the product 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

The Entrust Authority Security Toolkit for the Java Platform implements the functionality for a Bridge-Enabled Path Validation Module (PVM) as defined in the draft NIST Recommendation for X.509 Path Validation. The toolkit can also process delta-CRLs. When tested using the Public Key Interoperability Test Suite (PKITS) as specified in the NIST recommendation, the toolkit passed all of the tests. The toolkit 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.

The PD-VAL WG recommends the inclusion of the Entrust Authority Security Toolkit for the Java Platform on the Qualified Validation List.