PKI Interoperability Test Tool v1.2 (PITT) Usage Guide

Last updated: **September 2010**

CYGNACOM
SOLUTIONS

Table of Contents

Table of Figures

1 Introduction

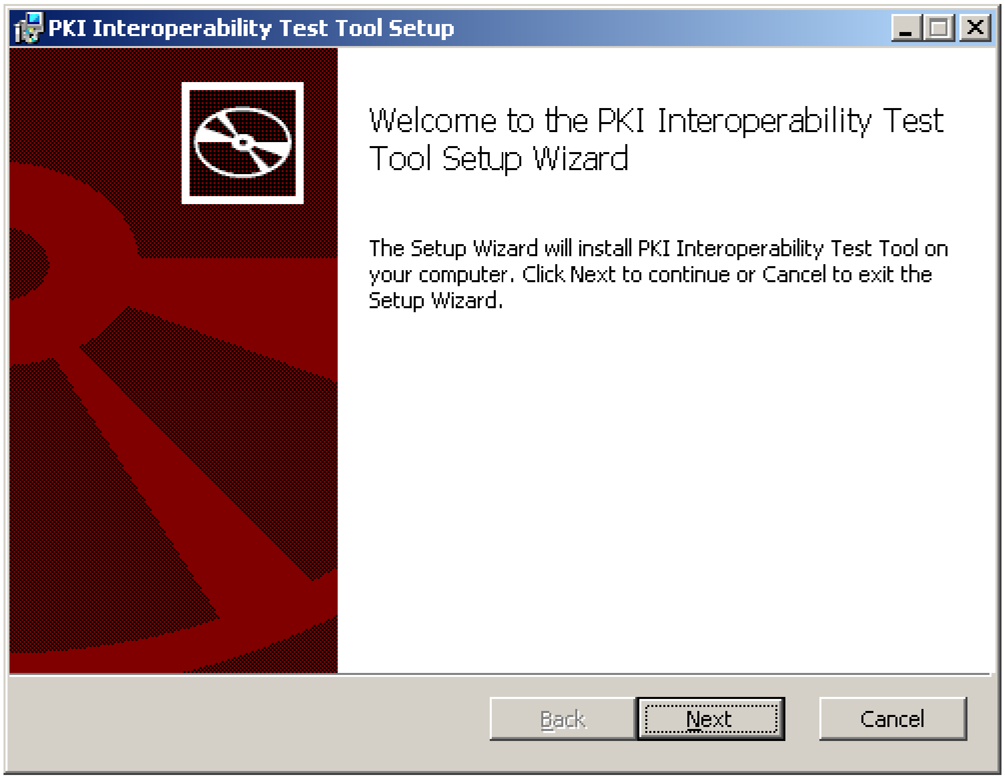
The PKI Interoperability Test Tool v1.1 (PITT) is intended to assist with evaluating interoperability alternatives to establish trust with prospective partner PKIs and to troubleshoot path processing problems.

2 Installation

PITT is installed using the PITT.msi installation package. This installs the PITT application, and dependencies, to a user selected folder. The default installation folder is:

```
    [Program Files]Cygnacom Solutions\PKI Interoperability Test Tool
```

Additionally, default project and results folders are created in the current user's Application Data folder. To install PITT, double-click PITT.exe and navigate through the installer.

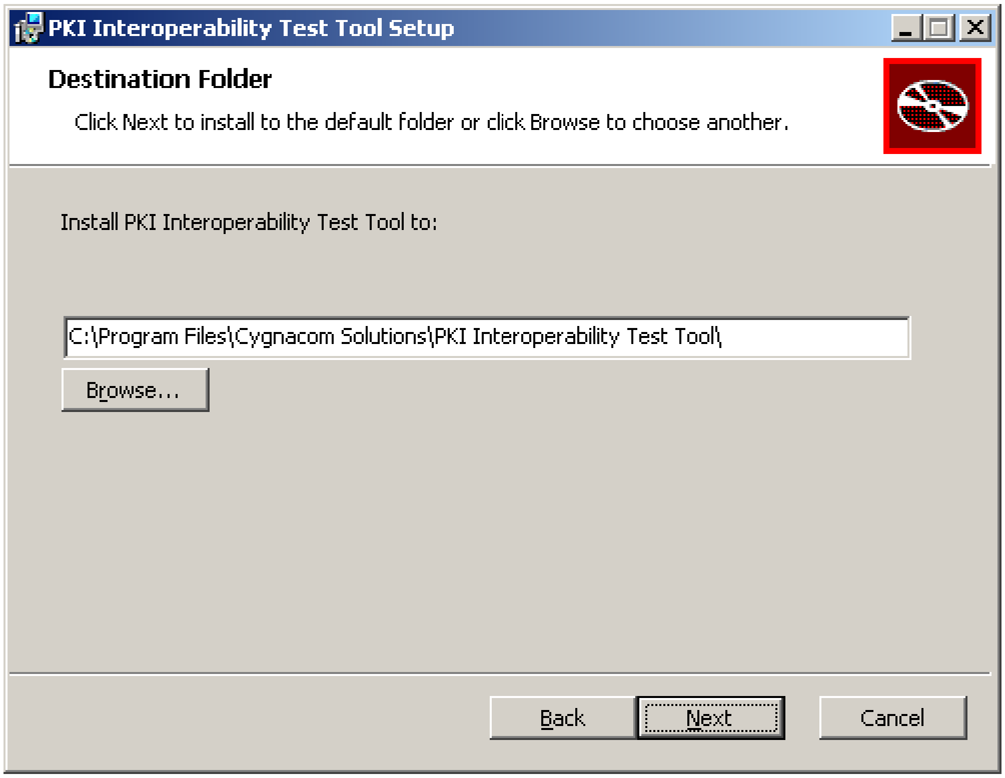


Welcome to the PKI Interoperability Test Tool Setup Wizard

The Setup Wizard will install PKI Interoperability Test Tool on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 1 PKI Interoperability Test Tool Setup

The only customizable option in the installer is the destination folder where PITT will be installed, as shown in the screen shot below. Click **Browse** if an alternative destination folder is desired. Click **Next** to continue installing.



PKI Interoperability Test Tool Setup

Destination Folder

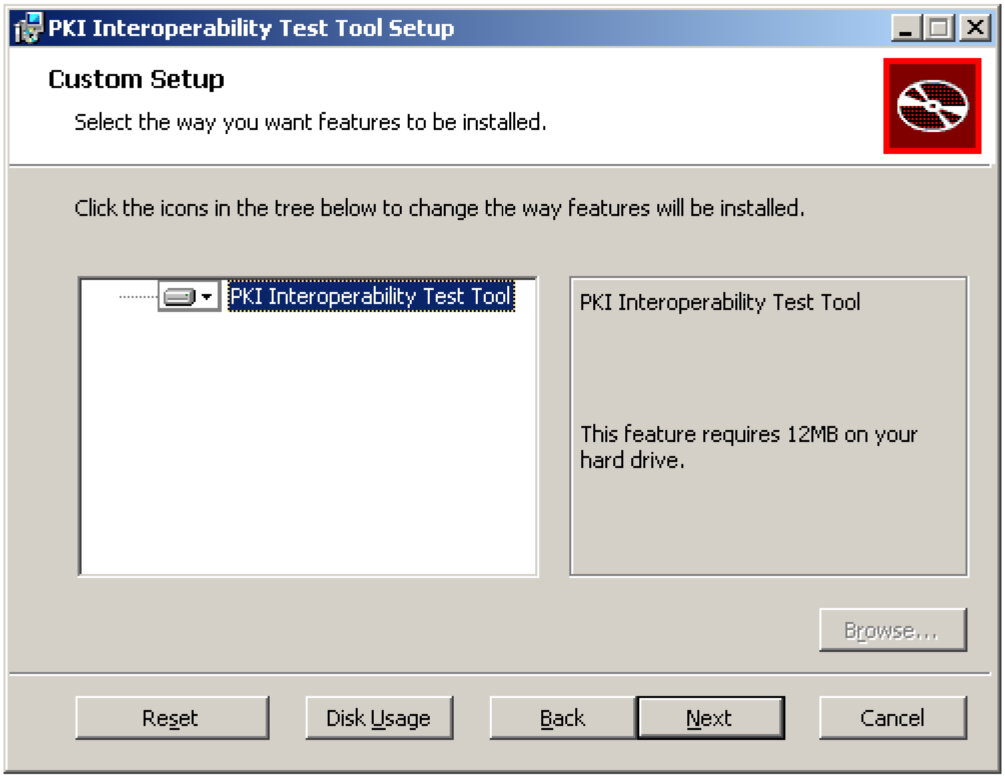
Click Next to install to the default folder or click Browse to choose another.

Install PKI Interoperability Test Tool to:

C:\Program Files\Cygnacom Solutions\PKI Interoperability Test Tool\

Figure 2 Destination folder

The PITT installer contains a single feature. Click **Next** to continue installing.



PKI Interoperability Test Tool Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

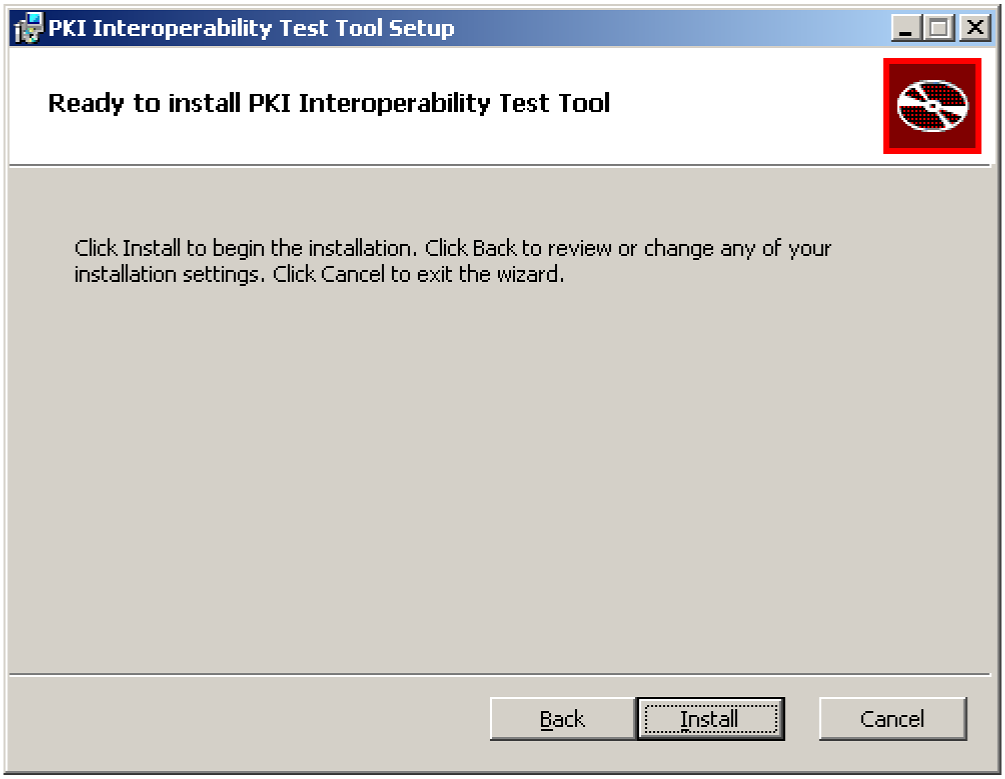
PKI Interoperability Test Tool

PKI Interoperability Test Tool

This feature requires 12MB on your hard drive.

Figure 3 Custom Setup

Click the **Install** button to install PITT.

