Department of Defense (DoD) Public Key Infrastructure (PKI) Combined Communications Electronics Board (CCEB) Partner PKI Interoperability Test Plan

13 June 2011

Version 1.0

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
10/15/2012	1.0	Final.
05/15/2011	1.0b	Initial draft.

Contents

Introduction

This document provides guidance and steps necessary to conduct Public Key Infrastructure (PKI) interoperability testing of Combined Communications Electronics Board (CCEB) partner PKIs with which the Department of Defense (DoD) desires to interoperate. This document focuses on usage of both the direct trust model and the cross certification trust model as the means of achieving PKI interoperability. As a result of CCEB and DoD secure information sharing initiatives, DoD and its partners are required to establish and maintain secure PKI interoperability. DoD Instruction 8520.02[1] is the governing policy document for DoD PKI and DoD relying party responsibilities. The CCEB draft paper "CCEB Publication 1010 – PKI Cross-Certification between CCEB Nations" (Pub1010)[2] lays out the requirements for cross-certification and interoperability among CCEB partners.

Scope of Test Plan

This test plan primarily utilizes the PKI Interoperability Test Tool (PITT) which is built on PKI Framework (PKIF) and Crypto++ and has proven very useful in assessing PKIX RFC 5280 compliance and in diagnosing infrastructure problems. This document details the set of preliminary actions and test procedures required to utilize PITT to assess a partner PKI for standards compliance.

Purpose of Testing

The purpose of this testing is to analyze and validate the PKIs of CCEB partners so that standards compliance is ensured and basic PKI services perform as expected across multiple international domains and repositories.

[1] DoD 8520.02 can be found at http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf.
[2] PUB1010 can be found at TBD.

Testing Overview

Interoperability testing will validate the use of end entity certificates issued by intended partner PKIs on DoD systems. Testing will be conducted by the Joint Interoperability Test Command (JITC). JITC testers will use the PKI Interoperability Test Tool (PITT) to inspect and validate all the required attributes/elements of the intended partner PKI.

Objectives

The primary objectives of this testing are listed as follows:

A. Trust partner root certificate(s) either directly or through cross-certification.

B. Discover and validate all possible trust paths from the end entity certificates to the root.

C. Check the availability and correctness of all Universal Resource Indicators (URIs) in certificate extensions.

D. Ensure revocation checking mechanisms are working properly.

To accomplish the above objectives two different interoperability types will be tested:

1. Direct trust interoperability, in which the intended partner PKI's root CA certificate is explicitly trusted by the DoD relying party, and used to validate end entity certificates from the partner PKI.

2. Cross-certificate trust interoperability, in which a DoD CA certificate cross-certified with an intended partner PKI CA is trusted by the DoD relying party, and used to validate end entity certificates from the partner PKI.

A third type, transitive trust interoperability, in which DoD CA certificate cross-certified with an intended partner PKI CA is trusted by the DoD relying party, and used to validate end entity certificates from a third party PKI that is cross-certified with the partner PKI, is provided as an optional test in Appendix A.

About PITT

The PKI Interoperability Test Tool (PITT) allows for the inspection and troubleshooting of certificate path processing for a given PKI using both PKIF and Microsoft CAPI. PITT's path processing element is based on the RFC 5280 path processing algorithm, described in detail in *Section 6* of RFC 5280 which can be found at: http://www.ietf.org/rfc/rfc5280.txt.

Preliminary Actions

Before testing begins, testers must gather all required materials and set up the test systems. The PKI belonging to the testers' organization, in this case the DoD PKI, is referred to as the Host PKI, and the external PKI to be tested is referred to as the Partner PKI. For the purpose of testing transitive trust, the third party PKI cross-certified with the Partner PKI but not the Host PKI will be referred to as the Third Party PKI.

Obtain Required Materials

The following materials should be obtained from the Host PKI:

- Self-signed Root Certificate Authority (CA) certificate which will be used as the Host PKI's cross-certificate trust anchor. For DoD PKI, this will be US CCEB JITC Interoperability Root CA 1

The following materials should be obtained from the Partner PKI:

- Self-signed Root CA certificate
- Intermediate/Subordinate CA certificate(s) associated with end entity certificates
- A valid set of ALL the public end entity certificates to be evaluated. Evaluated certificates may include software or hardware certificates (i.e. ID/authentication, card-authentication, signature, encryption, server authentication, and any other applicable certificates)
- At least one revoked end entity certificate (revoked certificates should be from the same issuing CA as the valid set of certificates)
- Optionally, to test transitive trust, the Partner PKI should provide a set of valid end entity certificates from a Third Party PKI that are known to be accepted by the Partner PKI.

These materials should be obtained via a secure and trustworthy method. The purpose of each certificate and its revocation status should be clearly indicated in the filename. Example: r*oot_CA.cer, intermediate_CA.cer, valid_signature.cer, revoked_authentication.cer.*

Test System Requirements

The following are operating system and software requirements to be used for testing:

