Configuring PKI Settings Using PKIFv2 Resources

Introduction

The PKIF public key enablement library provides a set of graphical interfaces to enable easy configuration of parameters that govern PKI-related processing. These interfaces can be integrated into applications providing a consistent configuration interface and creating opportunities for shared configurations. This document describes each of the configuration user interfaces. These interfaces are not generally intended for use by end users, who typically need not possess the knowledge necessary to configure PKI-related settings. Instead these interfaces are intended for use by administrators and PKI-savvy users.

PKI Environment Definition

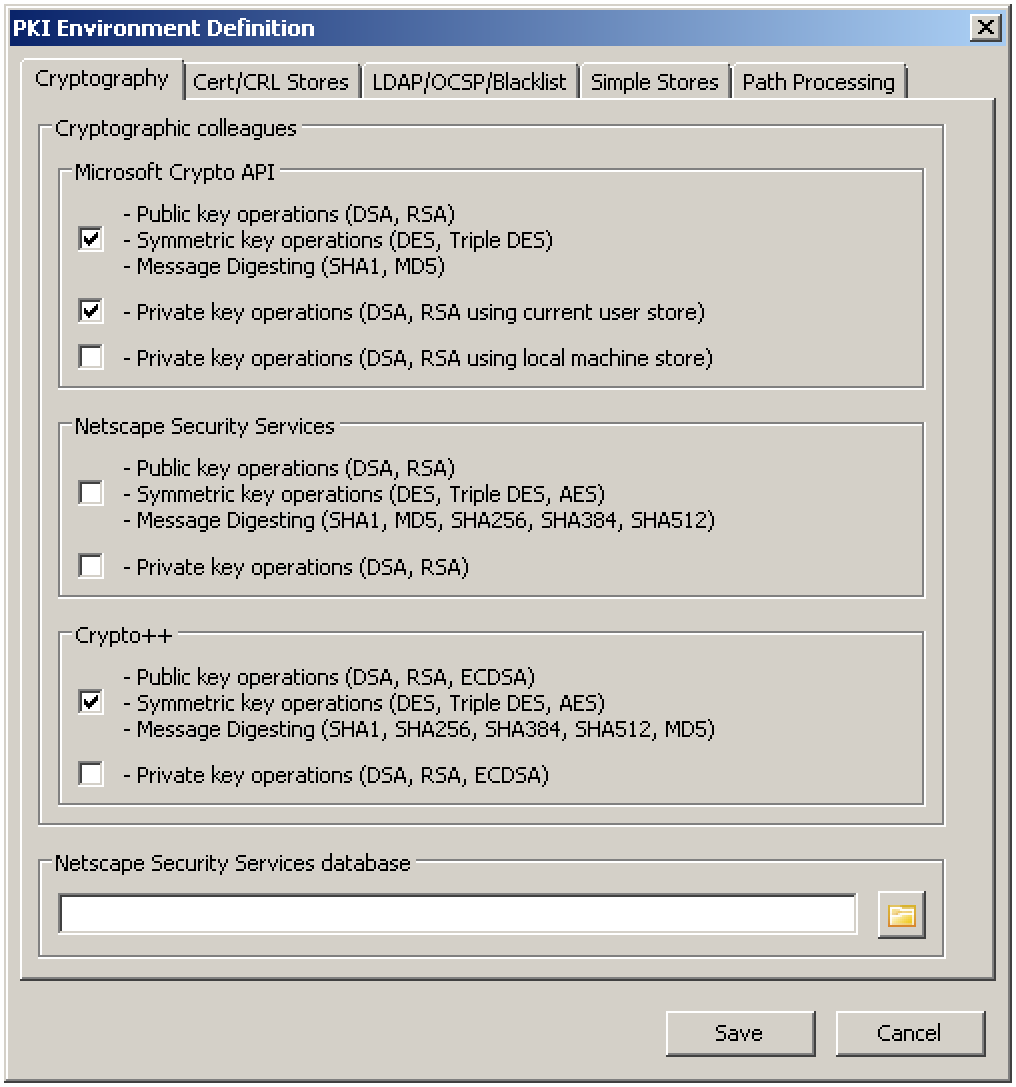
The PKI Environment Definition interfaces enable the specification of the resources that will be used when performing PKI-related processing such as signature verification and certification path processing. These settings are broken down into five categories:

- Cryptography
- Cert/CRL Stores
- LDAP/OCSP/Blacklist
- Simple Stores
- Path Processing

Each of these categories is further subdivided. Within each sub-category multiple options may be available. The options within each sub-category are described below.

Cryptography

The **Cryptography** panel **must** be configured for all applications of PKIF. These settings define the components used when verifying or generating digital signatures, generating message digests, generating random numbers and encrypting or decrypting data.



Cryptographic colleagues

Microsoft Crypto API

☑ - Public key operations (DSA, RSA)
- Symmetric key operations (DES, Triple DES)
- Message Digesting (SHA1, MD5)

☑ - Private key operations (DSA, RSA using current user store)

☐ - Private key operations (DSA, RSA using local machine store)

Netscape Security Services

☐ - Public key operations (DSA, RSA)
- Symmetric key operations (DES, Triple DES, AES)
- Message Digesting (SHA1, MD5, SHA256, SHA384, SHA512)

☐ - Private key operations (DSA, RSA)

Crypto++

☑ - Public key operations (DSA, RSA, ECDSA)
- Symmetric key operations (DES, Triple DES, AES)
- Message Digesting (SHA1, SHA256, SHA384, SHA512, MD5)

☐ - Private key operations (DSA, RSA, ECDSA)

Netscape Security Services database

Figure 1 Cryptography panel

Cryptographic Colleagues

PKIF can be used with any of three different cryptographic back-ends:

- Microsoft CAPI: http://msdn2.microsoft.com/en-us/library/aa380256.aspx
- Netscape Security Services: http://www.mozilla.org/projects/security/pki/nss/
- Crypto++: http://www.cryptopp.com/

For each back-end, there are at least two checkboxes. One checkbox is associated with functionality that does not require the use of a private key, i.e., signature verification. The other checkbox is associated with functionality that does require the use of a private key, i.e., signature generation. For Microsoft CAPI, private key functionality is represented by two checkboxes, one of which should be used when the configuration will be consumed by an end user application and the other used when the configuration will e consumed by a service.

Internally, PKIF will use the first available back-end capable of fulfilling a particular request. When multiple back-ends are in use, PKIF queries the back-ends in the following order: Microsoft CAPI, NSS then Crypto++. If all three backends were selected, Microsoft CAPI would always be used for RSA signature verification and Crypto++ would always be used for ECDSA signature verification.

When Netscape Security Services (NSS) is used, an NSS database must be specified in the text box at the bottom of the panel.

Cert/CRL Stores

The **Cert/CRL Stores** panel **must** be configured for all applications of PKIF that require certification path processing. Minimally, a trust anchor store must be specified.

Trust Anchor Stores

Four trust anchor store options are available. The **Current User Store** option corresponds to the Microsoft CAPI current user certificate store. This option is appropriate for scenarios in which the configuration will be consumed by an end user application. The **Local Machine Store** option corresponds to the Microsoft CAPI local computer certificate store. This option is appropriate for scenarios in which the configuration will be consumed by a service.