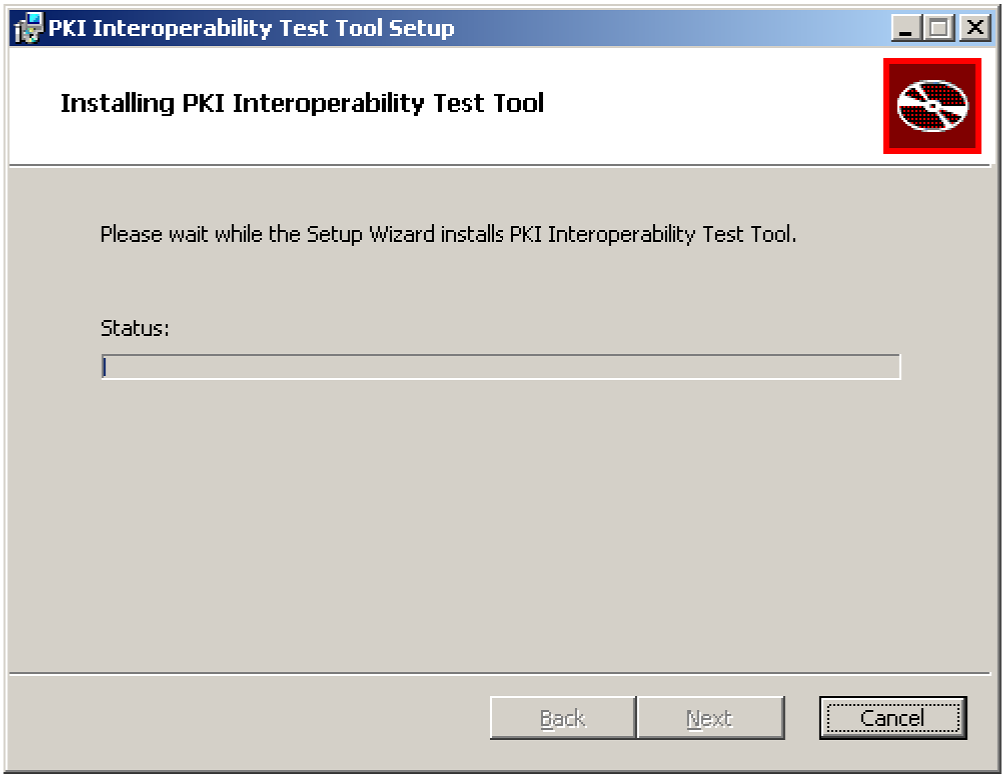


Ready to install PKI Interoperability Test Tool

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 4 Ready to install

Wait patiently while PITT is installed, then click **Next**.



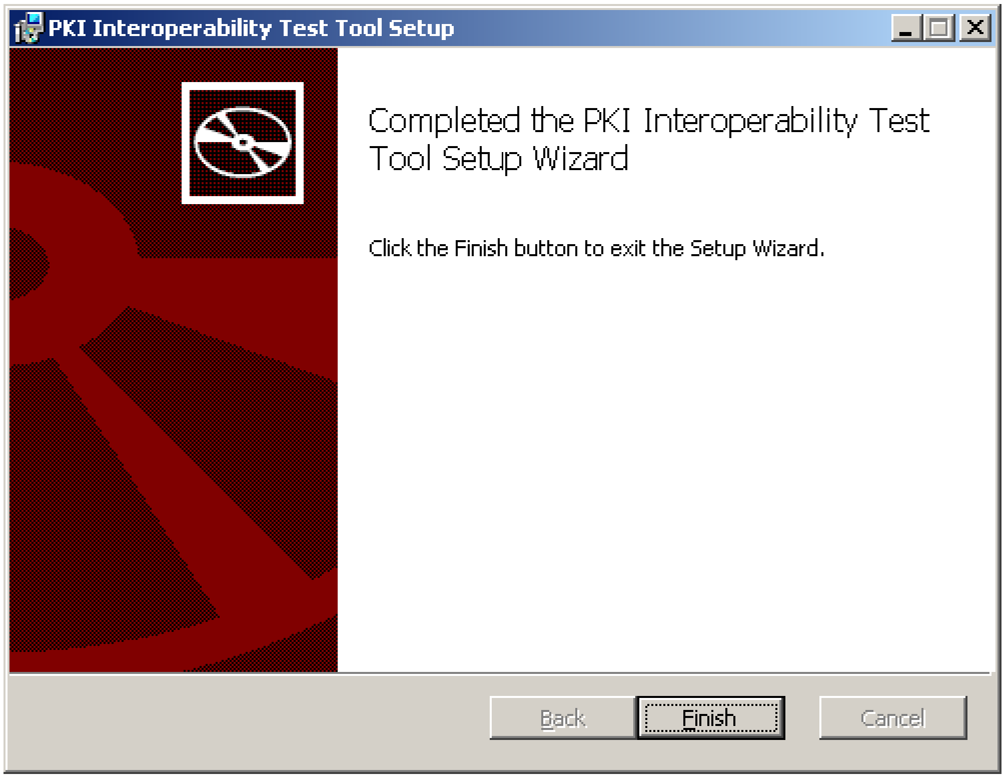
Installing PKI Interoperability Test Tool

Please wait while the Setup Wizard installs PKI Interoperability Test Tool.

Status:

Figure 5 Installing PKI Interoperability Test Tool

Click F**inish** to close the installer. PITT can be launched via a Start menu shortcut or by double clicking the PITT.exe file in the destination folder.



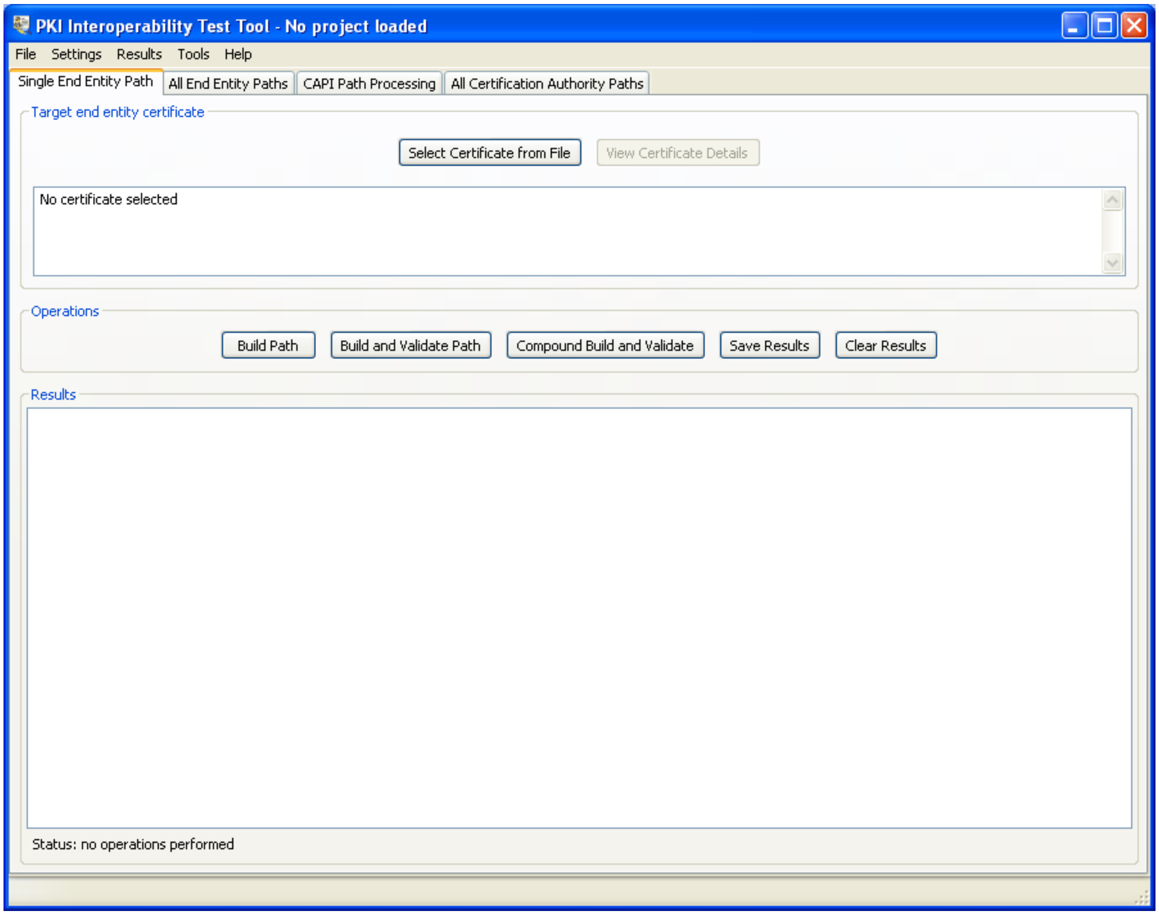
Completed the PKI Interoperability Test Tool Setup Wizard

Click the Finish button to exit the Setup Wizard.

igure 6 Installation complete

3 Quick Start Guide

The PITT installer includes default PKI environment settings that enable basic usage scenarios. These settings apply to the **Single End Entity Path**, **All End Entity Paths** and **All Certification Authority Paths** tabs. The settings do not apply to the **CAPI Path Processing** tab.



No certificate selected

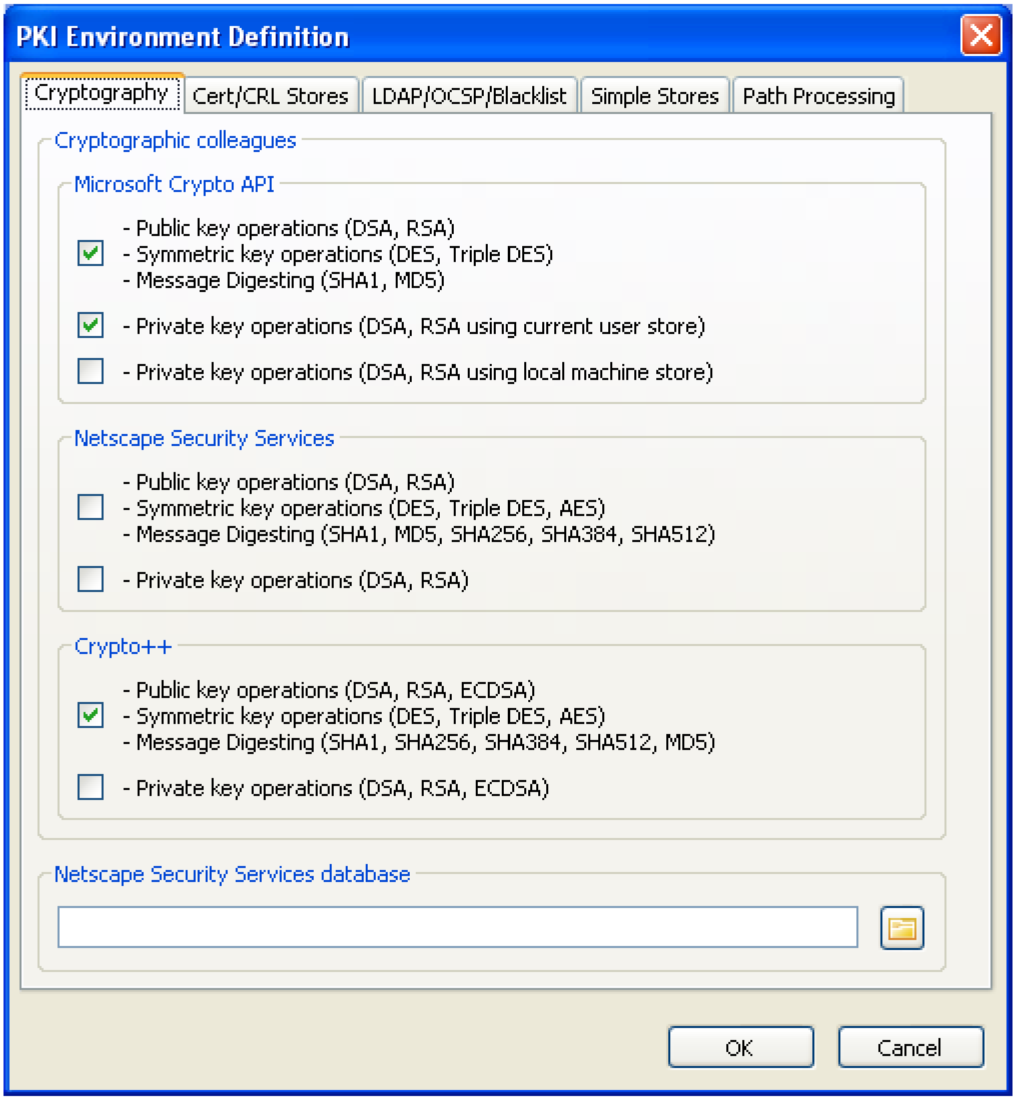
Status: no operations performed

Figure 7 PKI Interoperability Test Tool

3.1 Default settings

The PITT installer established default settings suitable for basic usage scenarios. These settings are described below.