- Virtual machines (VM) are to be used for all testing. This allows the use of snapshots to restore to a default state to avoid contamination of results. The recommended application for loading the VMs is the freely available VMware Server 2.0[3].
- To account for operating system differences, three VMs should be built, running the 64-bit versions of Windows XP, Windows Vista, and Windows 7 respectively. The operating systems should be installed with default options and configured according to the requirements of the test network environment.
- Each VM should have the latest version of PITT installed.
- Each VM should have Wireshark 1.4[4] or later installed.
- Each VM should have Tumbleweed Desktop Validator 4.10 or later installed and configured as the default CAPI revocation provider.
- For each VM, verify that Automatic Root Certificates Update is turned off :
    - Click **Start**, and **Run**. Type "**mmc"**. Add the **Group Policy Object** snap-in for the local computer.
    - Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Internet Communication Management**, and then click **Internet Communication settings**.
    - In the details pane, double-click **Turn off Automatic Root Certificates Update**, and then click **Enabled**.
    - Open a command window and type "`gpupdate /force`".
- For the Windows XP VM only, verify that Name Constraints Registry Fix has been applied:
    - Click **Start**, and **Run**. Type "**regedit"** to edit the registry.
    - Navigate to the following registry key and add the following value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificate
s\root\ProtectedRoots], "Flags"=dword:0x20
```

[3] Download from http://downloads.vmware.com/d/info/datacenter_downloads/vmware_server/2_0.
[4] Download from http://www.wireshark.org/download.html.

Testing Direct Trust Interoperability

The Direct Trust model requires the Host PKI to directly trust the Partner PKI's trust anchor (self-signed Root CA certificate). In a production environment, the DoD relying party will be required to trust the Partner PKI's root certificate and have access to the revocation information of the Partner PKI in order to determine the validity of the Partner PKI certificates.

Direct Trust Test Plan

JITC testers will use the latest version of PITT to test each end entity certificate supplied by the Partner PKI. For each certificate two test cases will be used, each utilizing a different path processing engine and trusted certificate store. These are:

- Path processing using Crypto API (CAPI) engine and the Windows Certificate Store.
- Path processing using PKI Framework (PKIF) engine and the PITT Simple Store.