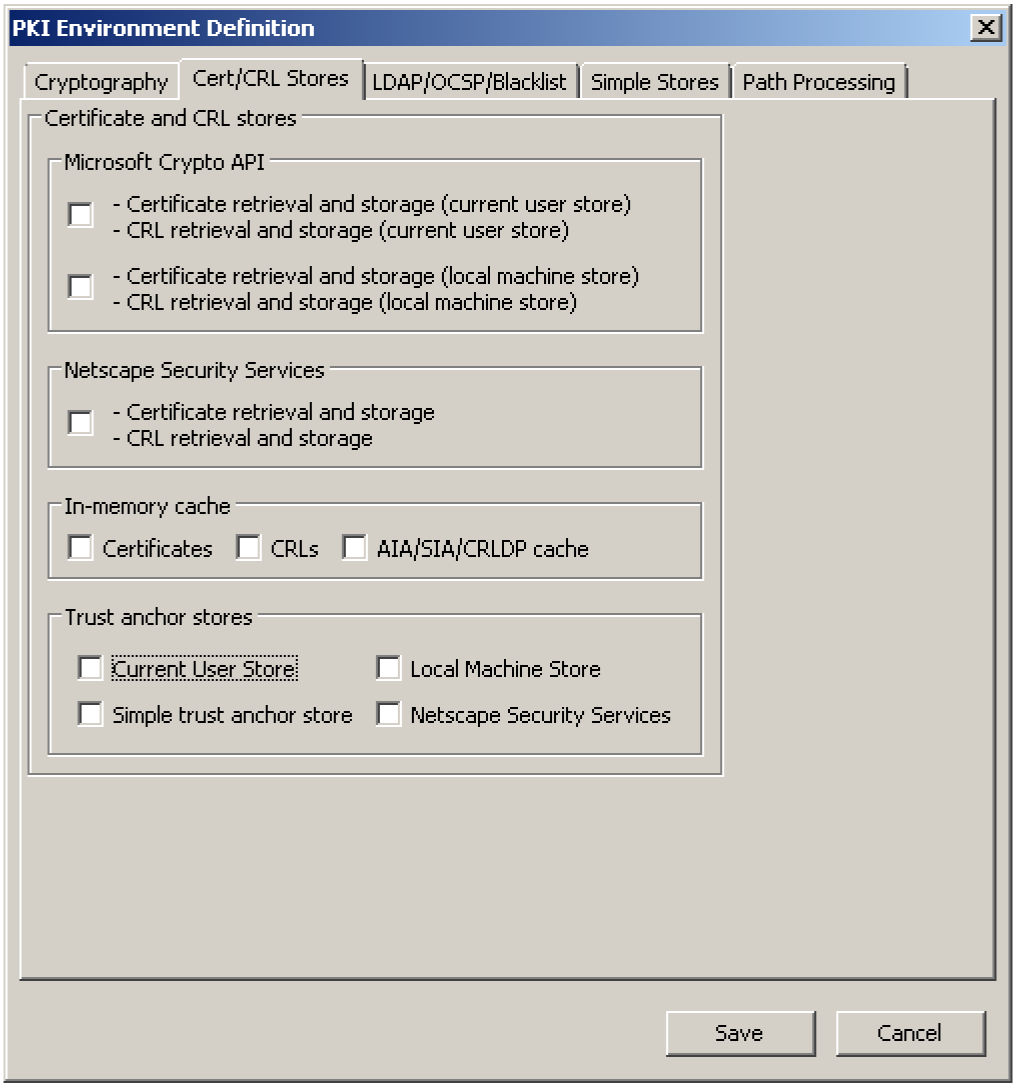
The **Simple trust anchor store** option allows the operator to specify one or more trust anchors on the **Cert/CRL Stores** panel. The trust anchors must be available in X.509 certificate format (but need not be self-signed). The configuration medium to which trust anchors stored in this manner must be secured using operating system mechanisms. Generally, this option is only appropriate for testing, debugging or in tightly controlled environments. If this option is not selected, the trust anchor list management options on the **Cert/CRL Stores** panel will be disabled.

The **Netscape Security Services** option corresponds to an NSS trust store. When this option is selected, an NSS database must be specified in the text box at the bottom of the panel.

If multiple trust anchor stores are selected, all will be queried during certification path validation.

Certificate and CRL stores

Five certificate and CRL store options are available. The **Current User Store** option in the Microsoft Crypto API box corresponds to the Microsoft CAPI current user certificate store. This option is appropriate for scenarios in which the configuration will be consumed by an end user application. The **Local Machine Store** option the Microsoft Crypto API box corresponds to the Microsoft CAPI local computer certificate store. This option is appropriate for scenarios in which the configuration will be consumed by a service.



Certificate and CRL stores

Microsoft Crypto API

□ - Certificate retrieval and storage (current user store)
- CRL retrieval and storage (current user store)

□ - Certificate retrieval and storage (local machine store)
- CRL retrieval and storage (local machine store)

Netscape Security Services

□ - Certificate retrieval and storage
- CRL retrieval and storage

In-memory cache

□ Certificates □ CRLs □ AIA/SIA/CRLDP cache

Trust anchor stores

□ Current User Store □ Local Machine Store
□ Simple trust anchor store □ Netscape Security Services

Figure 2 Cert/CRL Stores panel

The **Certificates** and **CRLs** options in the In-memory cache box allows the operator to specify one or more certificates or CRLs on the **Cert/CRL Stores** panel. If these options are not selected, the certificate and CRL list management options on the **Cert/CRL Stores** panel will be disabled.

AIA/SIA/CRLDP cache option allows the operator to enable a cache that will store information from URI based operations. If present, this cache will be consulted first before going to a remote source.

The **Netscape Security Services** option corresponds to an NSS trust store. When this option is selected, an NSS database must be specified in the text box at the bottom of the panel.

If multiple certificate or CRL stores are selected, all will be queried during certification path validation or during revocation status determination. LDAP-accessible directory servers specified on the **LDAP directories, OCSP responders, Server blacklist** panel will also be consulted for certificates or CRLs as necessary and in accordance with any namespace restrictions associated with the directory.

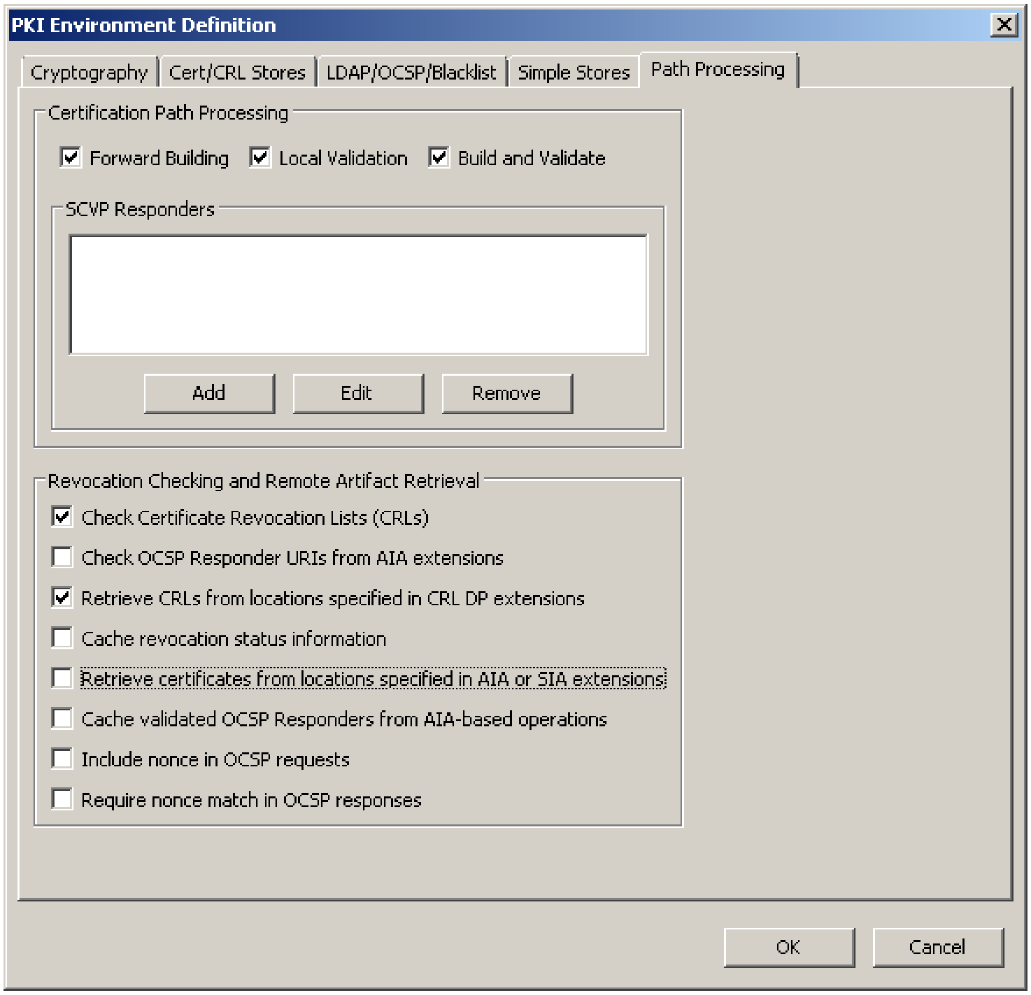
Certification Path Processing

There are three options available for controlling certification path processing. All three options should be checked for most applications of PKIF. Additional options, such as support for SCVP, may be available in the future.