The default cryptography settings include support for all algorithms currently supported by PKIF. The **Private key operations** option in the **Microsoft Crypto API** is enabled in the event that signed OCSP requests are used (though this is not typical). If signed OCSP requests are not used, both **Microsoft Crypto API** options could be unchecked, using **Crypto++** for all cryptographic operations.



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++

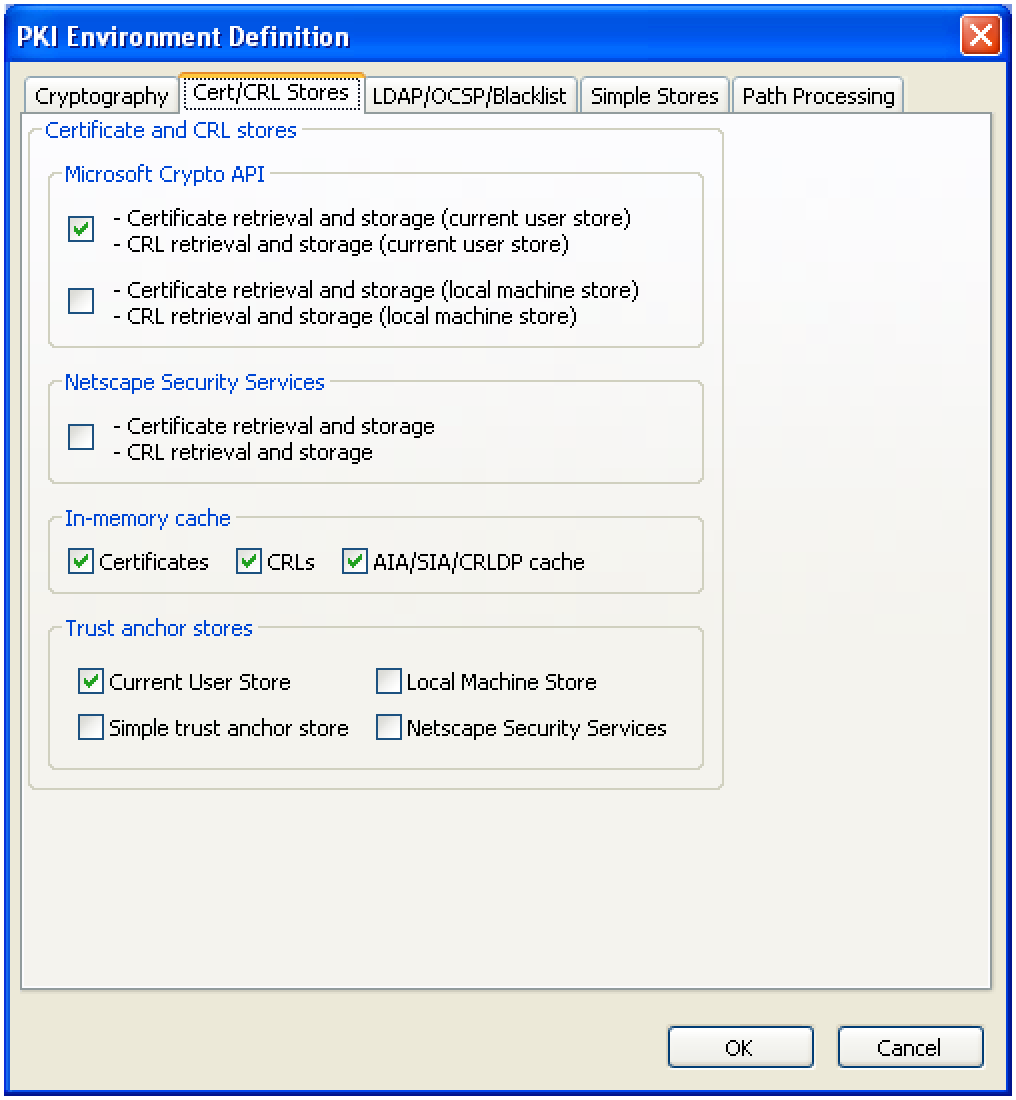
☑ - Public key operations (DSA, RSA, ECDSA)
- Symmetric key operations (DES, Triple DES, AES)
- Message Digesting (SHA1, SHA256, SHA384, SHA512, MD5)

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

Netscape Security Services database

Figure 8 Default Cryptography settings

The default certificate and CRL store settings enable the usage of Microsoft CAPI certificate stores for trust anchor and intermediate CAs and provide in-memory stores for certificates and CRLs plus an in-memory cache for items retrieved from URIs specified in AIA, SIA and CRL DP extensions.



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

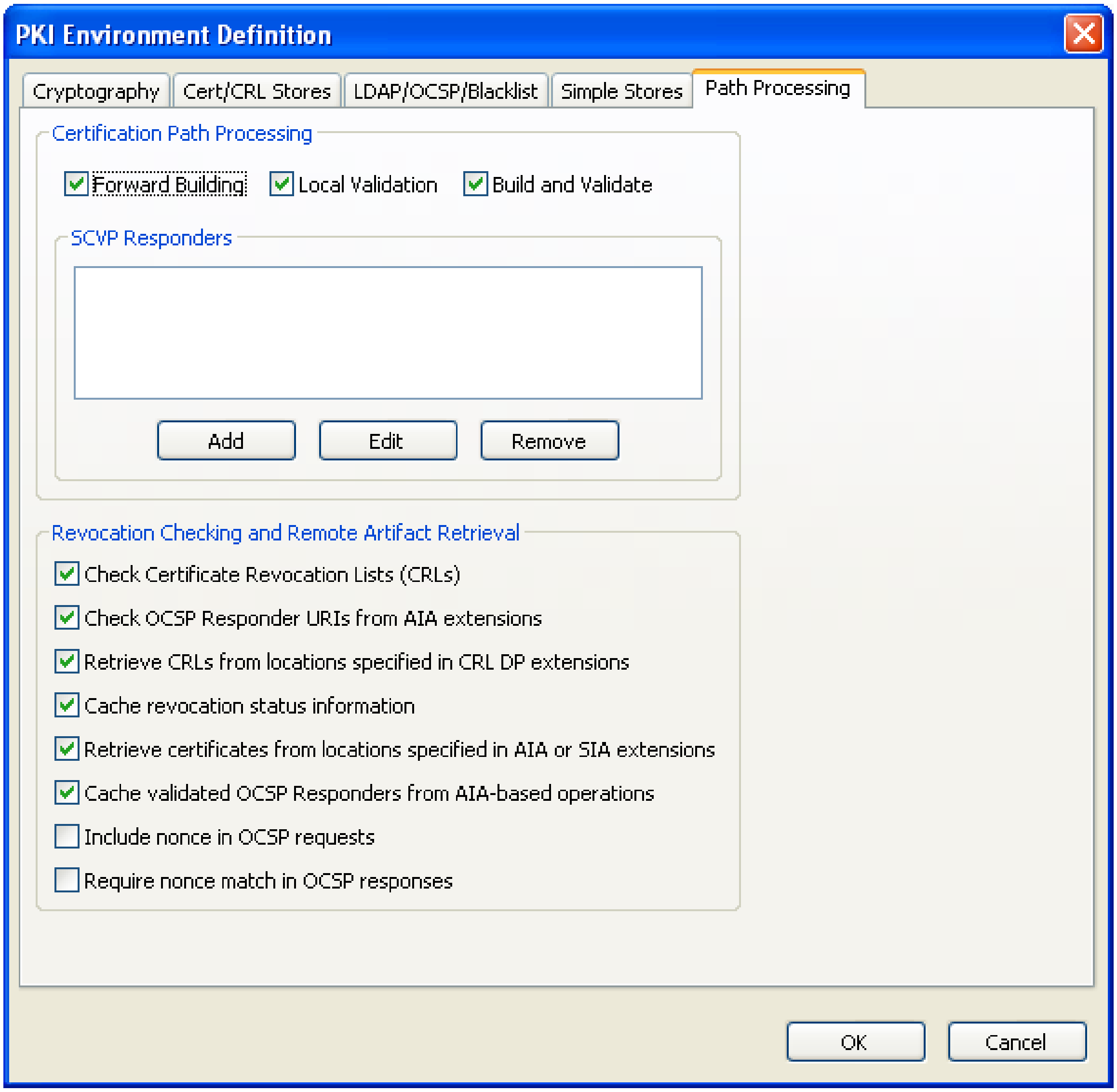
☑ Certificates ☑ CRLs ☑ AIA/SIA/CRLDP cache

Trust anchor stores

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

Figure 9 Default Cert/CRL Stores settings

The default path processing settings enable all path processing features except SCVP. This includes support for checking CRLs and OCSP responses. CRLs are retrieved from locations identified in CRL DP extensions, certificates are retrieved from location specified in authorityInfoAccess (AIA), subjectInfoAccess (SIA) and issuerAltName (IAN) extensions and OCSP responders specified in AIA extensions are queried. Revocation status is cached, as are validated OCSP responders. By default nonces are not included in OCSP requests (and nonce matches are not required).



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

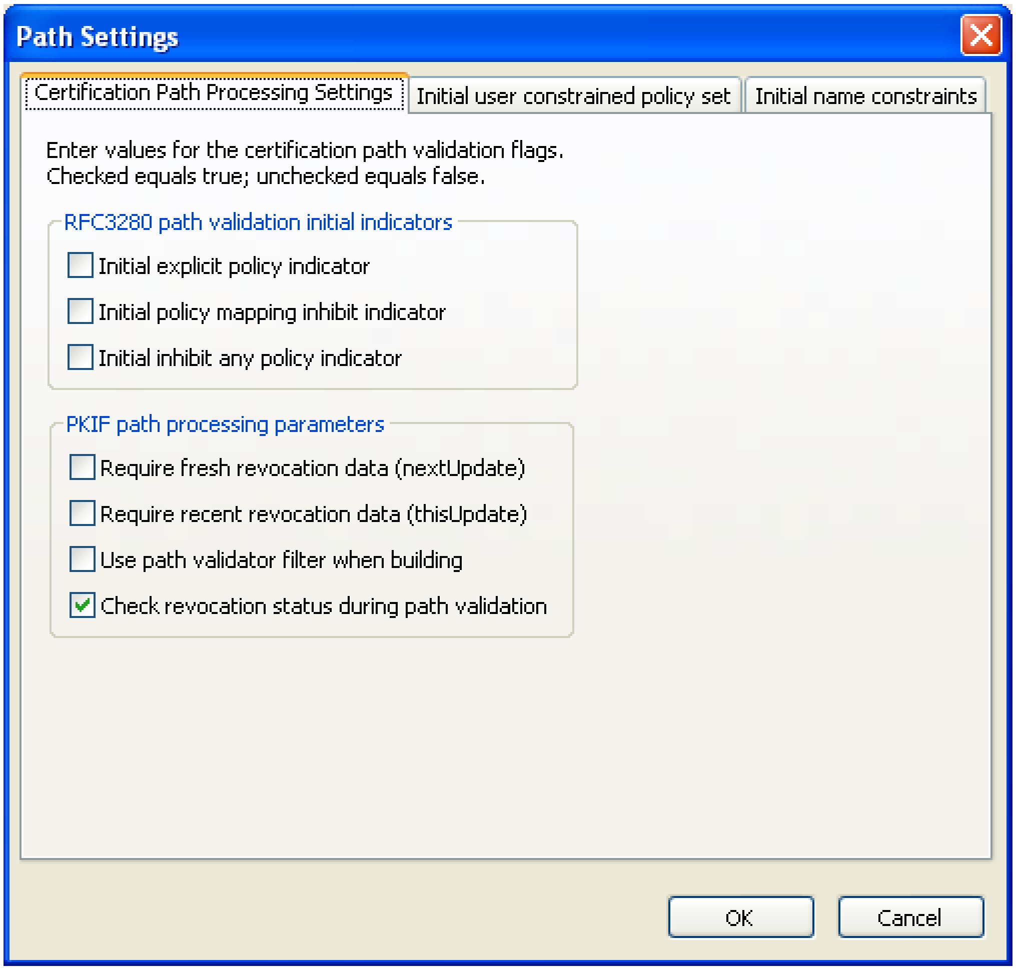
☑ Cache validated OCSP Responders from AIA-based operations

□ Include nonce in OCSP requests

□ Require nonce match in OCSP responses

Figure 10 Default Path Processing settings

The default certification path processing settings are somewhat specific to PITT usage. The **Use path validator filter when building** option is off. In most usage scenarios, this option is turned on. For PITT, the option is off so all builder output is made available.


