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 CoreStreet offering consists of PathBuilder 1.0, which is a Delegated Path Discovery (DPD) server, and a PKI Toolkit, which is a library that performs path validation using the information provided by the server. The DPD server provides the client with pre-discovered certification paths along with pre-signed OCSP responses for each certificate in the path. The PKI Toolkit then uses the certificates and the OCSP responses provided by the server to validate the certification path.

CoreStreet also offers a Validation Client, which is built on top of the PKI Toolkit. Applications may be PKI enabled by either incorporating the PKI Toolkit library into the application or by incorporating an interface to the Validation Client. When the Validation Client is used, the PKI enabled application and the Validation Client run as separate processes, that communicate via interprocess communication. The Validation Client is responsible for managing configuration settings.

In the test environment, a Test Tool was used. The test tool was designed to interact with the Validation Client in the same way that a PKI enabled application would. The Test Tool passed the certificates to be validated to the Validation Client and then displayed the results that were returned by the Validation Client. CoreStreet offers application plug-ins that are designed to interact with the Validation Client, but the PD-VAL WG has not yet tested these plug-ins. A detailed synopsis of the test results is provided below.

Based on the test results, the PD-VAL WG recommends CoreStreet PathBuilder 1.0 when used in combination with the CoreStreet PKI Toolkit as an acceptable toolkit 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

The CoreStreet offering provides path discovery and validation using a client/server approach. The client presents the target certificate to be validated to the server, PathBuilder 1.0. The server returns a certification path to the client along with certificate status information for each certificate in the path. The client is then responsible for using this information to validate the target certificate.

Agencies that use the CoreStreet offering may either operate the Delegated Path Discovery (DPD) server (PathBuilder 1.0) themselves or make use of a DPD server that is operated by a third party as a service. At the moment, information about CA certificates and the locations of CRLs must be manually entered into the DPD server, however, CoreStreet indicates that support for an automated "spider" that would locate CA certificates and CRLs is planned.

Using the naming scheme from the draft NIST Recommendation for X.509 Path Validation, the Desktop Validation Client is a Bridge-Enabled Path Validation Module, with the exception that the PKI Toolkit cannot process CRLs. Rather than using CRLs, the PKI Toolkit uses OCSP responses, which are provided by the DPD server, to determine the revocation status of certificates. The DPD server is responsible for processing CRLs to extract the information needed to generate the OCSP responses. The DPD server is capable of processing full CRLs, segmented CRLs, and delta-CRLs, however, PD-VAL WG recommends configuring the DPD server so that it will not process segmented CRLs.

There is a significant concern about the way that the DPD server segmented CRLs. When the DPD server is generating OCSP responses for certificates, the server only has access to the CRLs issued by

CAs that issued the certificates. So, the server must be able to determine the revocation status of every certificate issued by a CA using only the CRLs issued by that CA. With a segmented CRL, the CRL itself does not provide enough information to determine which certificates are covered by that CRL. Similarly, if one has a collection of segmented CRLs issued by a CA, there is no way to know if those CRLs collectively cover all of the certificates issued by a CA or if the CA has issued other CRLs that cover certificates that are not covered by the CRLs in the collection.

When a CA only issues segmented CRLs, the DPD server can be configured to collect the segmented CRLs from the CA and then use these segmented CRLs to generate OCSP responses. Using this configuration, however, the DPD server will incorrectly indicate that some revoked certificates are valid if the collection of CRLs used by the server does not happen to cover all of the certificates issued by the CA. According to CoreStreet, it is the responsibility of the server's administrator to ensure that all of the CRL segments have been fetched in order to ensure that correct OCSP responses are generated for all certificates. In most cases, the only option would be to obtain all of the CRLs available on the CA's directory and hope that this constitutes all of the CRLs that have been issued. However, since communication with the directory is insecure there is a risk that the administrator will think that all necessary CRL segments have been obtained even if they have not. CoreStreet understands that this is an issue and so prefers to use full CRLs when possible. The PD-VAL WG believes that in order to avoid the risks associated with the use of segmented CRLs, CoreStreet should only use full CRLs and that the DPD server should be configured to reject CRLs that are not full. In the current FPKI, most if not all of the CAs issue full CRLs and any CAs that are only issuing segmented CRLs should be able to issue full CRLs in addition to segmented CRLs without much trouble.

PathBuilder 1.0 and the PKI Toolkit were also tested using the Directory based and LDAP URI based tests from the Path Discovery Test Suite at both the Rudimentary and Basic levels and passed all of the tests except for two of the LDAP URI based tests. Since CoreStreet passed the two corresponding Directory based tests and the Path Discovery Test Suite is still in draft form, it is possible that this failure is a result of a problem with the test suite rather than with PathBuilder 1.0 or the PKI Toolkit.

The PD-VAL WG recommends the inclusion of CoreStreet PathBuilder 1.0 when used in combination with the CoreStreet PKI Toolkit on the Qualified Validation List.