In each test case the trusted certificate store will contain the Partner PKI's root CA certificate as the trust anchor, as well as any necessary intermediate CA certificates. The path processing engine will attempt to build and validate all possible trust paths from the end entity certificate to the trust anchor. The resulting log will be examined for errors and other information. The results obtained using CAPI will indicate each type of error encountered during path processing with an error code. The results obtained using PKIF will provide information in the following areas:

- Overall Validation Check: provides an overview of the trust path's validity. Critical failures such as revoked certificate, policy constraint or name constraint violation will be shown here.
- Certificate Path Check: provides detailed information about each certificate in the trust path and its revocation checking method and status. Failure in revocation status checking will be shown here.
- Universal Resource Indicator (URI) Check: provides information about the URIs contained in each certificate, their correctness and accessibility.

Findings from the test results will be classified according to their severity:

- Critical: a major error that prevents successful path validation, such as revoked certificate, name or policy constraints violation, or inaccessible revocation information.
- Non-Critical: a minor irregularity or non-compliance that does not prevent successful path validation in most standard path processing implementations, such as the presence of a self-signed certificate in an URI.

The Direct Trust Test is successful if for each end entity certificate tested, both the PKIF and the CAPI test cases returned at least one valid trust path and that trust path contained no critical finding. All findings, critical or non-critical, should be recorded and forwarded to the Partner PKI.

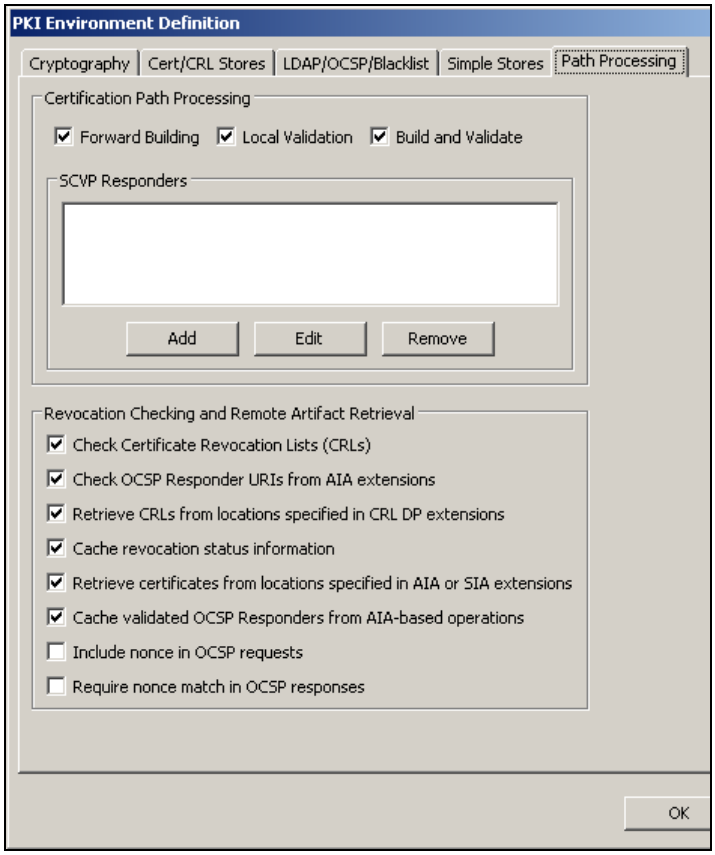
Direct Trust Test Procedures

The following are the testing procedures for each test case:

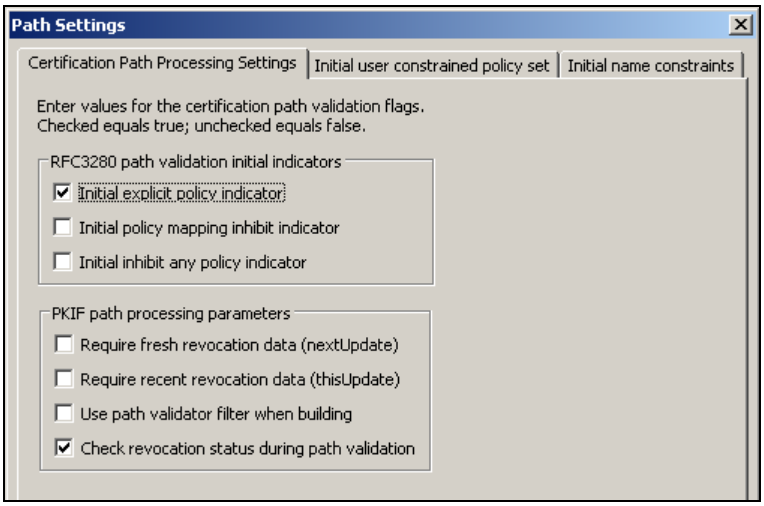
NOTE: These steps should be repeated on all 3 operating systems (XP, Vista, and Windows 7) for each end-entity certificate that was obtained in the Preliminary Actions including the revoked certificate.

Preparation of Default VM Snapshot

1. Launch PITT. Verify that the title bar displays "No project loaded." If a project file is loaded, in the menu bar select **File → Close Project** to unload it.
2. In the menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
3. Select the **LDAP/OCSP/Blacklist** tab and verify that all entries are blank.
