

# PKIF OCSP Plug-in for Microsoft Windows: Installation and Configuration

## Introduction

The PKIF OCSP Plug-in for Microsoft Windows is a revocation provider for the Microsoft Cryptographic API (CAPI). Applications that obtain basic PKI functionality from CAPI will call the PKIF OCSP Plug-in when validating a certificate. Many commonly used applications, such as Outlook, Internet Explorer and Infopath, use CAPI for PKI-related processing.

## Installation

The PKIF OCSP Plug-in for Microsoft Windows is installed using a standard Windows installer. To begin plug-in installation, double-click the PkifOcsplug.msi file. The following dialog will be displayed. Click the **N**ext button.

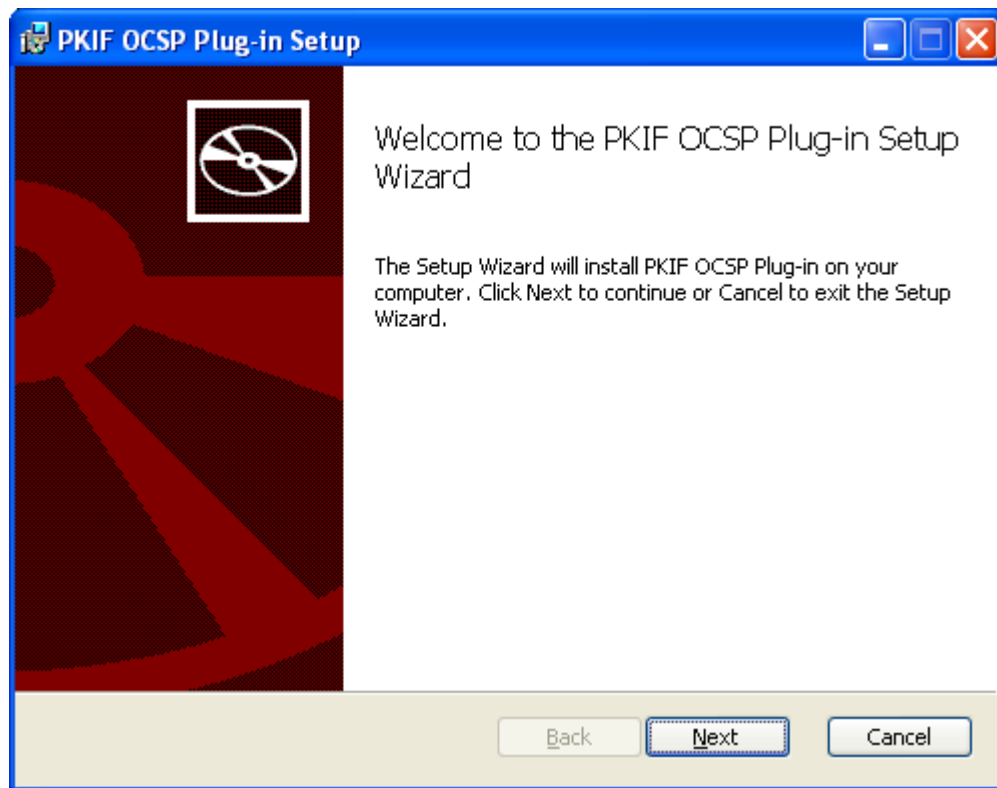
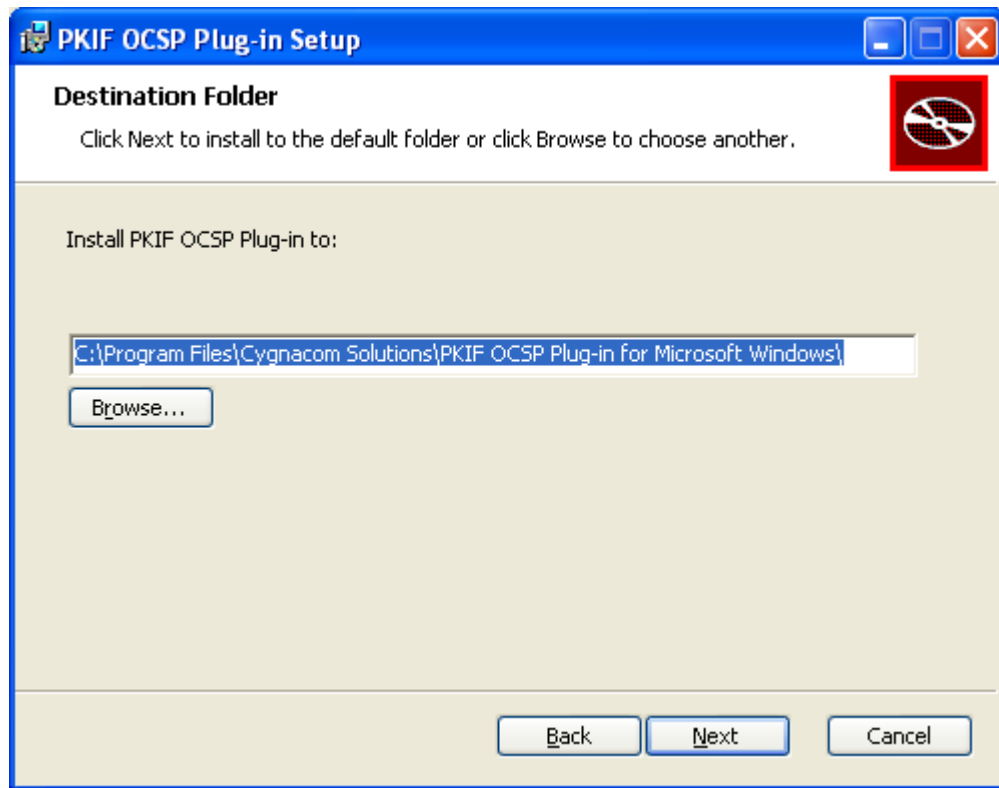