Revocation Checking

There are three options for controlling revocation status determination on this panel (plus the OCSP responders entered on the **LDAP directories, OCSP responders, Server blacklist** panel). If the **Check Certificate Revocation Lists (CRLs)** option is selected, then the available CRL stores and enterprise LDAP directories will be checked for CRLs using issuer names and DN components in CRL DP extensions. If the **Check OCSP Responder URIs from AIA extensions** option is checked, then an OCSP request will be sent to the responder indicated in the AIA extension to determine the revocation status of the certificate. If the **Retrieve CRLs from location specified in CRL DP extensions** option is checked, then LDAP or HTTP resources indicated in a CRL DP extension will be checked for CRLs (provided the server is not on the server blacklist). If **Cache revocation status information** option is checked the revocation status information will be maintained for 1 day and up to 1000 entries. Enabling **Retrieve certificates from locations specified in AIA or SIA extensions** checkbox will allow certificate retrieval from AIA and SIA extensions. If **Cache validate OCSP Responders from AIA-based operations** is checked then invalid OCSP responders will not be consulted multiple times. If **Include nonce in OCSP request** option is checked OCSP requests will contain a nonce. Enabling **Require nonce match in OCSP request** option will enforce nonce matching.

If multiple revocation status determination options are selected, the following order will be observed: enterprise OCSP responders will be consulted first, AIA-based OCSP responders will be consulted second, local CRL stores will be checked third and remote CRL sources checked last.



Certification Path Processing

☑ Forward Building ☑ Local Validation ☑ Build and Validate

SCVP Responders

Revocation Checking and Remote Artifact Retrieval

☑ Check Certificate Revocation Lists (CRLs)
☐ Check OCSP Responder URIs from AIA extensions
☑ Retrieve CRLs from locations specified in CRL DP extensions
☐ Cache revocation status information
☐ Retrieve certificates from locations specified in AIA or SIA extensions
☐ Cache validated OCSP Responders from AIA-based operations
☐ Include nonce in OCSP requests
☐ Require nonce match in OCSP responses

Figure 3 Path Processing panel

SCVP Responders

To add an SCVP responder to the list, click the **Add** button. The dialog shown below will be displayed. Enter the URL of the responder in the **Enter the URL of the target server** box. If **Delegate Path Discovery (DPD) only** is not checked the client will be operating in delegate path validation mode, if **Delegate Path Discovery (DPD) only** is enabled the client will be operating in delegated path discovery mode. In that case client will do all the validation tasks. To require signed DPD or to require a nonce enable **Require signed DPD** and **Require nonce** respectively.

There are 7 want backs that can be requested from the SCVP server. **Best Certification Path, Revocation information, Partial Path, Target certificate** wants backs can be requested by checking the appropriate checkbox. If SCVP server supports Evidence Record Syntax then ERS Partial Path, ERS Target Cert, and ERS Revocation Info want backs can be requested by selecting appropriate checkboxes. If ERS want backs were requested Evidence Record Verifier can be added by clicking **Configure ER Verified** button to validate evidence records. More detailed description of evidence record verifier dialog is provided below.

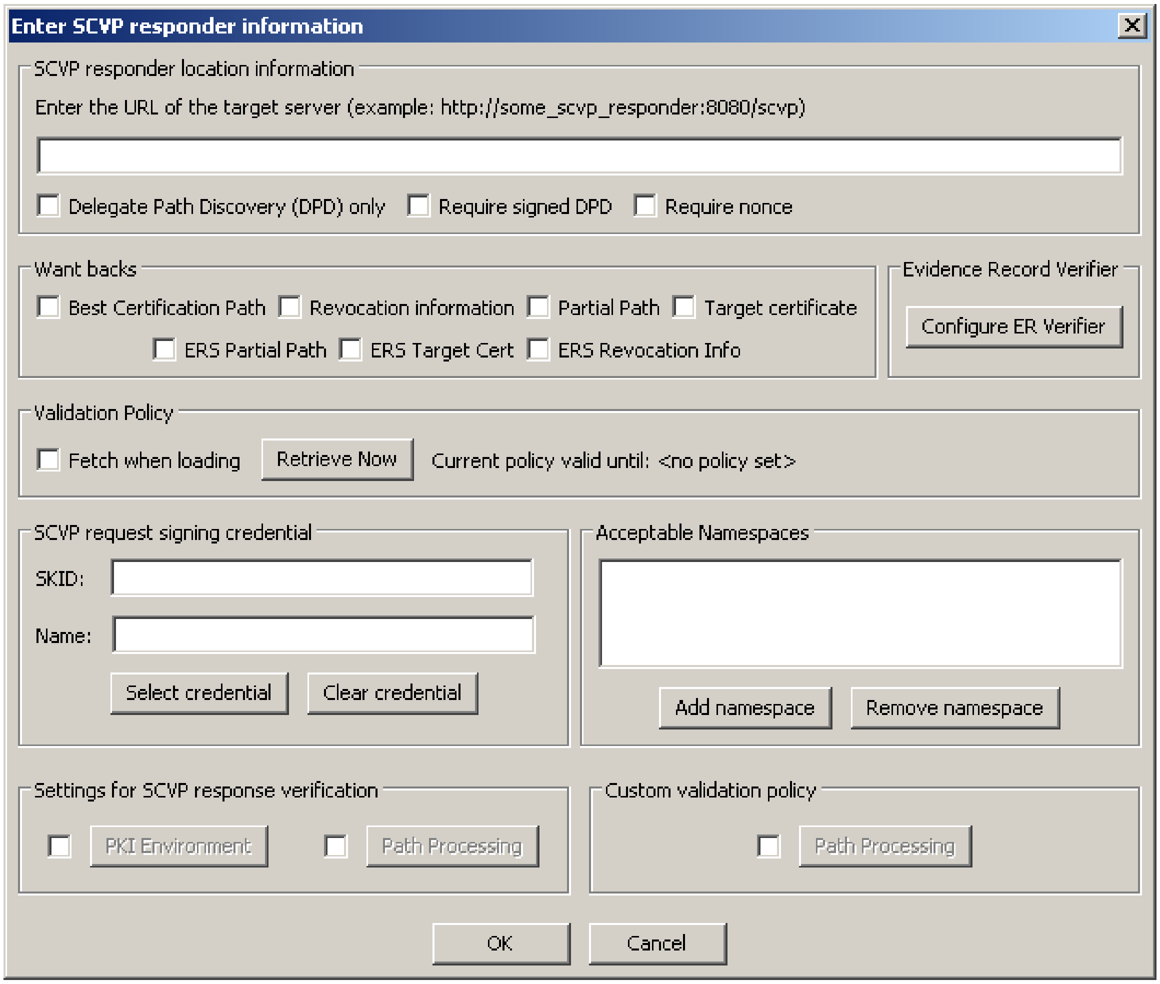
To retrieve validation policy when loading check **Fetch when loading** checkbox. To retrieve the policy now click **Retrieve Now** button.

To enable SVCP request signing, specify signing credential by clicking **Select credential** button and selecting an appropriate credential. This is optional; by default unsigned requests will be sent.

To add a namespace click the **Add namespace** and follow the directions provided below for specifying namespaces for LDAP-accessible directory servers.