4. Select the **Path Processing Tab** and verify that the options in the screenshot below are set:



5. Click **OK** to close the **PKI Environment Definition** window and return to the **Default Settings** window. Click **Define Path Settings.** In the **Path Settings** window verify that the following options under the **Certification Path Processing Settings** tab are set:



6. Verify that the **Initial User Constrained Policy Set** tab only contains one acceptable certificate policy "2.5.29.32.0".

7. Verify that the **Initial Name Constraints** tab is blank. Click **OK** to close the **Path Settings** window and click **Close** to go back to the PITT main window.

8. **Take a snapshot of the VM at a clean state before proceeding further.** In VMware Server 2.0 this is done by clicking **Take Snapshot** in the **Commands** panel. At this point no certificate has been added to the trusted certificate store and all default options for PITT have been set. **Testers will revert back to this snapshot at the start of each test case.**

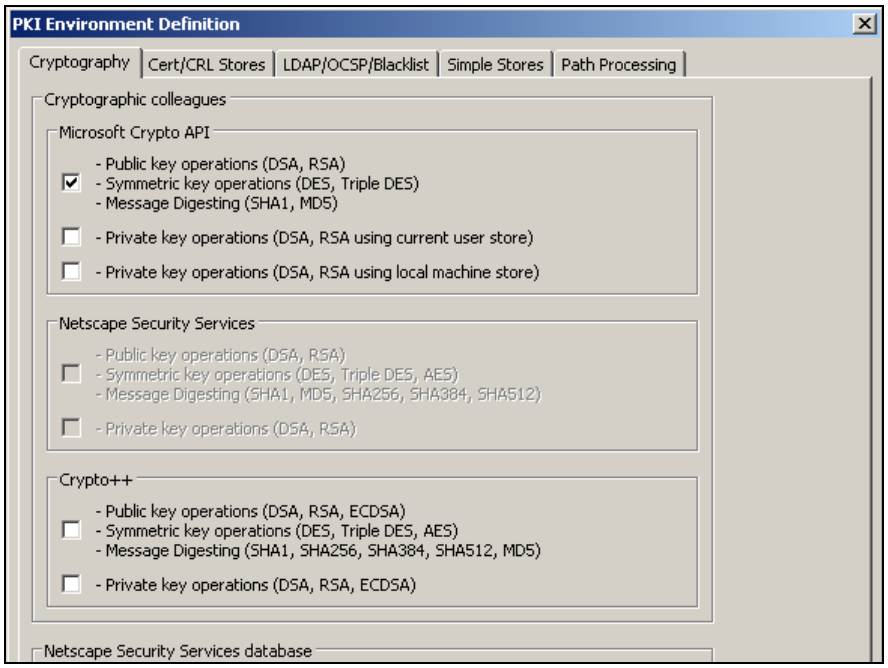
Direct Trust Test Case #1: CAPI Path Processing

1. Revert to the clean snapshot of the VM by choosing **Revert to Snapshot** in VMware Server 2.0.

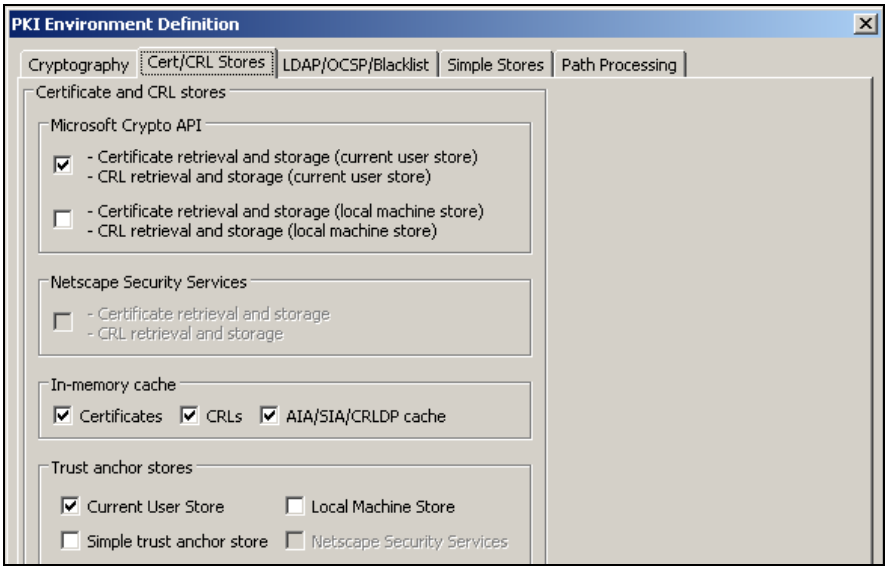
2. Update the Windows Certificate Store with the root and intermediate CA certificates of the Partner PKI. By default the **Current User** store will be used. Root CA certificates should be placed under **Trusted Root Certification Authorities**, and intermediate CA certificates should be placed under **Intermediate Certification Authorities**.

3. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.

4. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:

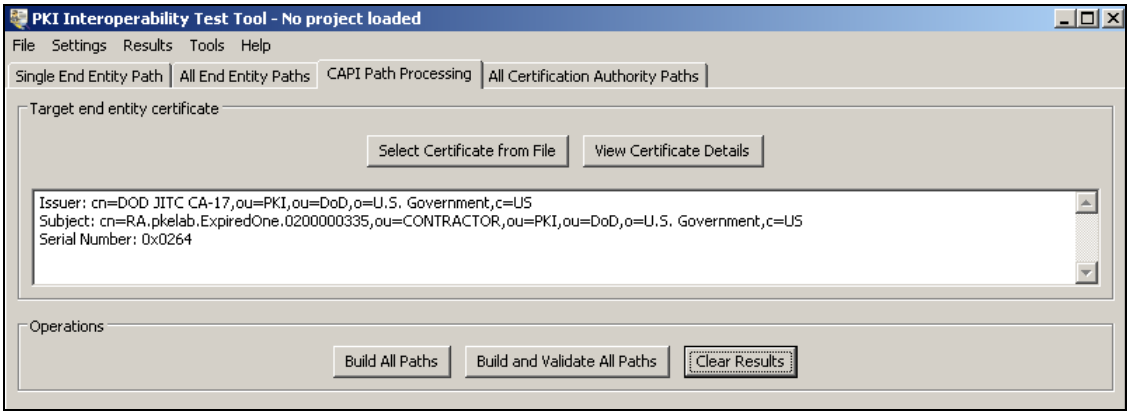


5. Select the **Cert/CRL Stores** tab and verify that the following options are set:



6. Click **OK** to close the **PKI Environment Definition** window and then click **Close** to go back to the PITT main window.

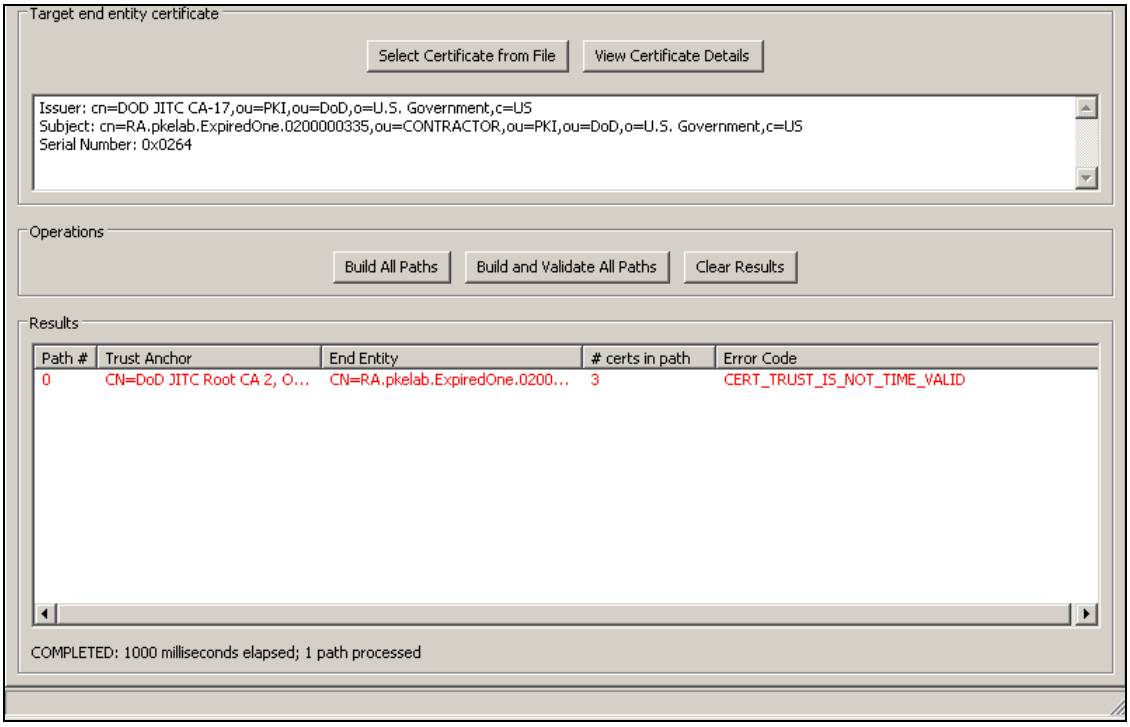
7. From the PITT main window, select the **CAPI Path Processing** tab. Click **Select Certificate from File** and load the end entity certificate to be tested.



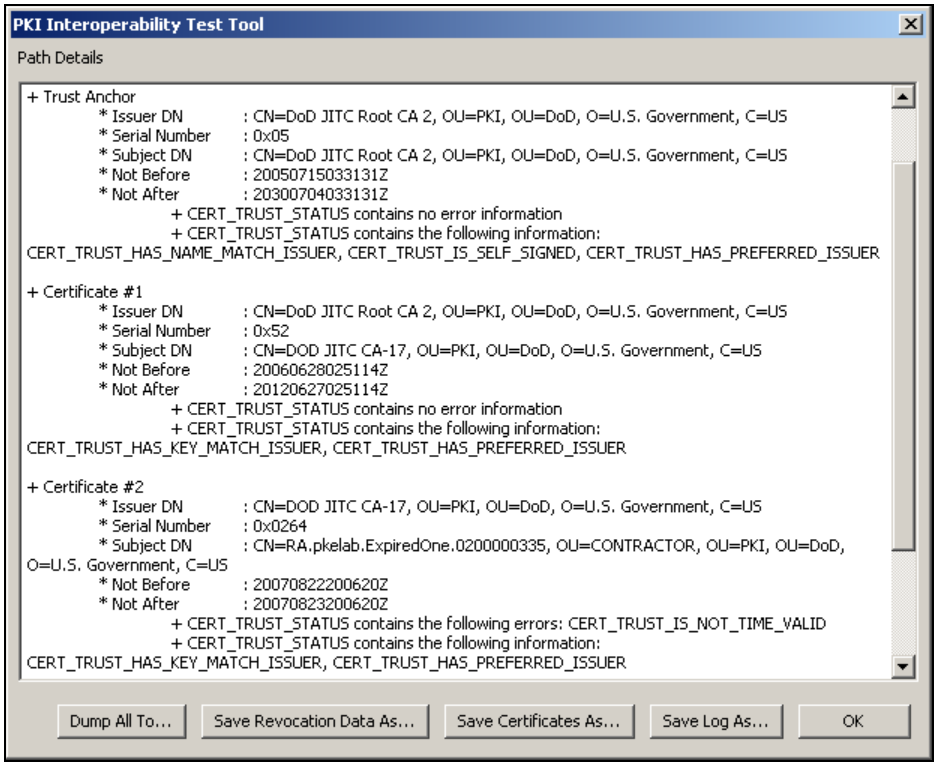
8. Once the certificate is loaded start an interface capture in **Wireshark.**

9. Return to PITT and in the **CAPI Path Processing** tab click **Build and Validate All Paths**.

10. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.



11. For each path listed, right-click on it and select **View Path Processing Results.**