Path Settings
Certification Path Processing Settings
Initial user constrained policy set
Initial name constraints
OK
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 11Default Certification Path Processing Settings

These settings can be configured as described in Edit Default PKI Settings section below.

4 Menus

This section describes the functionality available via the PITT menus.

4.1 File Menu

4.1.1 New Project

The **File->New Project** menu item causes the creation of a new project initialized with the current default PKI settings and no target certificates. The name of the project will appear in the title bar and project related menu options will be enabled. To configure the project, use the **Settings->Edit Project PKI Settings** menu item and select target certificates on each panel. After configuring the settings for the new project, save the settings using **File->Save Project** or **File->Save Project As**.

4.1.2 Open Project

The **File->Open Project** menu option can be used to open a previously saved project. The name of the project will appear in the title bar and project related menu options will be enabled. It is possible that some resources that were available when the settings were created are not available when settings are loaded; for example, an NSS database may have been moved or deleted.

4.1.3 Close Project

The **File->Close Project** menu option can be used to close an open project. Default PKI settings are restored and all target certificates, URI check results and path processing results are cleared. "No project loaded" appears in the title bar. Default PKI settings can be configured using the **Settings->Edit Default PKI Settings** menu option.

4.1.4 Save Project

The **File->Save Project** menu option can be used to save project settings for later use. The project file contains the target certificates from each panel plus the settings that can be reviewed and configured via the **Settings->Edit Project PKI Settings** menu option. The settings accessed via the **Settings->Edit Default PKI Settings** and **Settings->Edit PITT Settings** menu options are not stored in the project file. The project is saved to the location indicated in the title bar.

4.1.5 Save Project As

The **File->Save Project As** menu option is similar to the **File->Save Project** option except the user is allowed to specify a new name for the project settings. This allows the user to create project files containing settings with slight variations without re-entering all settings from scratch. The title bar will be updated to reflect the new project name.

4.1.6 Recent Projects

The **File->Recent Projects** menu option allows recently opened projects to be opened quickly.

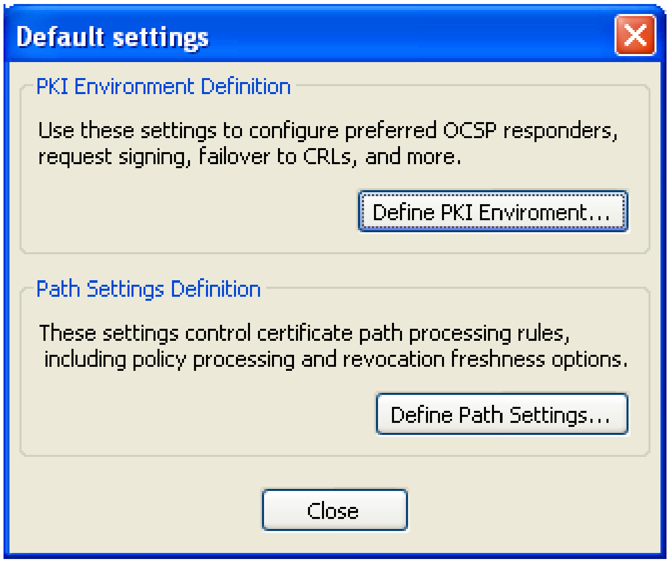
4.1.7 Exit

The **File->Exit** menu option is used to close the PITT.

4.2 Settings Menu

4.2.1 Edit Default PKI Settings

The **Settings->Edit Default PKI Settings** menu option is used to configure the default PKI settings, which are used no project is loaded. Default PKI settings are also used to initialize projects created using the **File->New Project** menu option. The following dialog is displayed when the **Edit Default PKI Settings** option is selected.



Use these settings to configure preferred OCSP responders, request signing, failover to CRLs, and more.

These settings control certificate path processing rules, including policy processing and revocation freshness options.

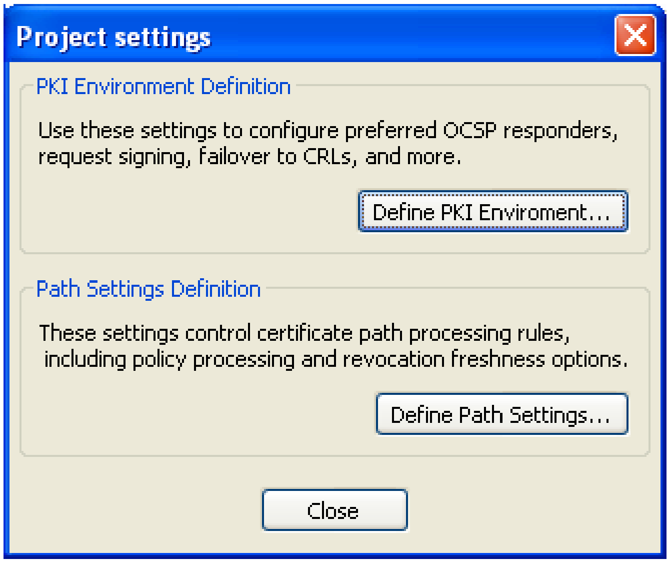
Figure 12 Edit Default PKI Settings

The **Define PKI Environment…** and **Define Path Settings…** buttons launch standard PKIF configuration dialogs. Usage of these dialogs is described in the PKIF Resources Usage Guide (http://pkif.sourceforge.net/pkifresources_usage.pdf). Default PKI settings are saved to the system registry.

Default PKI settings govern the behavior of the **Single End Entity Path**, **All End Entity Paths** and **All Certification Authority Paths** panels. The **CAPI Path Processing** panel is not affected except when the **PITT Settings-> Input policies to CAPI** options, in which case the **User constrained policy set** is used.

4.2.2 Edit Project PKI Settings

The **Settings->Edit Default PKI Settings** menu option is used to configure the default PKI settings, which are loaded when the PITT is launched and are used to initialize projects created using the **File->New Project** menu option. The following dialog is displayed when the option is selected.



Use these settings to configure preferred OCSP responders, request signing, failover to CRLs, and more.

These settings control certificate path processing rules, including policy processing and revocation freshness options.

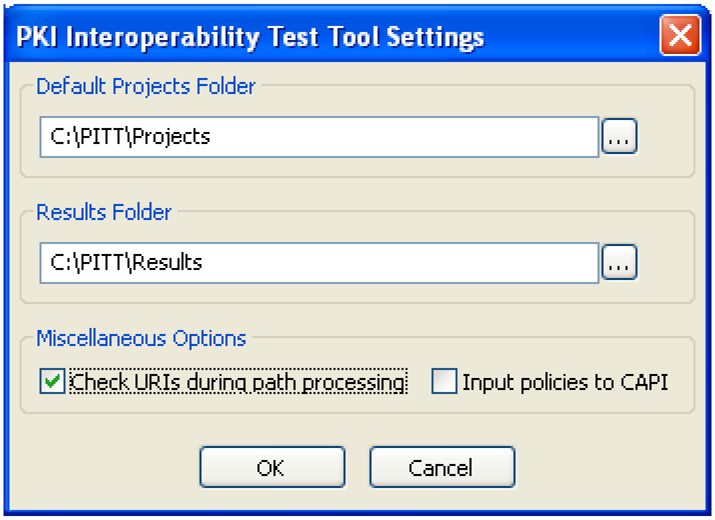
Figure 13 Edit Project PKI Settings

The **Define PKI Environment…** and **Define Path Settings…** buttons launch standard PKIF configuration dialogs. Usage of these dialogs is described in the PKIF Resources Usage Guide (http://pkif.sourceforge.net/pkifresources_usage.pdf).

Project PKI settings govern the behavior of the **Single End Entity Path**, **All End Entity Paths** and **All Certification Authority Paths** panels. The **CAPI Path Processing** panel is not affected except when the **PITT Settings-> Input policies to CAPI** options, in which case the **User constrained policy set** is used.

4.2.3 Edit PITT Settings

The **Settings->Edit PITT Settings** menu option is used to configure global settings that govern PITT operation. The following dialog is displayed when the option is selected.



Default Projects Folder: C:\PITT\Projects

Results Folder: C:\PITT\Results

☑ Check URIs during path processing ☐ Input policies to CAPI

Figure 14 PITT Settings

The **Default Projects Folder** option is used to set the location where projects will be created by default when the **File->New Project** menu option is selected. Users can select alternative storage locations when a project is created.

The **Results Folder** option is used to set the location where summary reports are generated.

The **Check URIs during path processing** option causes PITT to check all URIs in each certificate present in each certification path discovered on the **Single End Entity Path**, **All End Entity Paths** or **All Certification Authority Paths** panels. The results are written to the bottom of the path log for each path.

The **Input policies to CAPI** option causes PITT to input any certificate policy specified on the effective **Initial user constrained policy set** panel of the **Path Settings** notebook, i.e., the policy set from either the default PKI settings or project PKI settings.

4.3 Results Menu

4.3.1 Generate Summary Report

PITT can generate HTML reports summarizing the results produced on the **Single End Entity Path** panel. The report is generated using the PittReport.xsl file, which is installed beside Pitt.exe in the destination folder by the installer. This .xsl file is used to transform XML output that is written to the **Results Folder** to produce an HTML report. The location of the results can be configured as described in the Edit PITT Settings section. XML and HTML files are named using the time of generation.

4.3.2 Clear All Results

The **Results->Clear All Results** menu option clears any results on any of the panels.