Settings for SCVP response verification can be added in **Settings for SCVP response verification** section. To add PKI environment settings: check the box next to **PKI Environment** button and click it. **PKI Environment Definition** dialog will be displayed; this dialog is described in this document and can be populated in similar manner. To add path processing settings: check the box next to **Path Settings** button and click it. **Path Validation Settings** dialog will be displayed; this dialog is described at the end of this document. Settings in **Settings for SCVP response verification** section will be used to verify signatures on the SCVP responses and to verify SCVP responder certificate.

A custom validation policy can be specified in **Custom validation policy** section. To specify custom policy: check the box next to **Path Processing** button and click it, **Path Validation Settings** dialog will be displayed; this dialog is described at the end of this document.



Enter SCVP responder information

SCVP responder location information

Enter the URL of the target server (example: http://some_scvp_responder:8080/scvp)

□ Delegate Path Discovery (DPD) only □ Require signed DPD □ Require nonce

Want backs

□ Best Certification Path □ Revocation information □ Partial Path □ Target certificate

□ ERS Partial Path □ ERS Target Cert □ ERS Revocation Info

Evidence Record Verifier

Configure ER Verifier

Validation Policy

□ Fetch when loading Retrieve Now Current policy valid until: <no policy set>

SCVP request signing credential

SKID:

Name:

Select credential Clear credential

Acceptable Namespaces

Add namespace Remove namespace

Settings for SCVP response verification

□ PKI Environment □ Path Processing

Custom validation policy

□ Path Processing

OK Cancel

Figure 4 Adding an SCVP responder

Configuring Evidence Record Verifier

After clicking **Configure ER Verified** button in Enter SCVP responder information dialog, **Configure your evidence record verifier** dialog (shown below) will be displayed. The dialog contains three sections, current settings section, archival PKI Environment Settings section, and archival Path Processing Settings section. To specify current PKI environment settings click **PKI Environment** button. **PKI Environment Definition** dialog will be displayed; this dialog is described in this document and can be populated in similar manner. To specify current Path processing setting click **Path Settings** button. **Path Validation Settings** dialog will be displayed; this dialog is described at the end of this document. Current settings will be used to all validate evidence records unless archival settings have been specified and evidence record falls into the time period specified in the archival settings.

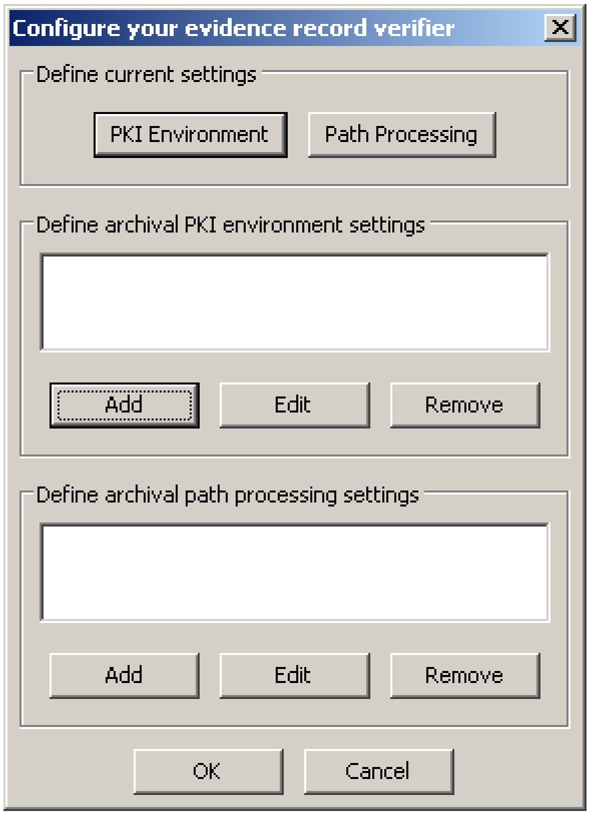

Configure your evidence record verifier
Define current settings
PKI Environment
Path Processing
Define archival PKI environment settings
Add
Edit
Remove
Define archival path processing settings
Add
Edit
Remove
OK
Cancel

Figure 5 Configuring evidence record verifier

To specify archival PKI environment settings click **Add** button in **Define archival PKI environment settings** section. Dialog shown below will be displayed. To specify time period for which these settings will be used click on the calendar button to the right of the text box and select an appropriate date. To specify PKI environment settings for that period click **PKI Environment Settings** button. **PKI Environment Definition** dialog will be displayed.

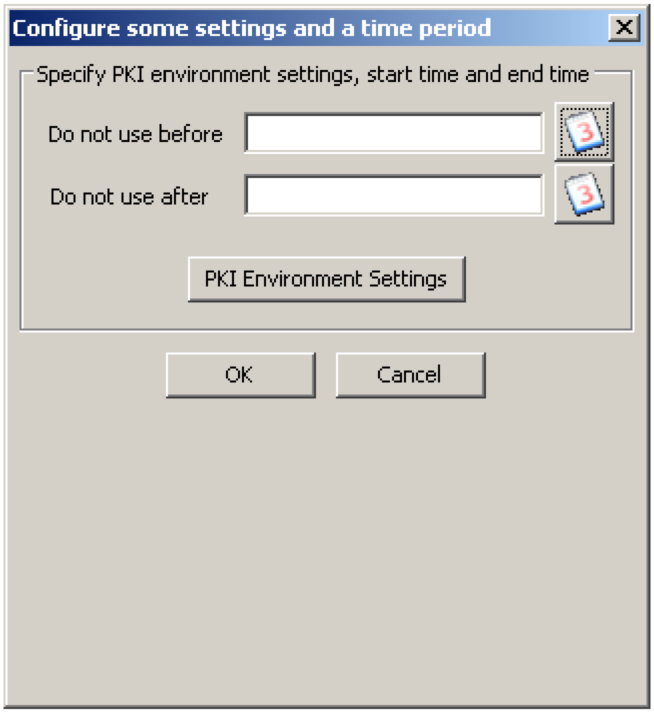
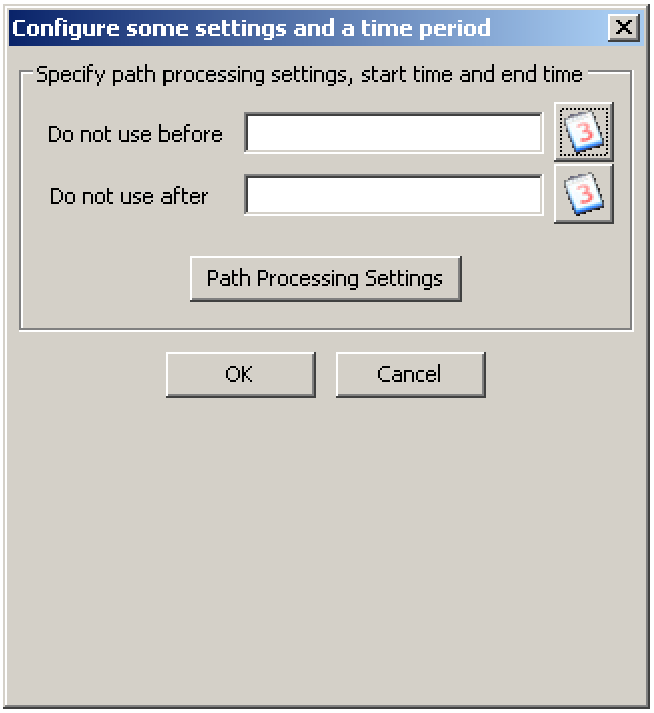

Configure some settings and a time period
Specify PKI environment settings, start time and end time
Do not use before
Do not use after
PKI Environment Settings
OK
Cancel

Figure 6 Configuring archival PKI environment settings

To specify archival path processing settings click **Add** button in **Define archival path processing settings** section. Dialog shown below will be displayed. To specify time period for which these settings will be used click on the calendar button to the right of the text box and select an appropriate date. To specify path processing settings for that period click **Path Processing Settings** button. **Path Validation Settings** dialog will be displayed.