12. Record the structure of the trust path in **Section 1-A** of the **Direct Trust CAPI Path Processing Results** table. List the type, certificate name (Common Name), and serial number of each certificate in the path, from the trust anchor to the end entity certificate. Example:

Type	**Certificate Name**	**Serial Number**
Trust Anchor	DoD JITC Root CA 2	0x05
Certificate 1	DoD JITC CA-17	0x52
Certificate 2	RA.pkelab.ExpiredOne	0x0264

13. The top of the results log will display "*Chain contains no error*" if the path is valid, or "*Chain contains the following errors*" followed by the error code[5] if the path is invalid. Record any chain error code in **Section 1-B** as a critical finding, or "*pass*" if no error is shown.

[5] Full list of *CERT_TRUST_STATUS* error codes and their explanation can be found at http://msdn.microsoft.com/en-us/library/aa377590%28VS.85%29.aspx.

14. For each certificate listed in the results logs, if no error was encountered the line *"CERT_TRUST_STATUS contains no error information"* will be shown. Otherwise the line *"CERT_TRUST_STATUS contains the following errors"* will be shown, followed by error code(s). Record any certificate error code in **Section 1-C** as a critical finding, or *"pass"* if no error is shown. Example:

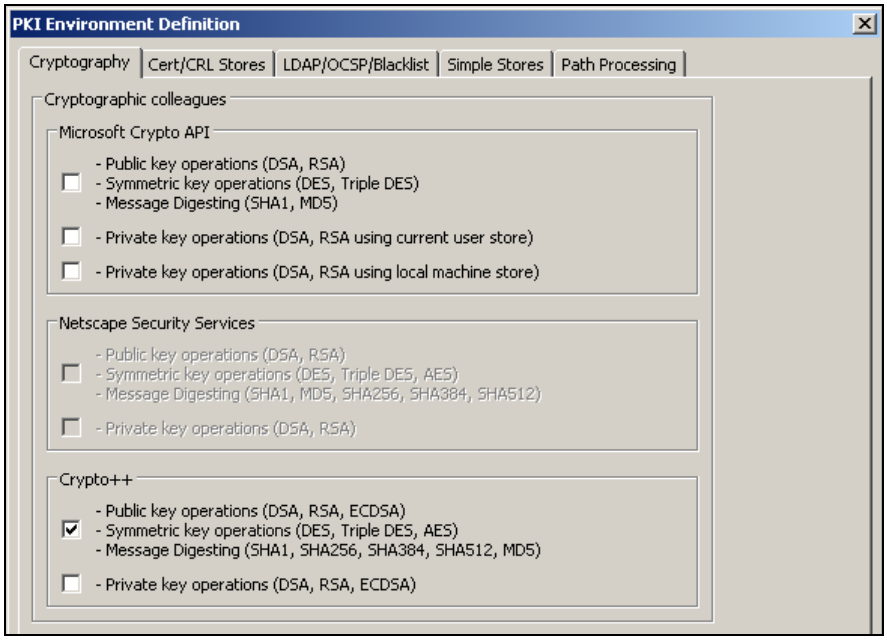
Certificate Name	Error Code(s)	Severity
DoD JITC Root CA 2		Pass
DoD JITC CA-17		Pass
RA.pkelab.ExpiredOne	CERT_TRUST_IS_NOT_TIME_VALID	Critical

NOTE: For the revoked end entity certificate, error code *"CERT_TRUST_IS_REVOKED"* should be treated as *"pass"*.

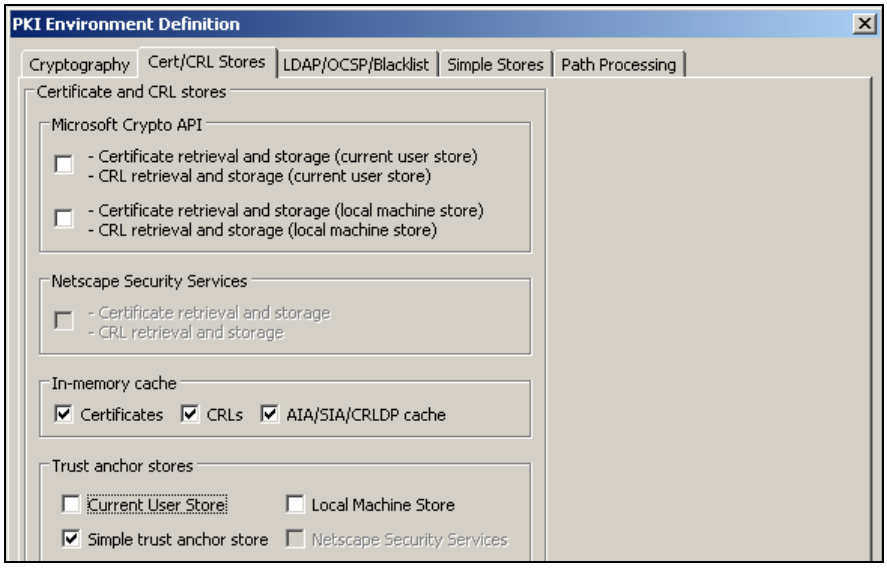
15. Click **Dump All To…** to save a copy of the results.

Direct Trust Test Case #2: PKIF Path Processing

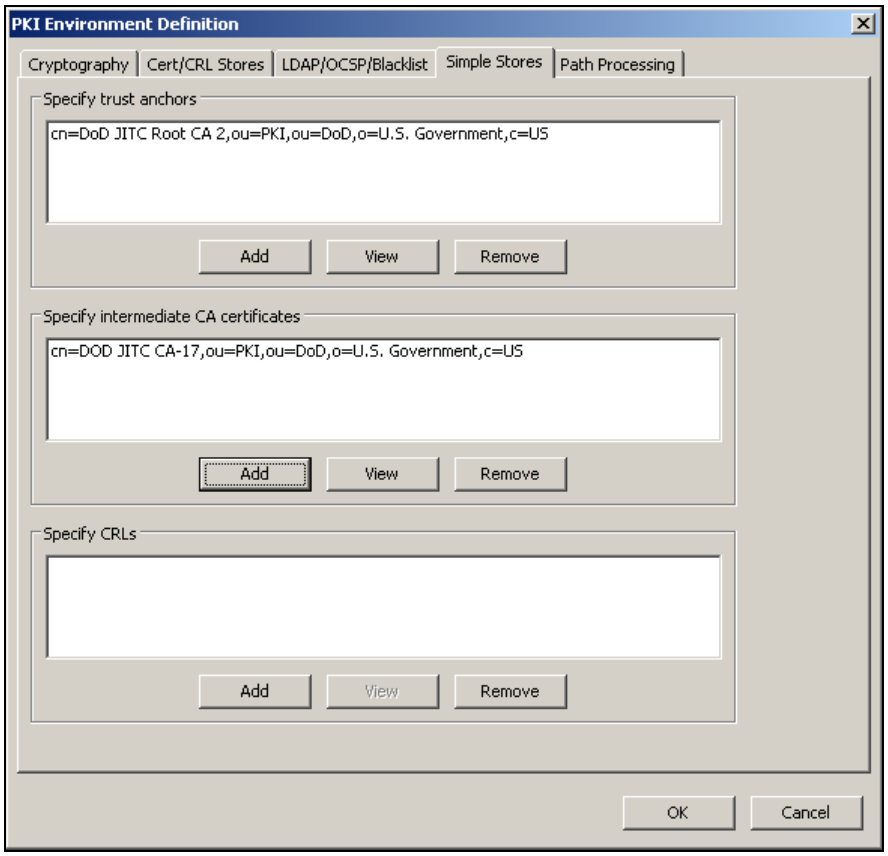
1. Revert to the clean snapshot of the VM.
2. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
3. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:



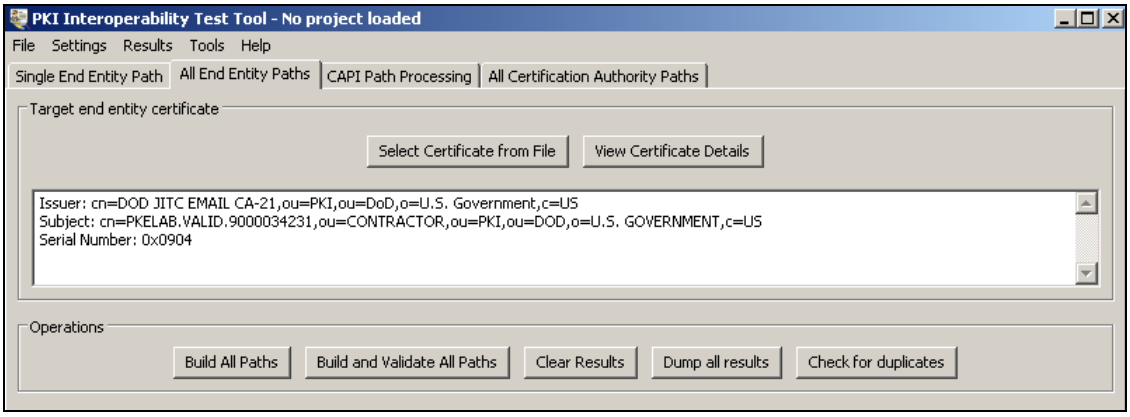
4. Select the **Cert/CRL Stores** tab and verify that the following options are set:



5. Select the **Simple Stores** tab and use the **Add** button to load the Partner PKI's root CA certificate into the **Specify trust anchor** panel and intermediate CA certificate(s) into the **Specify intermediate CA certificates** panel.



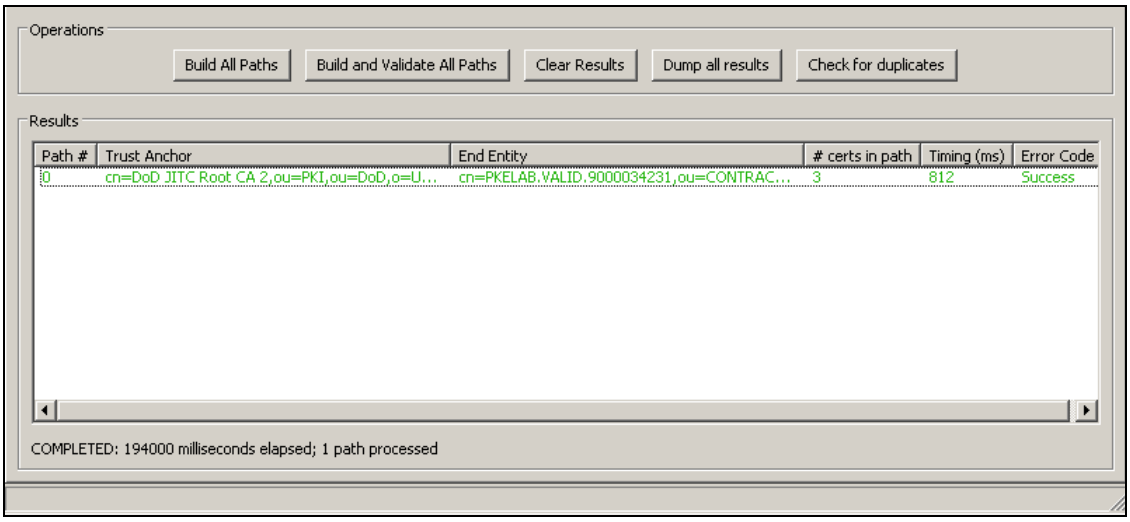
6. From the PITT main window, select the **All End Entity Paths** tab. Click **Select Certificate from File** and load the end entity certificate to be tested.



7. Once the certificate is loaded start an interface capture in **Wireshark.**

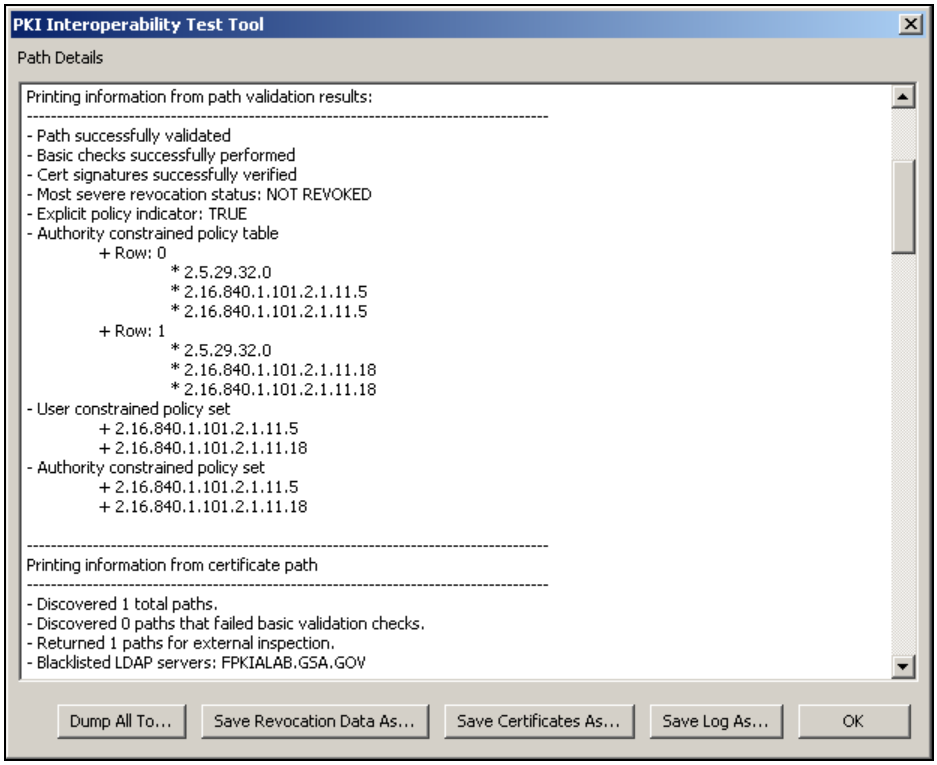
8. Return to PITT and in the **All End Entity Paths** tab click **Build and Validate All Paths**.

9. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.



10. For each path listed, right-click on it and select **View Path Processing Results.**

    Sample output:



11. Record the structure of the trust path in **Section 2-A** of the **Direct Trust PKIF Path Processing Results** table. List the type, Common Name (CN), and serial number of each certificate in the path, from the trust anchor to the end entity certificate. Example:

Type	Common Name	Serial Number
Trust Anchor	DoD JITC Root CA 2	0x05
Certificate 1	DoD JITC CA-17	0x52
Certificate 2	RA.pkelab.ExpiredOne	0x0264

12. **Overall Validation Check** – If the path is valid, *"NOT REVOKED"* will be shown under *"Most severe revocation status"*. Otherwise an error condition will be shown. Record the error condition in **Section 2-B** as a critical finding, or *"pass"* if no error.

    NOTE: For the revoked end entity certificate, a revoked status should be treated as *"pass"*.

13. **Certificate Path Check –** Under "*Printing information from certificate path*", for each certificate, record the status of the following checks:

    a. Record the *"diagnostic code"*. This will be *"0 : Success"* if all checks were successful, which should be classified as *"pass"*. If any check has failed, an error code will be displayed. Record the error code in **Section 2-C** as a critical finding.

       NOTE: For the revoked end entity certificate a diagnostic code of *"PATH_VALIDITY_PERIOD_VIOLATION"* should be treated as *"pass"*.

    b. For each *"Revocation source"* listed, record the *"Revocation source type"* (1 = CRL, 2 = OCSP) and the *"Revocation source error code"*, which will be *"0 : Success"* if a revocation source has no error. Record this as *"pass"* in **Section 2-C**. If any other error code is displayed, record it as a critical finding.

    Example:

Certificate Name:	DoD JITC Root CA 2			**Severity**
Diagnostic Code:	0 : Success			Pass
Certificate Name:	DoD JITC CA-17			
Diagnostic Code:	0 : Success			Pass
Revocation Type:	OCSP	**Revocation Source Error Code:**	0 : Success	Pass
Certificate Name:	RA.pkelab.ExpiredOne			
Diagnostic Code:	PATH_VALIDITY_PERIOD_VIOLATION			Critical
Revocation Type:	OCSP	**Revocation Source Error Code:**	OCSP_PATH_FAILED	Critical
Revocation Type:	CRL	**Revocation Source Error Code:**	0 : Success	Pass

14. **URI Check –** Each certificate will have a "*URI results*" section listing all URIs found in the certificate and their status. Record the certificate extension the URI belongs to, its access protocol, and the URI's status, which can be one of the following:

    a. "*URI_CORRECT_DATA*" indicates a correct and accessible URI. Record this as "*pass*" in **Section 2-D**.