Figure 1 PKIF OCSP Plug-in Setup

By default, the plug-in is installed to the following directory:

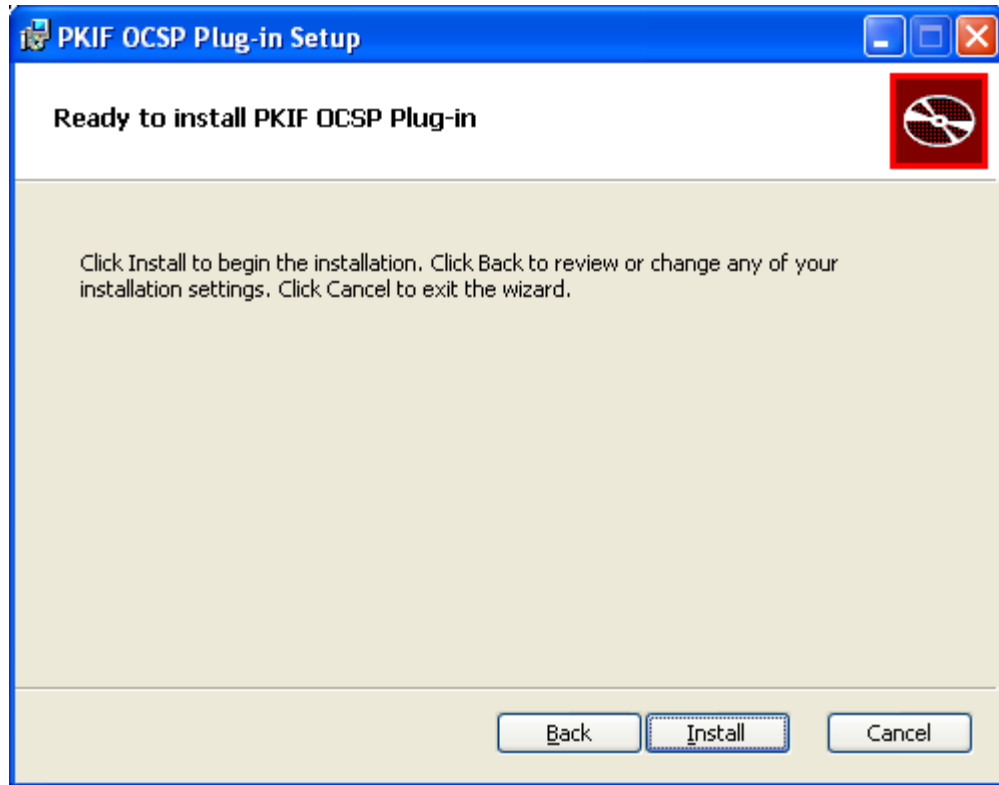
**C:\Program Files\Cygnacom Solutions\PKIF OCSP Plug-in for Microsoft Windows\.**

Browse to an alternative location, if desired, and then click the **N**ext button.