Configure some settings and a time period

Specify path processing settings, start time and end time

Do not use before

Do not use after

Figure 7 Configuring archival Path Processing settings

Archival settings will be used to verify evidence records that fall within specified time period.

LDAP directories, OCSP responders and Server blacklist

The **LDAP directories, OCSP responders, Server blacklist** panel can be used to specify optional settings related to the availability of infrastructure components such as LDAP-accessible directory servers or OCSP responders. Directory servers will be used to locate certificates, cross certificates and CRLs. OCSP responders will be used to determine the revocation status of certificates. The server blacklist will be used to avoid attempts at contacting broken infrastructure directories when resolving CRL DP, issuerAltName or AIA extensions.

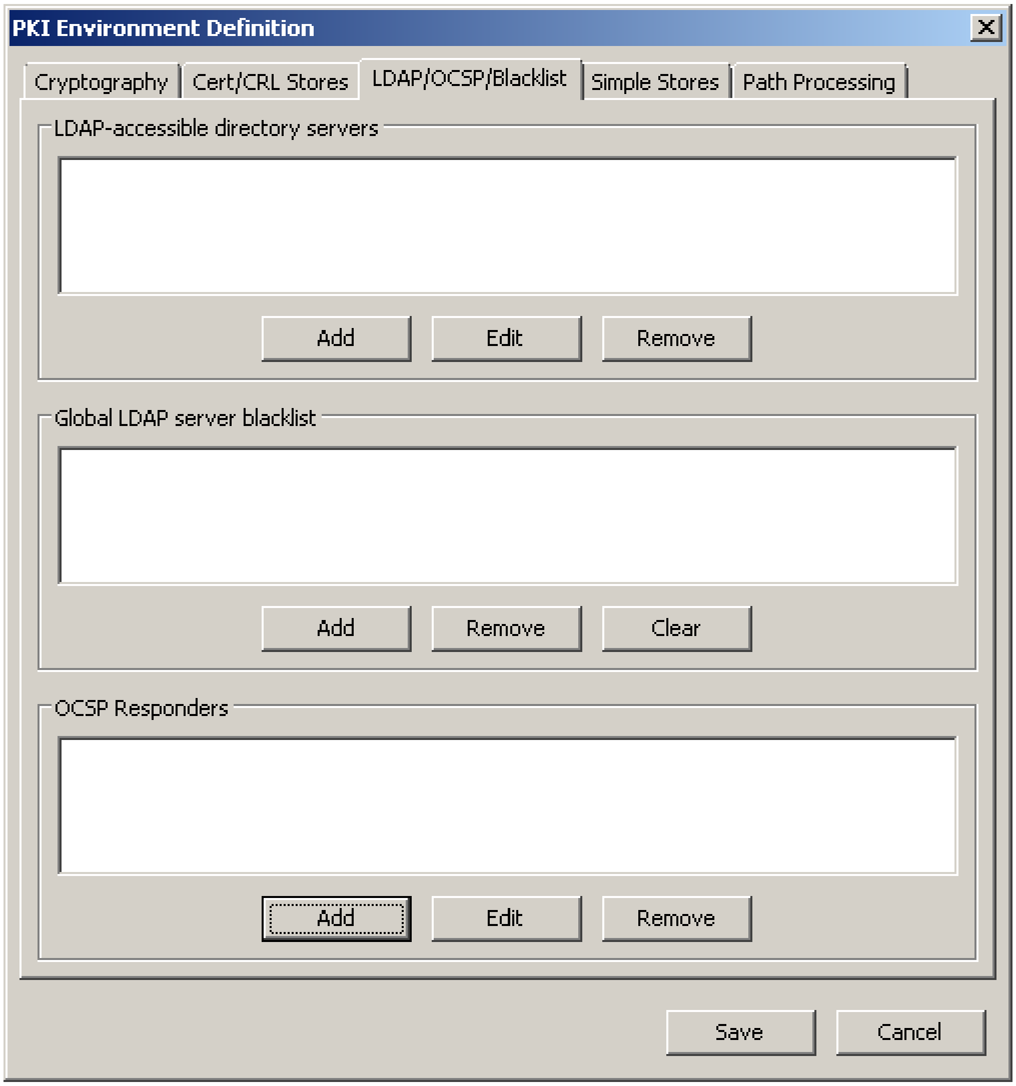
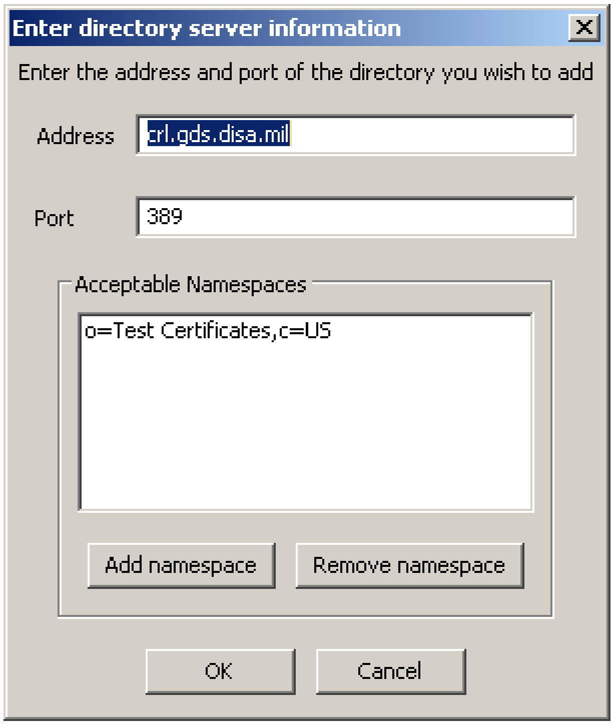


Figure 8 LDAP directories, OCSP responders, Server blacklist panel

LDAP-accessible Directory Servers

To add an LDAP-accessible directory server to the list, click the **Add LDAP Directory** button. The dialog shown below will be displayed. Enter the DNS name or IP address of the directory in the **Address** box. Enter the port in the **Port** box. The default LDAP port, 389, will appear automatically.



Enter directory server information

Enter the address and port of the directory you wish to add

Address: crl.gds.disa.mil

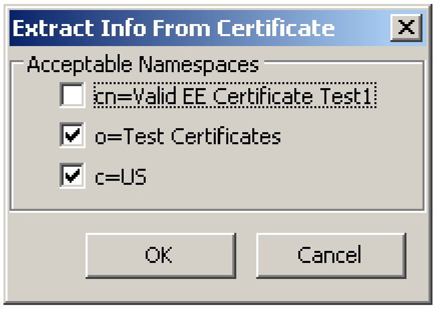
Port: 389

Acceptable Namespaces

o=Test Certificates,c=US

Figure 9 Adding an LDAP directory

To constrain queries sent to the directory to a particular namespace, click the **Add Namespace** button and browse to a file containing a DER-encoded X.509 certificate issued to an entity in the target namespace. The **Extract Info From Certificate** dialog will be displayed. Check the box beside the relative distinguished name element that corresponds to the intended degree of granularity and click the **OK** button. When searching for certificates or CRLs, the directory will only be consulted if the certificate subject name or CRL issuer name falls within the specified namespace. Namespaces can be used to avoid sending queries to enterprise directories for artifacts from an external PKI. To remove a namespace from the list, select the namespace to delete and click the **Remove namespace** button.



Extract Info From Certificate

Acceptable Namespaces

☐ cn=Valid EE Certificate Test1

☑ o=Test Certificates

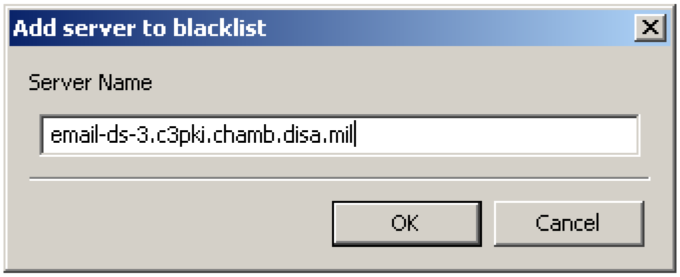
☑ c=US

Figure 10 Configuring a namespace

To edit a previously specified directory, select the directory to edit in the list and click the **Edit Selected Directory** button. Edit the directory specification and click the **OK** button. To remove a directory from the list, select the directory to delete in the list and click the **Remove Selected Directory** button.

