Entrust Secure Transaction Platform Verification Server 7.1 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.

Verification Server 7.1 with patch 103868 from Entrust is a Web service that supports the certificate validation portions of the XML Key Information Service Specification (X-KISS) 2.0, which is one part of the XML Key Management Specification (XKMS). The client sends a ValidateRequest message containing the certificate to be validated to the service, which performs the checks and responds with a ValidateResult message. The parameter values used to validate certificates (e.g., the set of acceptable certificate policies) are specified at the server using an Entrust policy certificate.

On behalf of the PD-Val WG, the FPKI Architecture Lab completed testing of Entrust Authority Verification Server on Tuesday, April 18, 2006. The test results indicated that the product is capable of performing path validation and discovery 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 Verification Server was deployed on IBM WebSphere Application Server version 6.0. The Verification Server, which uses the Entrust Authority Security Toolkit for the Java Platform to perform certification path discovery and validation, implements the functionality for a Bridge-Enabled Path Validation Module (PVM) as defined in the draft NIST Recommendation for X.509 Path Validation. The Verification Server can also process delta-CRLs. When tested using the Public Key Interoperability Test Suite (PKITS) as specified in the NIST recommendation, the Verification Server passed all of the tests. The Verification Server 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 Verification Server 7.1 on the Qualified Validation List.