4.4 Tools Menu

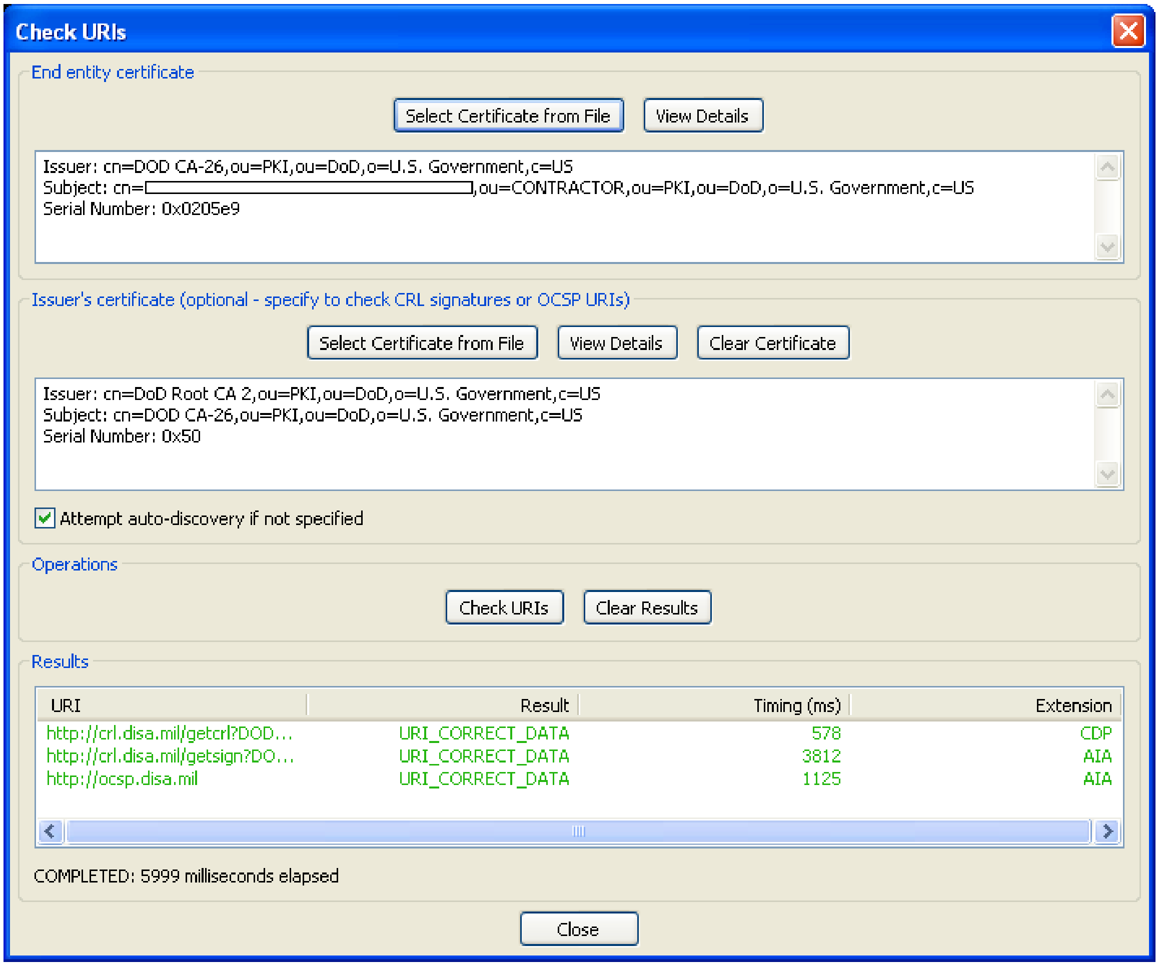
4.4.1 Check URIs in certificate

The **Tools->Check URIs in certificate** enable URIs contained in a certificate to be tested independent of certification path processing. Each HTTP[1] and LDAP URI present in an authority information access (AIA), subject information access (SIA) or CRL distribution points (CRL DP) extension will be retrieved and evaluated relative to the certificate containing the extension. If the issuer's certificate is specified or **Attempt auto-discovery if not specified** is checked (and is successful) then CRL signatures will be verified[2] and OCSP AIA URIs will be tested. The following screen shot shows the Check URIs dialog with results following a check URI operation. Note, full certification path processing is not performed in support of CRL signature verification or OCSP

[1] This excludes OCSP URIs, which are not inspected as part of this check.

[2] CRL signatures are only verified using the issuer's public key. To test scenarios involving CRLs signed with a new CA key or indirect CRLs, perform full certification path processing using one of the tabs.

processing. Use one of the panels to perform full path processing of revocation status providers in the context of a certificate validation.


Check URIs
End entity certificate
Select Certificate from File
View Details

Issuer: cn=DOD CA-26,ou=PKI,ou=DoD,o=U.S. Government,c=US
Subject: cn=[redacted],ou=CONTRACTOR,ou=PKI,ou=DoD,o=U.S. Government,c=US
Serial Number: 0x0205e9

Issuer's certificate (optional - specify to check CRL signatures or OCSP URIs)
Select Certificate from File
View Details
Clear Certificate

Issuer: cn=DoD Root CA 2,ou=PKI,ou=DoD,o=U.S. Government,c=US
Subject: cn=DOD CA-26,ou=PKI,ou=DoD,o=U.S. Government,c=US
Serial Number: 0x50

☑ Attempt auto-discovery if not specified

Operations
Check URIs
Clear Results
Results

URI	Result	Timing (ms)	Extension
http://crl.disa.mil/getcrl?DOD…	URI_CORRECT_DATA	578	CDP
http://crl.disa.mil/getsign?DO…	URI_CORRECT_DATA	3812	AIA
http://ocsp.disa.mil	URI_CORRECT_DATA	1125	AIA

COMPLETED: 5999 milliseconds elapsed

Figure 15 Check URIs dialog

To specify the certificate that contains the URIs to check, click the **Select Certificate from File** button, browse to a file containing a DER encoded certificate then click **Open**. The issuer name, serial number and subject name will be displayed in the **Target end entity certificate** text box. To view the certificate using the Microsoft shell viewer, click the **View Details** button.

To check the URIs in the certificate, click the **Check URIs** button.

URI_NOT_AVAILABLE indicates that URI is not available.
URI_CORRECT_DATA indicates that URI points to correct information for the target certificate.
URI_INCORRECT_DATA indicates that URI points to incorrect information for the target certificate.
URI_WARNING indicates that URI points to a certificate collection that includes a self-signed certificate.

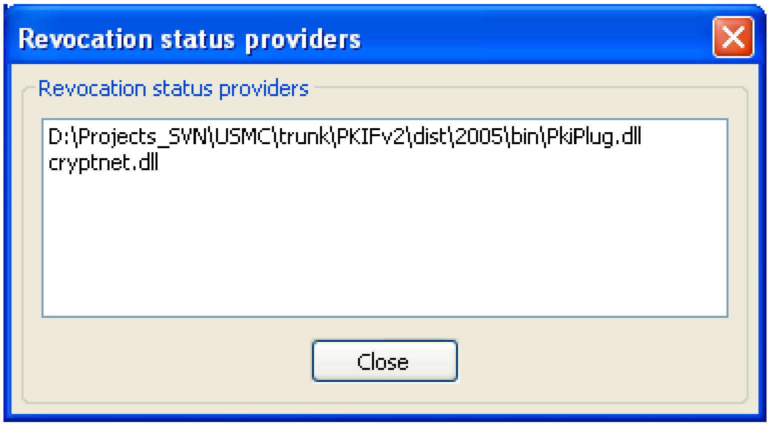
URI_UNKNOWN_ACCESS_METHOD indicates that SIA or AIA extension contains unknown access method.

4.4.2 List CAPI revocation status providers

The **Tools->List CAPI revocation status providers** menu item can be used to display a list of revocation status providers registered with the host operating system. The list presented is read from:

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 1\CertDllVerifyRevocation\DEFAULT

The following screenshot shows an example.



```
D:\Projects_SVN\USMC\trunk\PKIFv2\dist\2005\bin\PkiPlug.dll
cryptnet.dll
```

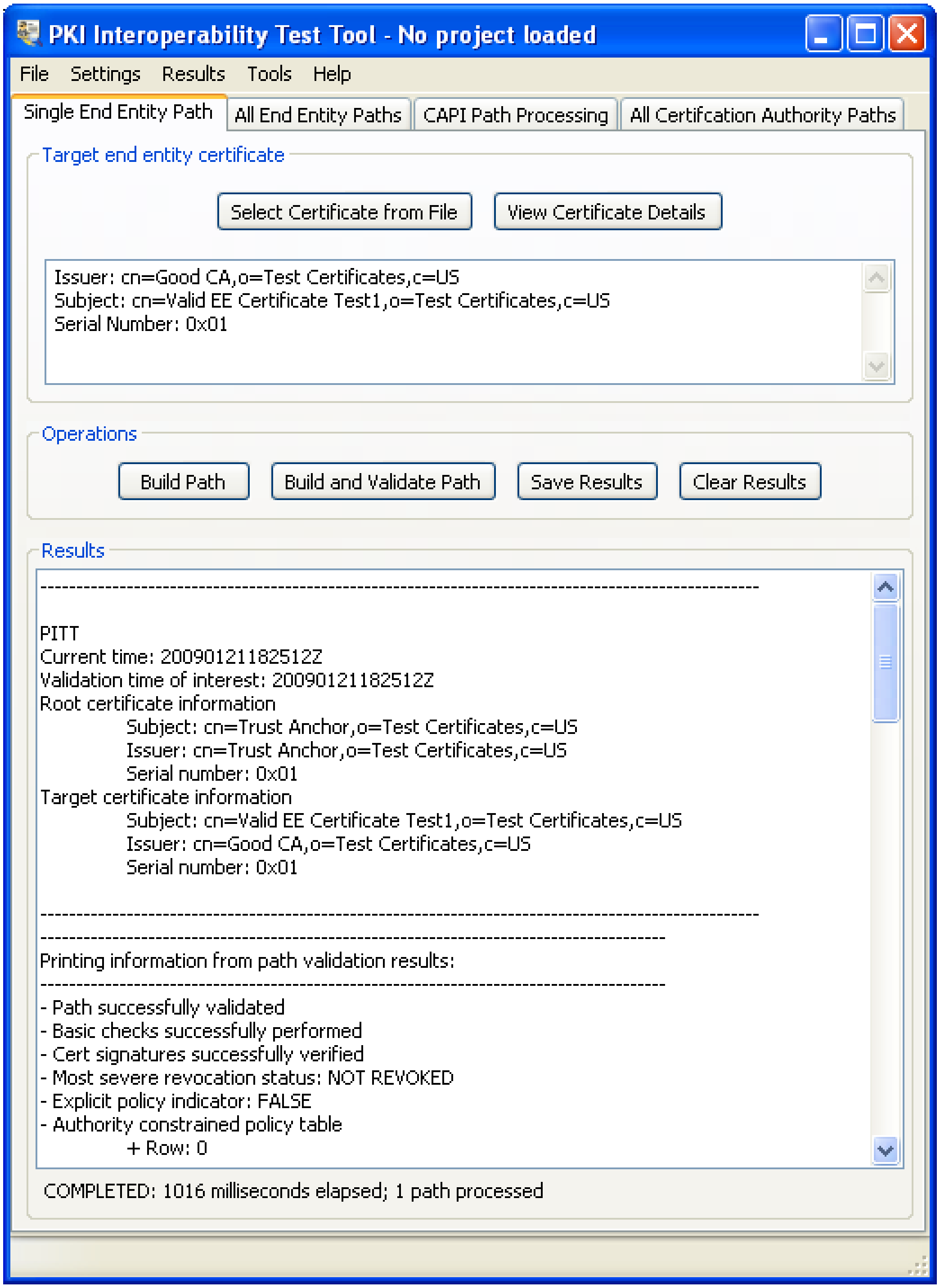
Figure 16 List revocation status providers dialog

5 Panels

PITT consists of four panels, each of which provides different functionality.

5.1 Single End Entity Path

The **Single End Entity Path** panel can be used to build the “best” certification path from a specified end entity certificate to an available trust anchor using PKIF. The following screen shot shows the Single End Entity Panel with results following a **Build and Validate Path** operation.



```
Issuer: cn=Good CA,o=Test Certificates,c=US
Subject: cn=Valid EE Certificate Test1,o=Test Certificates,c=US
Serial Number: 0x01
```

```
------------------------------------------------------------------------------------------


PITT
Current time: 20090121182512Z
Validation time of interest: 20090121182512Z
Root certificate information
            Subject: cn=Trust Anchor,o=Test Certificates,c=US
            Issuer: cn=Trust Anchor,o=Test Certificates,c=US
            Serial number: 0x01
Target certificate information
            Subject: cn=Valid EE Certificate Test1,o=Test Certificates,c=US
            Issuer: cn=Good CA,o=Test Certificates,c=US
            Serial number: 0x01


------------------------------------------------------------------------------------------
------------------------------------------------------------------------------
Printing information from path validation results:
------------------------------------------------------------------------------
- Path successfully validated
- Basic checks successfully performed
- Cert signatures successfully verified
- Most severe revocation status: NOT REVOKED
- Explicit policy indicator: FALSE
- Authority constrained policy table
            + Row: 0
```

```
COMPLETED: 1016 milliseconds elapsed; 1 path processed
```

Figure 17 Single End Entity Panel

To specify the certificate to which a certification path should be constructed, click the **Select Certificate from File** button, browse to a file containing a DER encoded certificate then click **Open**. The issuer name, serial number and subject name will be displayed in the **Target end entity certificate** text box. To view the certificate using the Microsoft shell viewer, click the **View Details** button.