Global LDAP Server Blacklist

In some environments, certificates are issued containing CRL DP extensions or AIA extensions that point to server resources that are taken out of service, are overburdened or are otherwise problematic. Application performance is negatively impacted when these resources are used. Most commonly, these problematic infrastructure components are directory servers. PKIFv2.1 provides a new blacklist feature to allow application administrators to specify servers that should be avoided during certification path processing. To add a server to the blacklist, click the **Add Server** button and enter the DNS name or IP address of the server in the resulting dialog box, as shown below.



Server Name: email-ds-3.c3pki.chamb.disa.mil

Figure 11 Adding a server to the blacklist

To remove a server from the blacklist, highlight the server to delete in the list and click the **Remove Server** button. To remove all entries from the blacklist, click the **Clear** button.

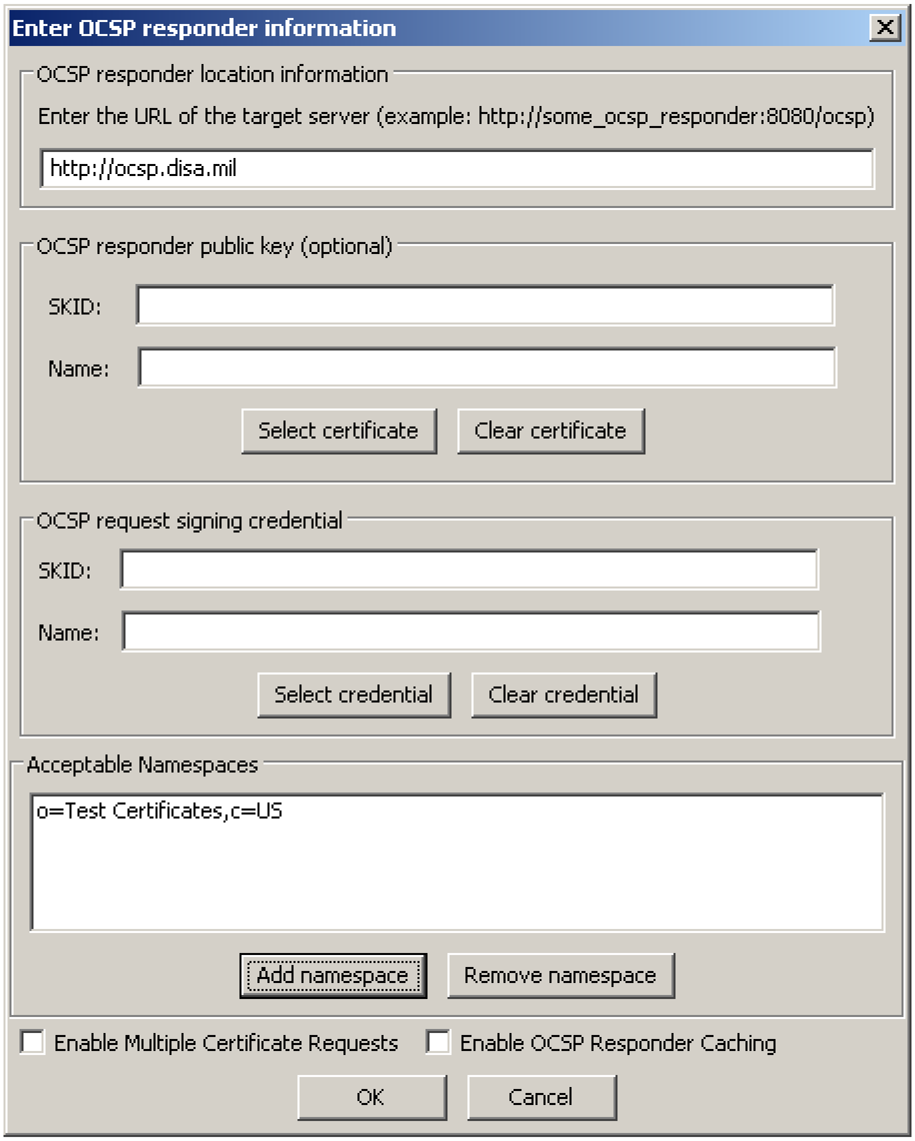
OCSP Responders

To add an OCSP responder to the list, click the **Add OCSP Responder** button. The dialog shown below will be displayed. Enter the URL of the responder in the **OCSP responder location information** box. To require the responder to sign using a particular certificate, click the **Select certificate** button and browse to a file containing the responder’s certificate. The certificate will still be verified to a trust anchor, but responses must be signed using the key included in the certificate selected here. If a self-signed certificate is used to verify response signatures, the certificate must reside in a trust anchor store selected on the **Cert/CRL Stores** panel.

To sign OCSP requests sent to this responder, click the **Select credential** button and choose a signing credential from the resulting dialog box. The credentials shown must reside in one of the private key stores associated with a cryptography back-end selected on the **Cert/CRL Stores** panel.

To add a namespace click the **Add namespace** and follow the directions provided above for specifying namespaces for LDAP-accessible directory servers.

OCSP requests can include requests for the status of multiple certificates, for example, all of the certificates included in a certification path. However, not all responders support requests containing multiple certificates. To avoid sending requests containing multiple certificates uncheck the **Enable Multiple Certificate Requests** option.



Enter OCSP responder information

OCSP responder location information

Enter the URL of the target server (example: http://some_ocsp_responder:8080/ocsp)

http://ocsp.disa.mil

OCSP responder public key (optional)

SKID:

Name:

OCSP request signing credential

SKID:

Name:

Acceptable Namespaces

o=Test Certificates,c=US

□ Enable Multiple Certificate Requests □ Enable OCSP Responder Caching

Figure 12 OCSP responder specification

To edit a previously specified responder, select the responder to edit in the list and click the **Edit Selected Responder** button. Edit the responder specification and click the **OK** button. To remove a responder from the list, select the responder to delete in the list and click the **Remove Selected Responder** button. To enable OCSP Responder Caching check **Enable OCSP Responder Caching** button.

Simple trust anchor, certificate and CRL stores

The **Simple Stores** panel can be used when the **Simple trust anchor store** option from the **Trust anchor stores** box or the **Certificates** or **CRLs** option for the **In-memory cache** box on the **Cert/CRL Stores** panel are selected.