**Figure 2 Installation directory selection**

The plug-in does not have any optional components. Click the **N**ext button on the third dialog (not shown). To complete the installation, click the **I**nstall button. This will copy the plug-in files to the selected file folder, set up the default registry configuration and register the plug-in with Microsoft CAPI.



**Figure 3 PKIF OCSP Plug-in Installation**

After the installation completes, click the **Finish** button (not shown). Close and restart any applications that use CAPI for PKI processing in order for the plug-in to be used.

## Configuration

The PKIF OCSP Plug-in installer will prepare a default set of configuration options that features the following options:

- Retrieve trust anchors, certificates and CRLs from the current user's CAPI certificate and CRL stores
- Use CAPI for cryptographic functionality
- Retrieve certificates and CRLs from LDAP and HTTP URIs included in issuerAltName, crlDistributionPoint or authorityInformationAccess certificate extensions
- Retrieve revocation status information from OCSP responders identified in authorityInformationAccess certificate extensions (responder certificates will be validated to a trust anchor in the current user's trust anchor store)

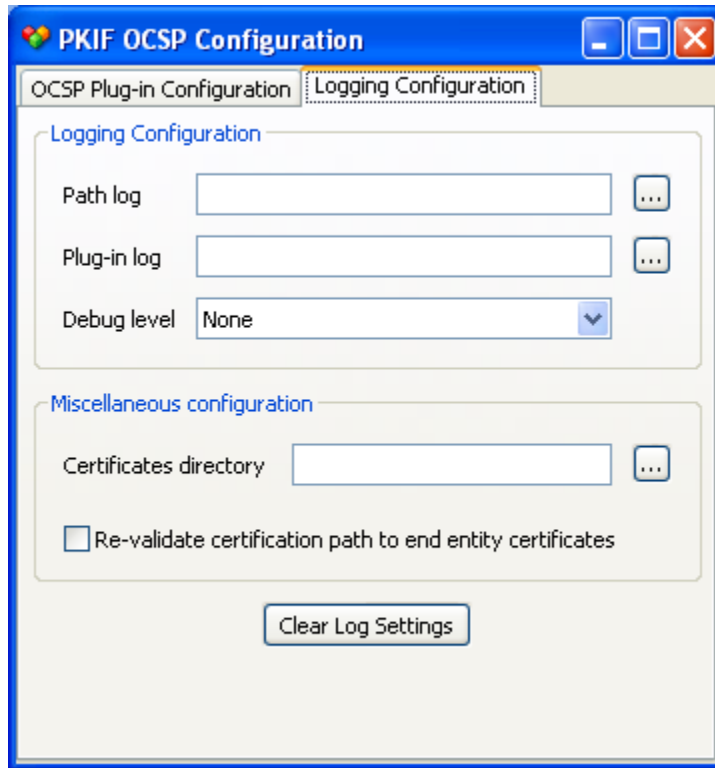
A configuration utility is provided with the plug-in to enable the default configuration to be changed. The OCSP Plug-in Configuration panel of the utility is shown below.



**Figure 4 PKIF OCSP Configuration Utility**

Usage of the PKI Environment Definition and Path Processing Definition options is described in [\*\*Configuring PKI Settings Using PKIFv2 Resources\*\*](#). The Status option can be used to register and unregister the plug-in with Microsoft CAPI. Following installation, the button should read **Disable**, as shown above. The plug-in can be unregistered by clicking the **Disable** button. After unregistering the plug-in, the button should be labeled **Enable** and can be used to register the plug-in with Microsoft CAPI. In this release, the **Configuration applies to all users** checkbox is checked and disabled. Settings apply to all users on a particular machine. Future versions may enable per-user configuration.

The plug-in provides various logging capabilities that can be used to troubleshoot problems with the plug-in or infrastructure problems. The Logging Configuration panel is shown below.



**Figure 5 Logging Configuration**

By default, logging is turned off by setting the **Debug level** option to **None**. The following debug levels are available, in order from least amount of output to most output” **None, Error, Information, Warning, Debug** and **Trace**. Most output is written to the file specified in the **Plug-in log** option. When the **Re-validate certification path to end entity certificates** option is checked, certification path result information is written to the file specified by the **Path log** parameter. When the **Re-validate certification path to end entity certificates** option is checked, the plug-in will perform full certification path processing for non-certification authority certificates. This can result in rejection of certificates that otherwise would have been accepted. If a folder is specified for the **Certificates directory** option, the plug-in will write out most certificates it handles during the course of determining the revocation status of a particular certificate (certificates used to verify the revocation status of a CRL issuer or OCSP responder may not be output). Certificates are written to a file named using a SHA1 hash of the certificate, as follows: <certificate thumbprint>.der. Clicking the **Clear Log Settings** button will reset the logging parameters to the values shown above.