To build a certification path without performing certification path validation, click the **Build Path** button. The effective PKI settings will be used to discover a certification path, if possible. The results of the operation will be written to the **Results** text box. Status information will be written immediately below the **Results** text throughout and following the operation.

To build and validate a certification path, click the **Build and Validate Path** button. The effective PKI settings will be used to discover and validate a certification path, if possible. The results of the operation will be written to the **Results** text box. Status information will be written immediately below the **Results** text throughout and following the operation.

To save the results of an operation, click the **Save Results** button then browse to the file folder to which the results should be written. Each artifact in the certification path, including revocation information if present, will be written to a file named with a hash of the artifact and an indication of the files contents. A file named PathManifest.txt will provide additional information that may be useful when reviewing the results of a processing a certification path.

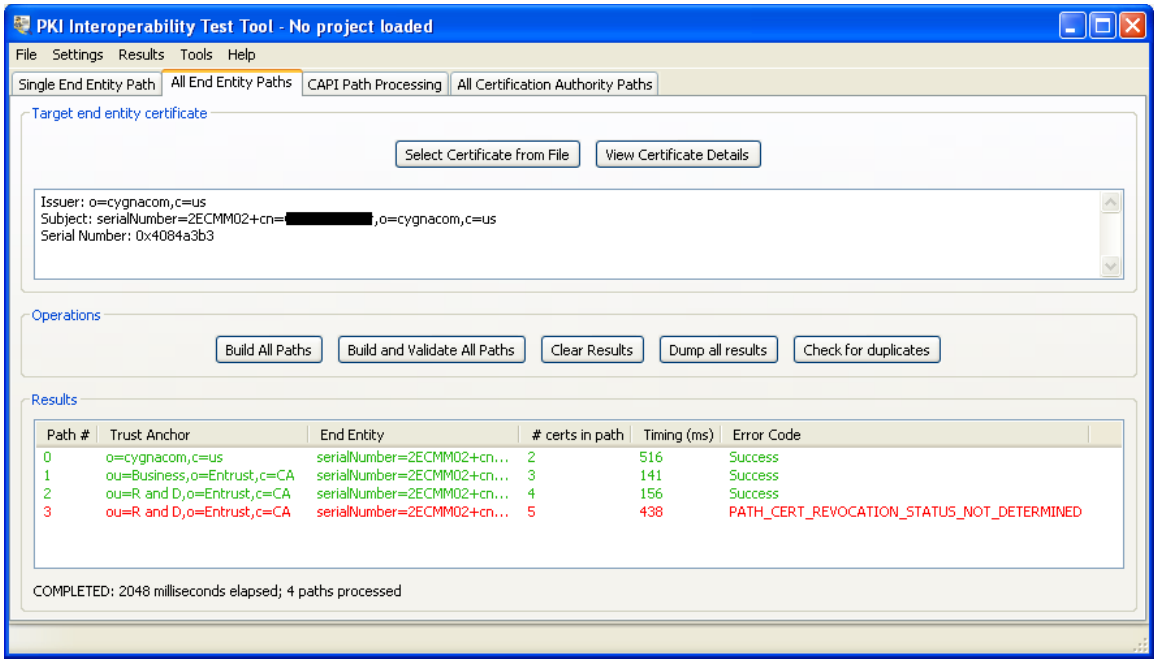
To clear the results of an operation, click the **Clear Results** button. Results are also cleared when **Build Path** or **Build and Validate Path** are clicked.

If the **Check URIs during path processing** option is enabled on the **Settings->PITT Settings** dialog, each URI in any authority information access, subject information access and CRL distribution point extension present in any certificate in the path will be accessed and checked for correctness relative to the certificate containing the URI. URI checking is wholly independent of certification path processing. Thus, artifacts may be retrieved multiple times during a single operation. This can result in path processing seeming non-responsive. The status indication will provide assurance that processing is still occurring and provide the elapsed time in milliseconds.

To stop a path processing operation prematurely, click the **Cancel** button. To stop a path processing operation immediately, click the **Cancel** button twice.

5.2 All End Entity Paths

The **All End Entity Paths** panel can be used to build all certification paths from a specified end entity certificate to an available trust anchor using PKIF. This panel is similar to the **Single End Entity Path** panel except that all possible certification paths are discovered and made available via a list box. The following diagram shows the **All End Entity Paths** panel with results following a **Build and Validate Paths** operation.


PKI Interoperability Test Tool - No project loaded
File Settings Results Tools Help
Single End Entity Path
All End Entity Paths
CAPI Path Processing
All Certification Authority Paths
Target end entity certificate
Select Certificate from File
View Certificate Details
Operations
Build All Paths
Build and Validate All Paths
Clear Results
Dump all results
Check for duplicates
Results

```
Issuer: o=cygnacom,c=us
Subject: serialNumber=2ECMM02+cn=[redacted],o=cygnacom,c=us
Serial Number: 0x4084a3b3
```

Path #	Trust Anchor	End Entity	# certs in path	Timing (ms)	Error Code
0	o=cygnacom,c=us	serialNumber=2ECMM02+cn...	2	516	Success
1	ou=Business,o=Entrust,c=CA	serialNumber=2ECMM02+cn...	3	141	Success
2	ou=R and D,o=Entrust,c=CA	serialNumber=2ECMM02+cn...	4	156	Success
3	ou=R and D,o=Entrust,c=CA	serialNumber=2ECMM02+cn...	5	438	PATH_CERT_REVOCATION_STATUS_NOT_DETERMINED

COMPLETED: 2048 milliseconds elapsed; 4 paths processed

Figure 18 All End Entity Paths Panel

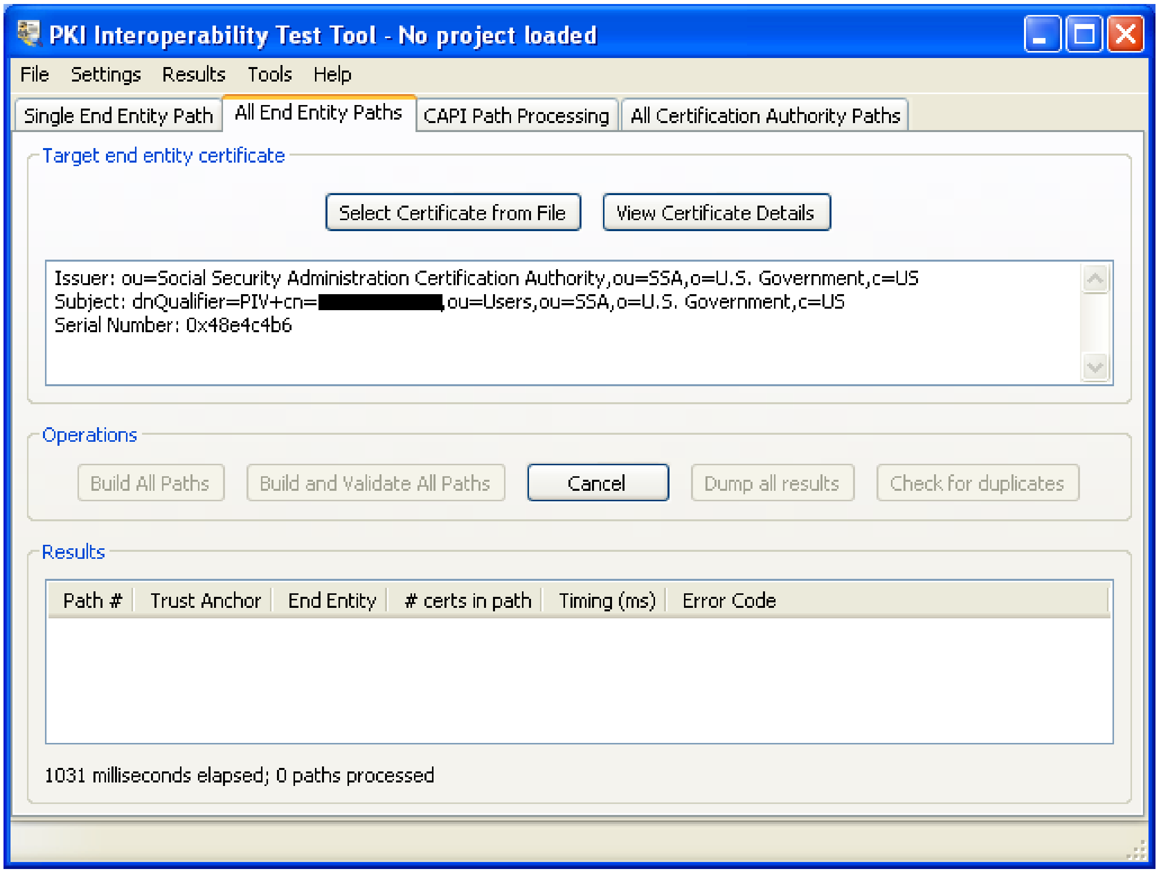
To specify the certificate to which a certification path should be constructed, click the **Select Certificate from File** button, browse to a file containing a DER encoded certificate then click **Open**. The issuer name, serial number and subject name will be displayed in the **Target end entity certificate** text box. To view the certificate using the Microsoft shell viewer, click the **View Details** button.

To build a certification path without performing certification path validation, click the **Build Path** button. The effective PKI settings will be used to discover a certification path, if possible. Each path will be writing to the **Results** text box, with a column showing the name of the trust anchor terminating the path, the name of the end entity, the number of certificates in the path (including the trust anchor and end entity) and the number of milliseconds required to build the path.

To build and validate a certification path, click the **Build and Validate Path** button. The effective PKI settings will be used to discover and validate a certification path, if possible. Each path will be writing to the **Results** text box, with a column showing the name of the trust anchor terminating the path, the name of the end entity, the number of certificates in the path (including the trust anchor and end entity) and the number of milliseconds required to build the path. Paths that were successfully validated will be colored green, paths that fail to validate will be colored red.

To clear the results of an operation, click the **Clear Results** button. Results are also cleared when **Build Path** or **Build and Validate Path** are clicked.

When the panel is busy, the **Build Path** and **Build and Validate Path** buttons are disabled and a **Cancel** button is displayed, as shown below.