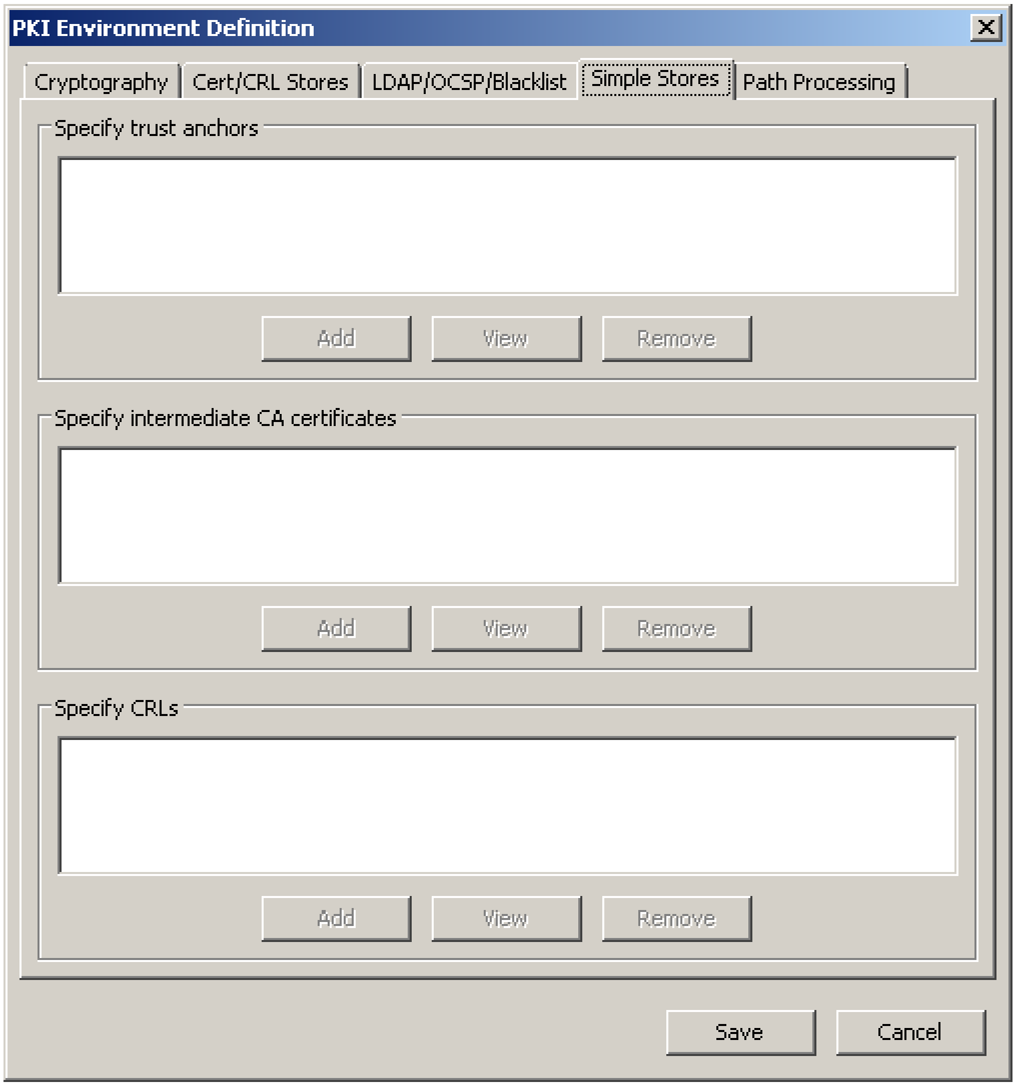


Figure 13 Simple Stores panel

Trust anchors

To add a trust anchor to the simple trust anchor store, click the **Add trust anchor** button and browse to a file containing the DER encoded X.509 certificate issued to the entity being explicitly trusted. To view a previously added certificate, select the item to view in the list and click the **View trust anchor** button. To remove a previously added certificate, select the item to delete in the list and click the **Remove trust anchor** button.

If the buttons associated with the trust anchor list appear grayed out, return to the **Cert/CRL Stores** panel and make sure the **Simple trust anchor store** option from the **Trust anchor stores** box is selected.

Certificates

To add a certificate to the simple certificate store, click the **Add certificate** button and browse to a file containing the DER encoded X.509 certificate to add. To view a previously added certificate, select the item to view in the list and click the **View certificate** button. To remove a previously added certificate, select the item to delete in the list and click the **Remove certificate** button.

If the buttons associated with the certificate list appear grayed out, return to the **Cert/CRL Stores** panel and make sure the **Certificates** option for the **In-memory cache** box is selected.

CRLs

To add a certificate to the simple CRL store, click the **Add CRL** button and browse to a file containing the DER encoded X.509 CRL to add. To view a previously added CRL, select the item to view in the list and click the **View CRL** button. To remove a previously added CRL, select the item to delete in the list and click the **Remove CRL** button.

If the buttons associated with the certificate list appear grayed out, return to the **Cert/CRL Stores** panel and make sure the **CRLs** option for the **In-memory cache** box is selected.

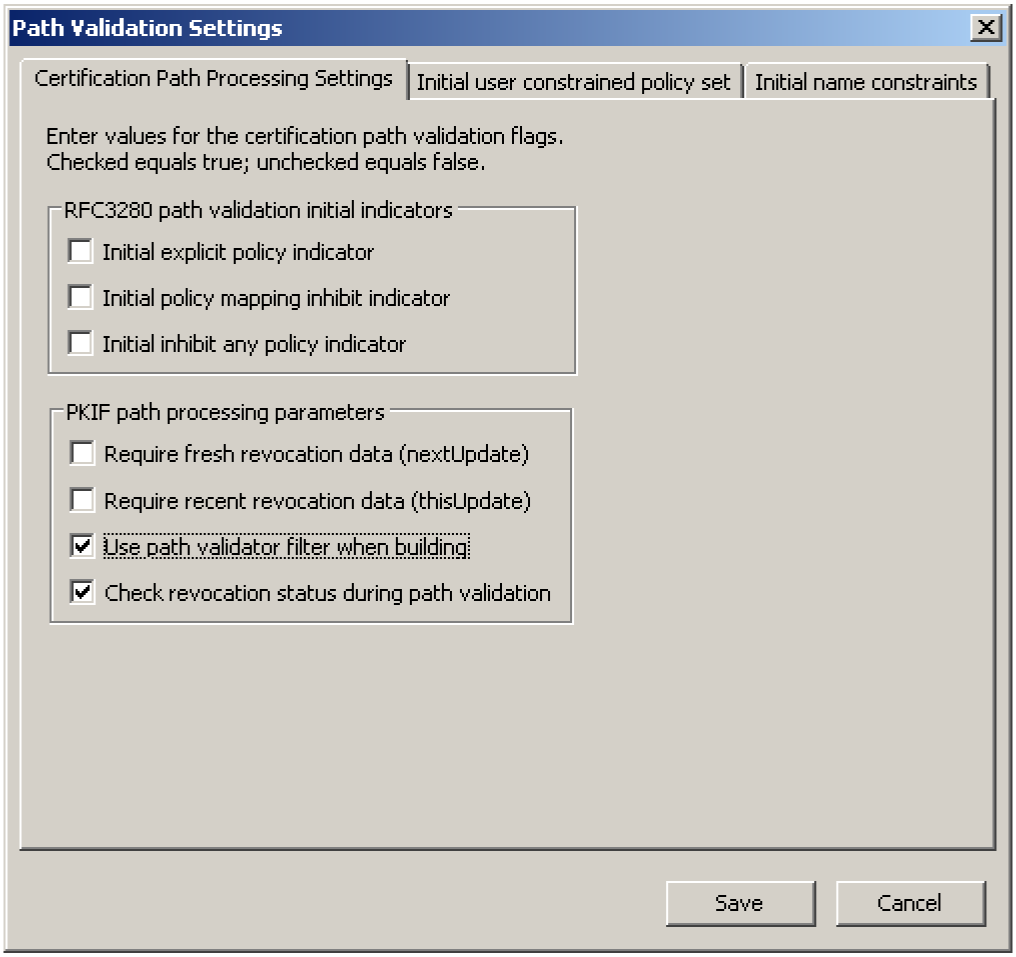
Path Settings Definition

The rules for certificate processing are defined in standards produced by the Internet Engineer Task Force's PKIX working group and include a standard set of inputs for certification path validation. The Path Settings Definition interfaces provide a means of specifying these standard input values, plus several additional parameters to govern certification path validation.

The **RFC3280 path validation initial indicators** box enables specification of the standard path validation inputs specified in RFC3280. The **PKIF path processing parameters** box enables specification of some additional parameters that govern path processing.

When the **Require fresh revocation data** option is selected, the validation time of interest must be before the nextUpdate value included in any revocation information artifacts consulted during path validation. When the **Require recent revocation data** option is selected, the thisUpdate value included in any revocation information artifacts consulted during path validation must be within the *n* days prior to the validation time of interest. By default, *n* is equal to thirty. By default, the validation time of interest is the current system time.

When the **Use path validator filter when building** option is selected, the path development engine will avoid returning paths that are known to be invalid (i.e., due to certificate expiration, certificate policy violations, etc.). When the **Check revocation status during path validation** option is checked, the revocation status of each certificate will be checked. These options are on by default and should remain on in most circumstances.