Note, the debugging logs grow without bounds. These features should be activated only when trying to diagnose a problem and should be disabled during normal use.

## **Centralized configuration**

Configuration settings for the plug-in are written to the following registry location:

**HKEY\_LOCAL\_MACHINE\Software\Cygnacom Solutions\OCSPPlugin.**

The values under this location can be captured by an administrator and distributed using an enterprise-wide configuration management tool, such as SMS or Group Policy, or by creating a custom installation package. The PKIF OCSP Plug-in Configuration utility is primarily intended for use by administrators in defining settings that will be distributed across an enterprise. The plug-in will recognize per-user settings that reside in the same location under HKEY\_CURRENT\_USER, but the configuration utility cannot be used to manage these settings.

## Configuration Strategies

The PKIF OCSP Plug-in can be configured to perform revocation status determination, or certification path processing, a number of different ways. By default, following installation, the plug-in is configured to provide revocation status for all certificates containing an AIA extension with an OCSP component. The figures below shows these default settings (all fields on the two panels not shown are blank).

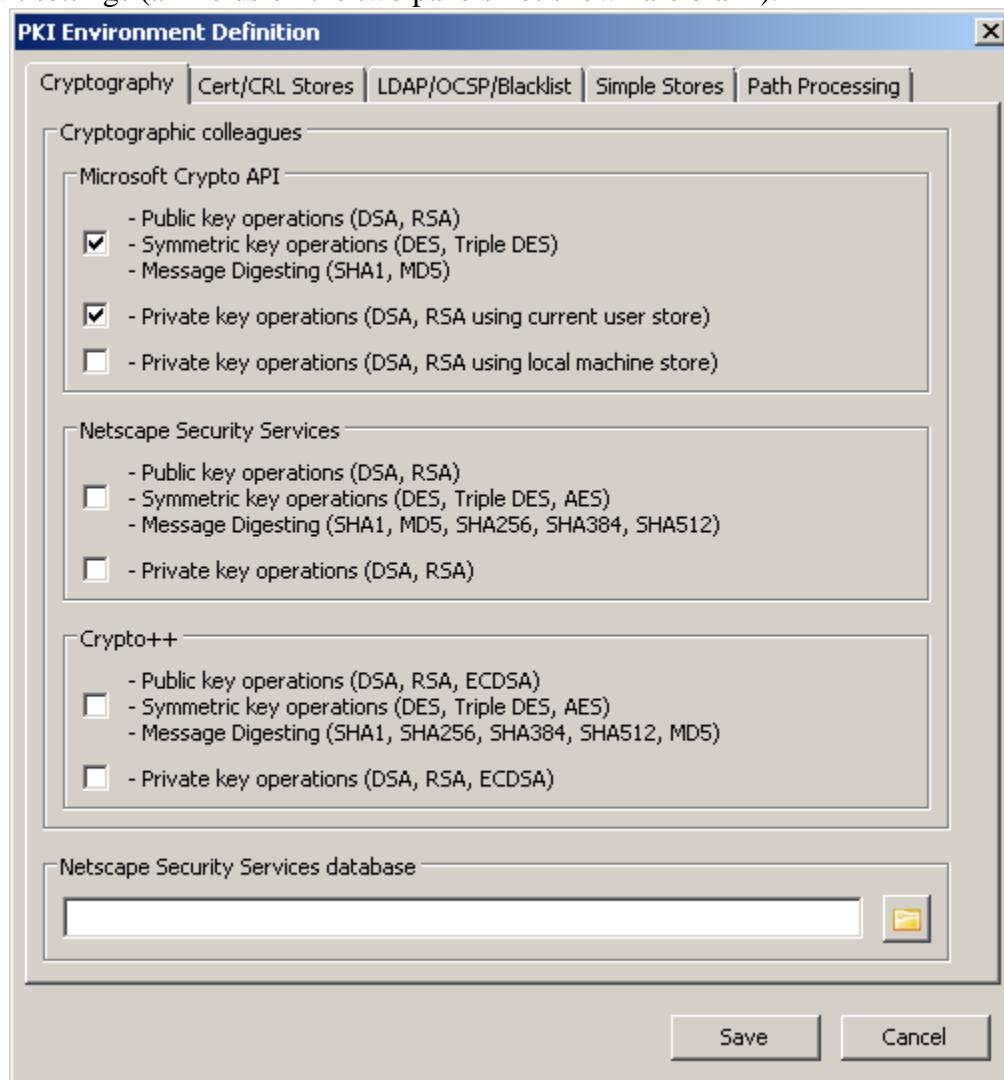
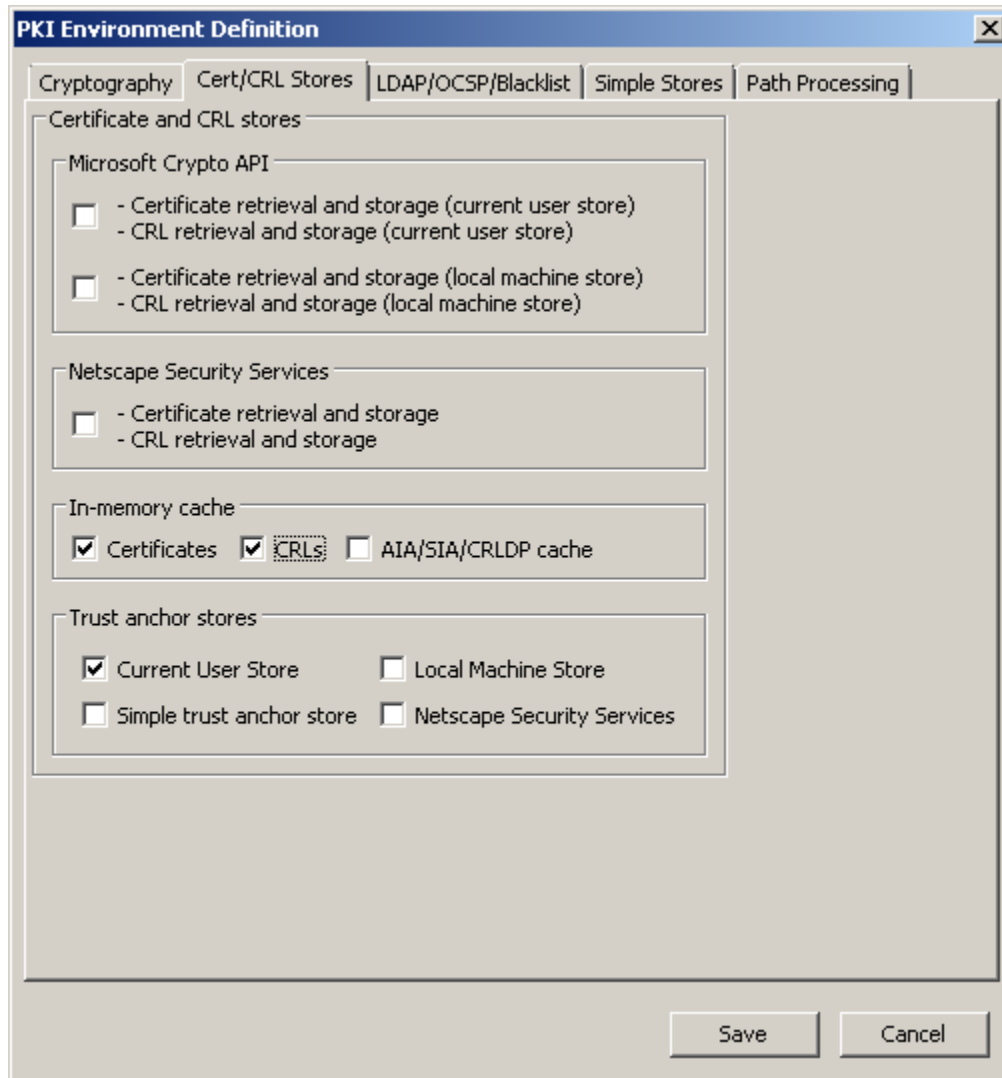
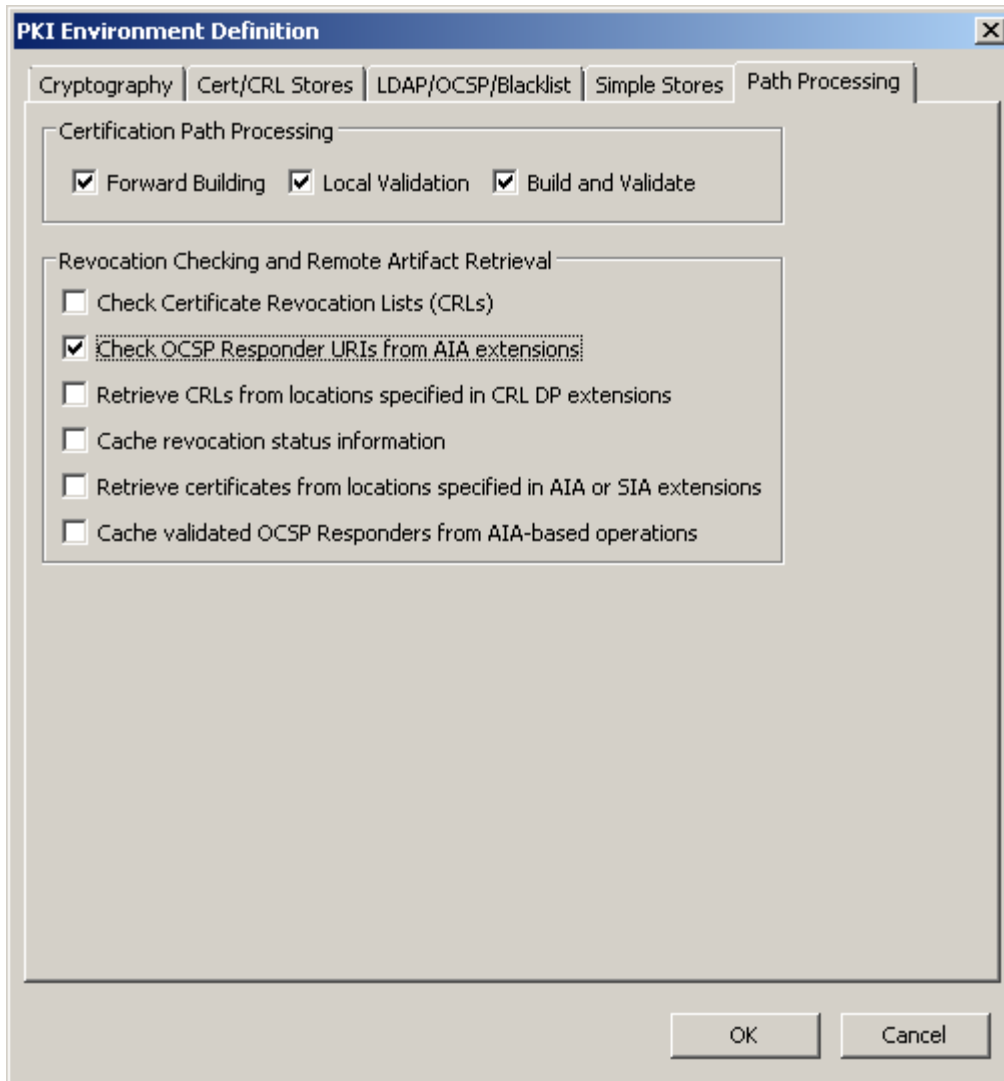


Figure 6 Default crypto settings for the PKIF OCSP Plug-in



**Figure 7 Default repository settings for the PKIF OCSP Plug-in**



**Figure 8 Default Path settings for the PKIF OCSP Plug-in**

Usage of the PKI Environment Definition and Path Processing Definition options is described in **Configuring PKI Settings Using PKIFv2 Resources**. There are several broad configuration strategies to consider when deploying the plug-in, including:

- AIA-based OCSP only (the default configuration)
- AIA-based OCSP and CRL DP-based CRLs
- AIA-based OCSP, CRL DP-based CRLs and CRLs from an enterprise directory
- OCSP from an enterprise OCSP responder only
- OCSP from an enterprise OCSP responder and AIA OCSP
- OCSP from an enterprise OCSP responder, AIA-based OCSP and CRL DP-based CRLs
- OCSP from an enterprise OCSP responder, AIA-based OCSP, CRL DP-based CRLs and CRLs from an enterprise directory

Multiple enterprise directories or OCSP responders can be specified, with each providing service for specific namespaces, if desired.