    b. "*URI_INCORRECT_DATA*" indicates that the URI contains incorrect information or lacks required information. Record this as a critical finding in **Section 2-D**.

    c. "*URI_NOT_AVAILABLE*" indicates an inaccessible URI. Record this as a critical finding in **Section 2-D**.

    d. "*URI_WARNING*" indicates the presence of a self-signed certificate in the URI. Record this as a non-critical finding in **Section 2-D**.

    Example:

Certificate Name:	DoD JITC Root CA 2					**Severity**
Extension:	SIA	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Extension:	SIA	**Protocol:**	LDAP	**Status:**	URI_NOT_AVAILABLE	Critical
Certificate Name:	DoD JITC CA-17					
Extension:	AIA	**Protocol:**	HTTP	**Status:**	URI_WARNING	Non-Critical
Extension:	SIA	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Extension:	CDP	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Certificate Name:	RA.pkelab.ExpiredOne					
Extension:	AIA	**Protocol:**	LDAP	**Status:**	URI_WARNING	Non-Critical
Extension:	AIA	**Protocol:**	HTTP	**Status:**	URI_INCORRECT_DATA	Critical
Extension:	CDP	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass

15. Click **Dump All To…** to save a copy of the results.

Direct Trust Test Results

Summarize the results in the following table. Use one set of tables for each trust path.

Direct Trust CAPI Path Processing Results

1-A. Trust Path Information (CAPI Test Procedure #12)		
Type	**Common Name**	**Serial Number**

1-B. Chain Error Code (CAPI Test Procedure #13)	**Severity (Critical, Non-Critical, or Pass)**

1-C. Certificate Error Code (CAPI Test Procedure #14)		
Certificate Name	**Error Code(s)**	**Severity**
Number of Critical Findings:		
Number of Non-Critical Findings:		

Direct Trust PKIF Path Processing Results

2-A. Trust Path Information (PKIF Test Procedure #11)		
Type	**Common Name**	**Serial Number**

2-B. Overall Validation Check (PKIF Test Procedure #12)	**Severity (Critical, Non-Critical, or Pass)**

2-C. Certificate Path Check (PKIF Test Procedure #13)				
Certificate Name:				**Severity**
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		

Direct Trust PKIF Path Processing Results (continued)

2-D. URI Check (PKIF Test Procedure #14)						
Certificate Name:						**Severity**
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
					Number of Critical Findings:	
					Number of Non-Critical Findings:	

Testing Cross-Certificate Trust Interoperability