Path Validation Settings
Certification Path Processing Settings
Initial user constrained policy set
Initial name constraints
Save
Cancel

Enter values for the certification path validation flags.
Checked equals true; unchecked equals false.

RFC3280 path validation initial indicators

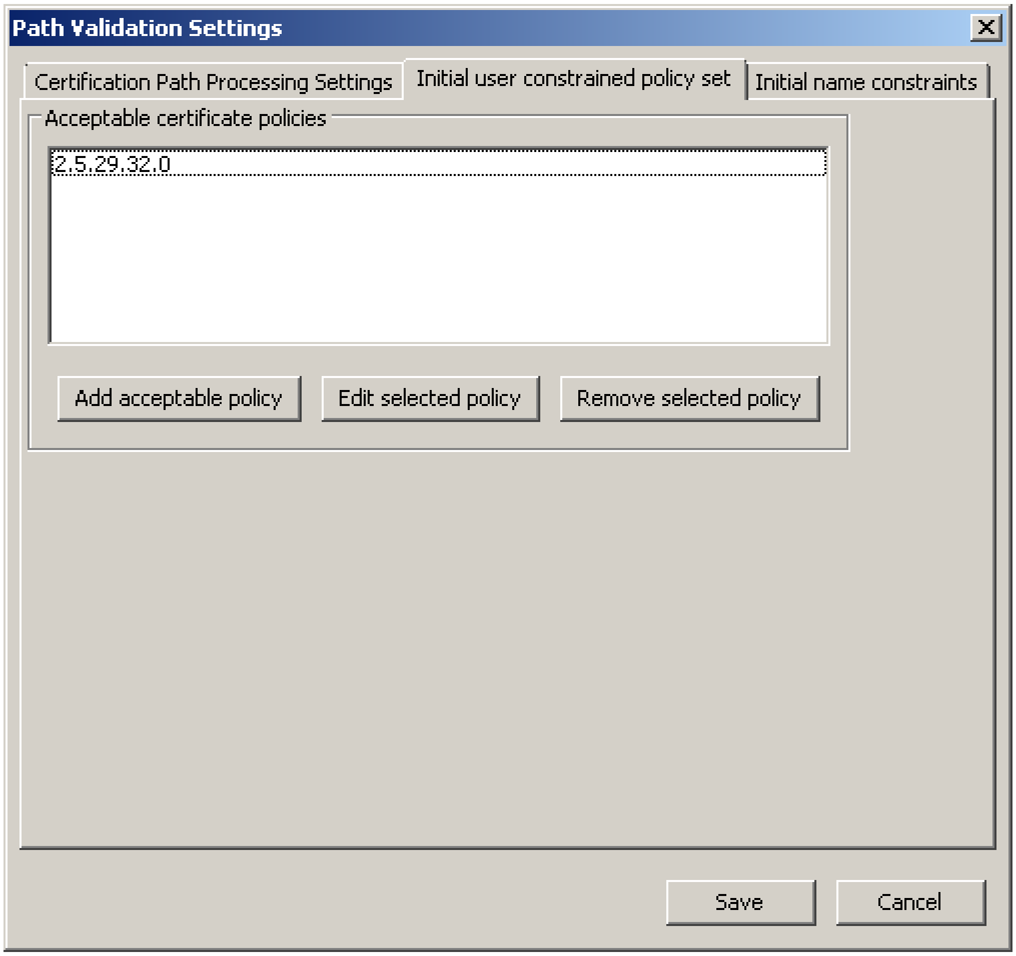
- ☐ Initial explicit policy indicator
- ☐ Initial policy mapping inhibit indicator
- ☐ Initial inhibit any policy indicator

PKIF path processing parameters

- ☐ Require fresh revocation data (nextUpdate)
- ☐ Require recent revocation data (thisUpdate)
- ☑ Use path validator filter when building
- ☑ Check revocation status during path validation

Figure 14 Certification Path Processing Settings

The **Acceptable certificate policies** list enables specification of the initial user constrained policy set, as described in RFC3280. To add a certificate policy to the list, click the **Add acceptable policy** button and enter the object identifier that identifies the desired certificate policy in the resulting dialog box. To edit a previously entered object identifier, select the item to edit in the list and click the **Edit selected policy** button. To remove a previously entered object identifier from the list, select the item to remove in the list and click the **Remove selected policy** button.



2.5.29.32.0

Figure 15 Initial user constrained policy set

The **Acceptable name constraints** list enables specification of the initial name constraints set, as described in RFC5280. To add a name constraint to the list, click the **Add name constraint** button, select name type and enter the desired name constraint in the resulting dialog box. Directory name types can be added using The **Extract Info From Certificate** dialog, by clicking on **Import from cert** button. To remove a previously entered object identifier from the list, select the item to remove in the list and click the **Remove name constraint** button.

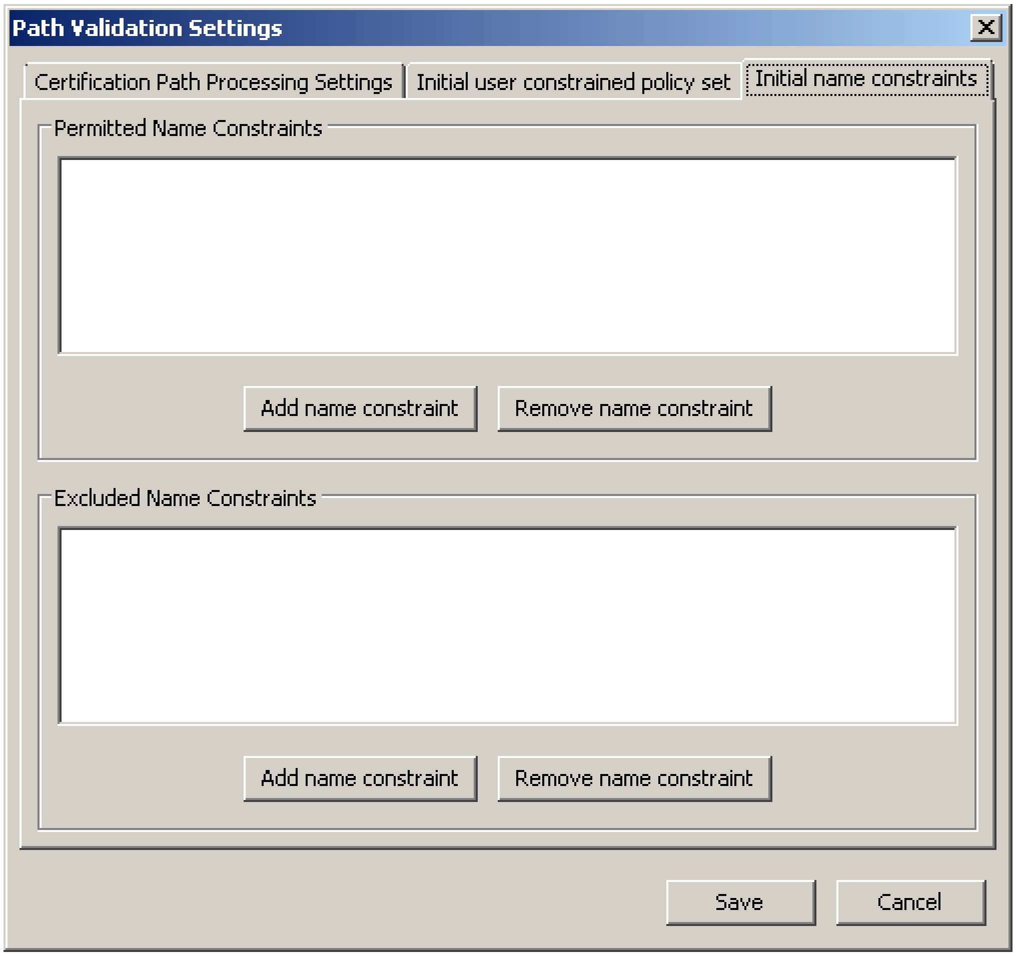


Figure 16 Initial name constraints