Issuer: ou=Social Security Administration Certification Authority,ou=SSA,o=U.S. Government,c=US
Subject: dnQualifier=PIV+cn=[redacted],ou=Users,ou=SSA,o=U.S. Government,c=US
Serial Number: 0x48e4c4b6

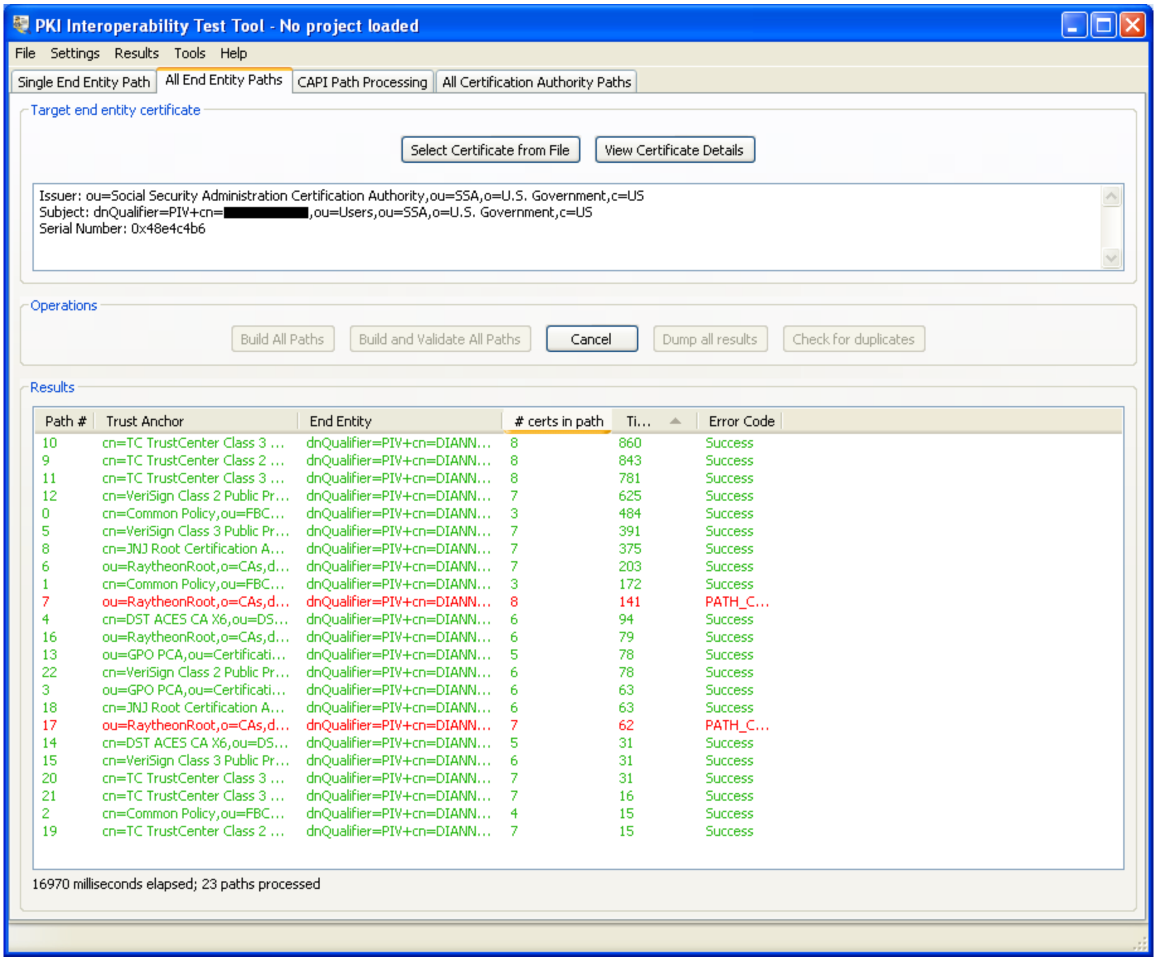
Path #	Trust Anchor	End Entity	# certs in path	Timing (ms)	Error Code

1031 milliseconds elapsed; 0 paths processed

Figure 19 All End Entity Paths panel (operation in progress)

To stop processing prematurely, click the **Cancel** button. To stop a path processing operation immediately, click the **Cancel** button twice.

The table can be sorted by clicking the header for the column containing the values that should be sorted. By default, the table is sorted using the **Path #** column. When a non-default column is used, an indication of sort direction is displayed adjacent to the column name. The following screen shot shows a table sorted on the **Timing (ms)** column from greatest value to least value.



Issuer: ou=Social Security Administration Certification Authority,ou=SSA,o=U.S. Government,c=US
Subject: dnQualifier=PIV+cn=[redacted],ou=Users,ou=SSA,o=U.S. Government,c=US
Serial Number: 0x48e4c4b6

Path #	Trust Anchor	End Entity	# certs in path	Ti...	Error Code
10	cn=TC TrustCenter Class 3 ...	dnQualifier=PIV+cn=DIANN...	8	860	Success
9	cn=TC TrustCenter Class 2 ...	dnQualifier=PIV+cn=DIANN...	8	843	Success
11	cn=TC TrustCenter Class 3 ...	dnQualifier=PIV+cn=DIANN...	8	781	Success
12	cn=VeriSign Class 2 Public Pr...	dnQualifier=PIV+cn=DIANN...	7	625	Success
0	cn=Common Policy,ou=FBC...	dnQualifier=PIV+cn=DIANN...	3	484	Success
5	cn=VeriSign Class 3 Public Pr...	dnQualifier=PIV+cn=DIANN...	7	391	Success
8	cn=JNJ Root Certification A...	dnQualifier=PIV+cn=DIANN...	7	375	Success
6	ou=RaytheonRoot,o=CAs,d...	dnQualifier=PIV+cn=DIANN...	7	203	Success
1	cn=Common Policy,ou=FBC...	dnQualifier=PIV+cn=DIANN...	3	172	Success
7	ou=RaytheonRoot,o=CAs,d...	dnQualifier=PIV+cn=DIANN...	8	141	PATH_C...
4	cn=DST ACES CA X6,ou=DS...	dnQualifier=PIV+cn=DIANN...	6	94	Success
16	ou=RaytheonRoot,o=CAs,d...	dnQualifier=PIV+cn=DIANN...	6	79	Success
13	ou=GPO PCA,ou=Certificati...	dnQualifier=PIV+cn=DIANN...	5	78	Success
22	cn=VeriSign Class 2 Public Pr...	dnQualifier=PIV+cn=DIANN...	6	78	Success
3	ou=GPO PCA,ou=Certificati...	dnQualifier=PIV+cn=DIANN...	6	63	Success
18	cn=JNJ Root Certification A...	dnQualifier=PIV+cn=DIANN...	6	63	Success
17	ou=RaytheonRoot,o=CAs,d...	dnQualifier=PIV+cn=DIANN...	7	62	PATH_C...
14	cn=DST ACES CA X6,ou=DS...	dnQualifier=PIV+cn=DIANN...	5	31	Success
15	cn=VeriSign Class 3 Public Pr...	dnQualifier=PIV+cn=DIANN...	6	31	Success
20	cn=TC TrustCenter Class 3 ...	dnQualifier=PIV+cn=DIANN...	7	31	Success
21	cn=TC TrustCenter Class 3 ...	dnQualifier=PIV+cn=DIANN...	7	16	Success
2	cn=Common Policy,ou=FBC...	dnQualifier=PIV+cn=DIANN...	4	15	Success
19	cn=TC TrustCenter Class 2 ...	dnQualifier=PIV+cn=DIANN...	7	15	Success

16970 milliseconds elapsed; 23 paths processed

Figure 20 Results table with non-default sorting

5.2.1 Viewing result details

Right-clicking an entry in the **Results** box will display the context menu shown below.

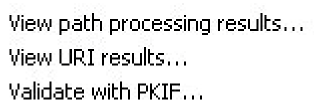


Figure 21 Results context menu

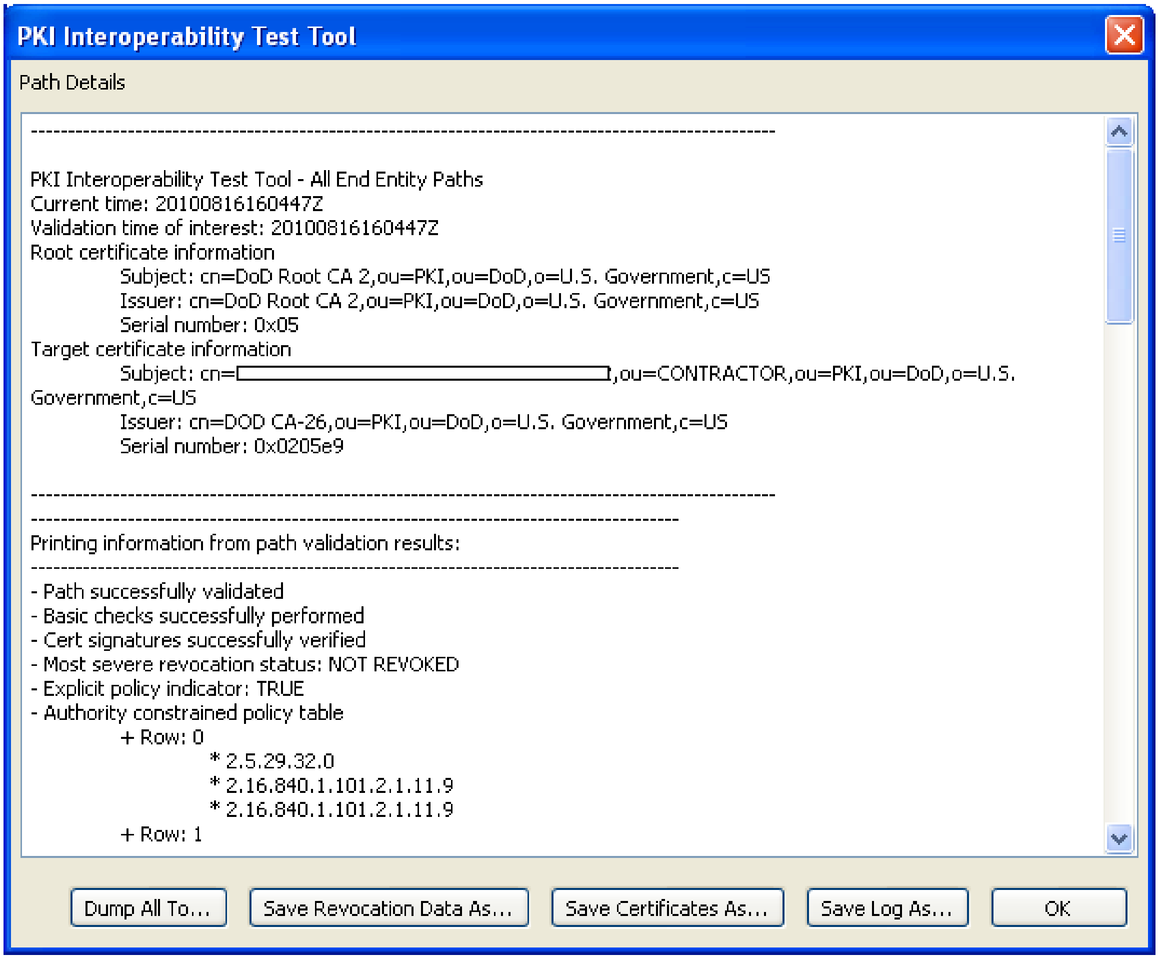
Clicking the **View path processing results…** option, or double clicking an entry, will display a dialog showing information about the path.

Clicking the **View URI results…** option will show the status of each URI from an AIA, SIA or CRL DP extension from each certificate in the certification path. The **View URI results…** option is only available when the **Check URIs during path processing** option is enabled, as described in the Edit PITT Settings section

Clicking the **Validate with PKIF…** option will cause the selected path to be validated using the PKIF library. A dialog will be displayed when the operation completes showing information about the path.

5.2.2 Certification Path Dump Dialog

When path processing results are viewed by double clicking a result on the **All End Entity Paths** or **All Certification Authority Paths** panels or by invoking the **View path processing results…** context menu option, a dialog similar to the one shown below is displayed.



```
---------------------------------------------------------------------------------------------------

PKI Interoperability Test Tool - All End Entity Paths
Current time: 20100816160447Z
Validation time of interest: 20100816160447Z
Root certificate information
            Subject: cn=DoD Root CA 2,ou=PKI,ou=DoD,o=U.S. Government,c=US
            Issuer: cn=DoD Root CA 2,ou=PKI,ou=DoD,o=U.S. Government,c=US
            Serial number: 0x05
Target certificate information
            Subject: cn=[redacted],ou=CONTRACTOR,ou=PKI,ou=DoD,o=U.S.
Government,c=US
            Issuer: cn=DOD CA-26,ou=PKI,ou=DoD,o=U.S. Government,c=US
            Serial number: 0x0205e9

---------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------
Printing information from path validation results:
--------------------------------------------------------------------------------------
- Path successfully validated
- Basic checks successfully performed
- Cert signatures successfully verified
- Most severe revocation status: NOT REVOKED
- Explicit policy indicator: TRUE
- Authority constrained policy table
            + Row: 0
                        * 2.5.29.32.0
                        * 2.16.840.1.101.2.1.11.9
                        * 2.16.840.1.101.2.1.11.9
            + Row: 1
```

Figure 22 Path Details Dialog

The **Path Details** area of the dialog provides a textual representation of certification path details. If the **Check URIs during path processing** option is enabled, the results of URI checking will also be displayed.

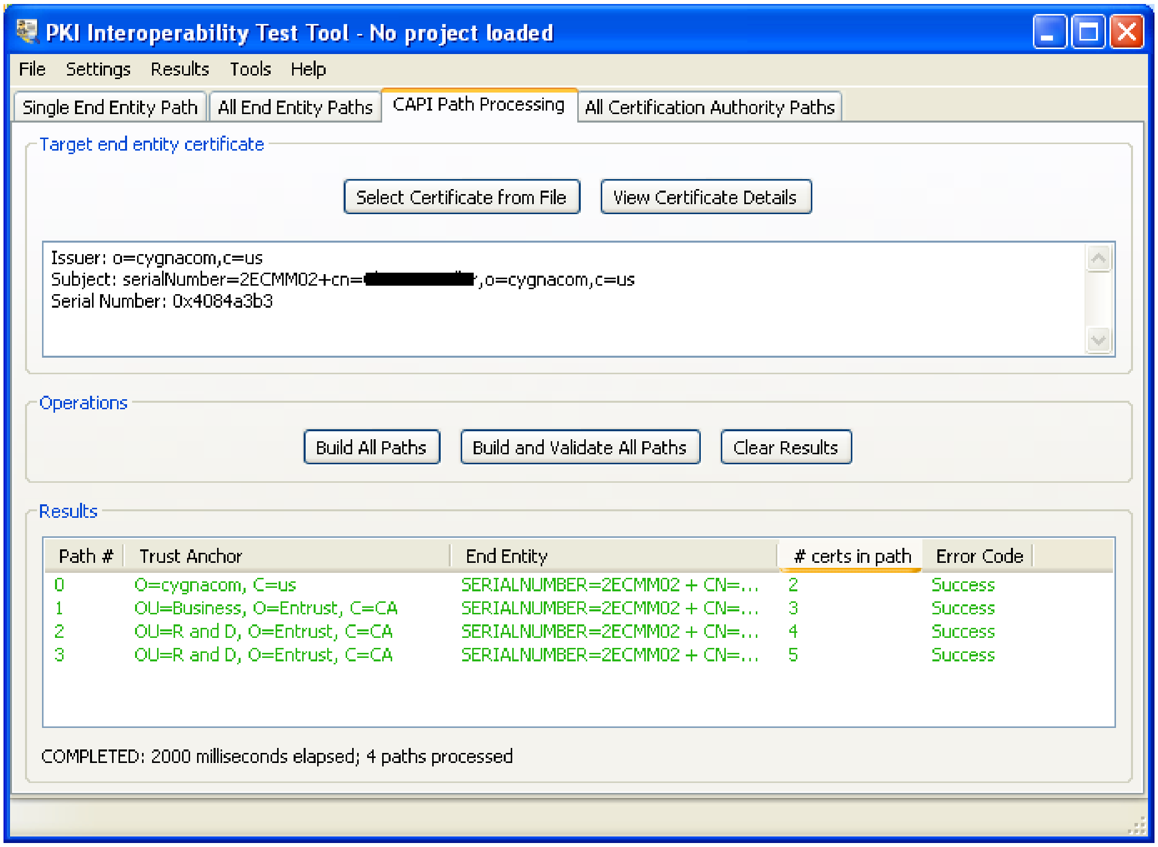
The **Dump All To…** button can be used to dump the certificates and revocation information that compose the certification path to a folder. File names are automatically generated and a file named PathManifest.txt is written to the folder to provide information about the artifacts written to the folder. The text log is written to the folder as PathLog.txt.

The **Save Revocation Data As…** and **Save Certificates As…** buttons can be used to dump revocation information or certificates only, respectively. File names are not automatically generated when using these options. Instead, the user is prompted to provide a name for each artifact.

The **Save Log As…** button can be used to save the text log to a file.

5.3 CAPI Path Processing

The **CAPI Path Processing** panel can be used to build all certification paths from a specified end entity certificate to an available trust anchor using CAPI. This panel is similar to the **All End Entity Paths** panel except that CAPI is used to perform certification path processing. Results made available via a list box. The following diagram shows the **CAPI Path Processing** panel with results following a **Build and Validate Paths** operation.


PKI Interoperability Test Tool - No project loaded
File
Settings
Results
Tools
Help
Single End Entity Path
All End Entity Paths
CAPI Path Processing
All Certification Authority Paths
Target end entity certificate
Select Certificate from File
View Certificate Details
Operations
Build All Paths
Build and Validate All Paths
Clear Results
Results

Issuer: o=cygnacom,c=us
Subject: serialNumber=2ECMM02+cn=[redacted],o=cygnacom,c=us
Serial Number: 0x4084a3b3

Path #	Trust Anchor	End Entity	# certs in path	Error Code
0	O=cygnacom, C=us	SERIALNUMBER=2ECMM02 + CN=…	2	Success
1	OU=Business, O=Entrust, C=CA	SERIALNUMBER=2ECMM02 + CN=…	3	Success
2	OU=R and D, O=Entrust, C=CA	SERIALNUMBER=2ECMM02 + CN=…	4	Success
3	OU=R and D, O=Entrust, C=CA	SERIALNUMBER=2ECMM02 + CN=…	5	Success

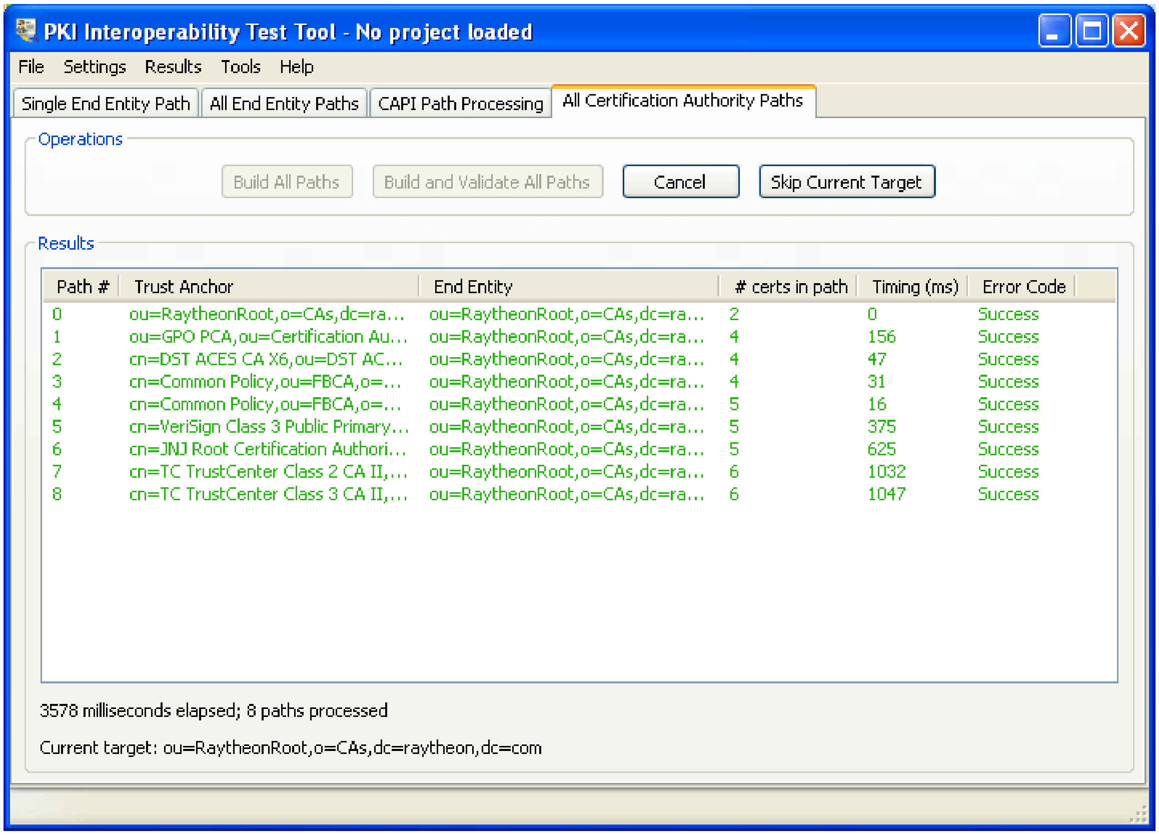
COMPLETED: 2000 milliseconds elapsed; 4 paths processed

Figure 23 CAPI Path Processing panel

The behavior of the **CAPI Path Processing** panel differs from the other panels in that CAPI returns all paths at the same time.

5.4 All Certification Authority Paths

The **All Certification Authority Paths** panel can be used to build all certification paths from the available trust anchors to available certification authority certificates using PKIF. This panel is similar to the **All End Entity Paths** panel except that no target certificate is specified. Instead, an attempt is made to build all possible certification paths from all available CA certificates. The results are made available via a list box. The following diagram shows the **All Certification Authority Paths** panel during a **Build and Validate Paths** operation.



Path #	Trust Anchor	End Entity	# certs in path	Timing (ms)	Error Code
0	ou=RaytheonRoot,o=CAs,dc=ra...	ou=RaytheonRoot,o=CAs,dc=ra...	2	0	Success
1	ou=GPO PCA,ou=Certification Au...	ou=RaytheonRoot,o=CAs,dc=ra...	4	156	Success
2	cn=DST ACES CA X6,ou=DST AC...	ou=RaytheonRoot,o=CAs,dc=ra...	4	47	Success
3	cn=Common Policy,ou=FBCA,o=...	ou=RaytheonRoot,o=CAs,dc=ra...	4	31	Success
4	cn=Common Policy,ou=FBCA,o=...	ou=RaytheonRoot,o=CAs,dc=ra...	5	16	Success
5	cn=VeriSign Class 3 Public Primary...	ou=RaytheonRoot,o=CAs,dc=ra...	5	375	Success
6	cn=JNJ Root Certification Authori...	ou=RaytheonRoot,o=CAs,dc=ra...	5	625	Success
7	cn=TC TrustCenter Class 2 CA II,...	ou=RaytheonRoot,o=CAs,dc=ra...	6	1032	Success
8	cn=TC TrustCenter Class 3 CA II,...	ou=RaytheonRoot,o=CAs,dc=ra...	6	1047	Success

3578 milliseconds elapsed; 8 paths processed

Current target: ou=RaytheonRoot,o=CAs,dc=raytheon,dc=com

Figure 24 All Certification Authority Paths panel (in progress)

To stop processing prematurely, click the **Cancel** button. To stop a path processing operation immediately, click the **Cancel** button twice. To skip the certification authority currently being processed, click the **Skip Current Target** button.

Appendix A – Shortcut Keys

Shortcut keys	Description	Equivalent menu item
Ctrl + N	Opens a new project.	File->New Project
Ctrl + O	Opens an existing project.	File->Open Project
Ctrl + C	Closes current project.	File->Close Project
Ctrl + S	Saves current project.	File->Save Project
Ctrl + Shift + S	Saves current project to a different location.	File->Save Project As
Shift + D	Launches dialog box to edit default PKI settings.	Settings->Edit Default PKI Settings
Shift + P	Launches dialog box to edit project PKI settings.	Settings->Edit Project PKI Settings
Shift + S	Launches dialog box to edit PITT settings.	Settings->Edit PITT Settings
Ctrl + G	Generates a summary report.	Project->Generate Summary Report
Ctrl + R	Clears all results.	Project->Clear All Results
Ctrl + U	Launch dialog to enable checking URIs in a certificate.	Tools->Check URIs in certificate