In the cross-certificate trust model, a CA issues a certificate to another CA that it trusts. A set of cross-certificates issued in both directions provides bi-directional trust. Trust can also be one-way if only one CA signs a certificate for the other CA. In a production environment, the DoD relying party will trust the US DoD CCEB Interoperability Root CA 1 self-signed certificate which allows for cross-certificate trust with the Partner PKI through bilateral cross-certificates.

Cross-Certificate Trust Test Plan

JITC testers will use the latest version of PITT to test each end entity certificate supplied by the Partner PKI. For each certificate two test cases will be used, each utilizing a different path processing engine and trusted certificate store. These are:

- Path processing using Crypto API (CAPI) engine and the Windows Certificate Store.
- Path processing using PKI Framework (PKIF) engine and the PITT Simple Store.

In each test case the trusted certificate store will contain the self-signed **US DoD CCEB [JITC] Interoperability Root CA 1 (CCEB IRCA1)** certificate as the trust anchor. The path processing engine will attempt to build and validate all possible trust paths from the end entity certificate to the trust anchor. The resulting log will be examined for errors and other information. The results obtained using CAPI will indicate each type of error encountered during path processing with an error code. The results obtained using PKIF will provide information in the following areas:

- Overall Validation Check: provides an overview of the trust path's validity. Critical failures such as revoked certificate, policy constraint or name constraint violation will be shown here.
- Certificate Path Check: provides detailed information about each certificate in the trust path and its revocation checking method and status. Failure in revocation status checking will be shown here.
- Universal Resource Indicator (URI) Check: provides information about the URIs contained in each certificate, their correctness and accessibility.

Findings from the test results will be classified according to their severity:

- Critical: a major error that prevents successful path validation, such as revoked certificate, name or policy constraints violation, or inaccessible revocation information.

- Non-Critical: a minor irregularity or non-compliance that does not prevent successful path validation in most standard path processing implementations, such as the presence of a self-signed certificate in an URI.

The Cross-Certificate Trust Test is successful if for each end entity certificate tested, both the PKIF and the CAPI test cases returned at least one valid trust path and that trust path contained no critical finding. All findings, critical or non-critical, should be recorded and forwarded to the Partner PKI.

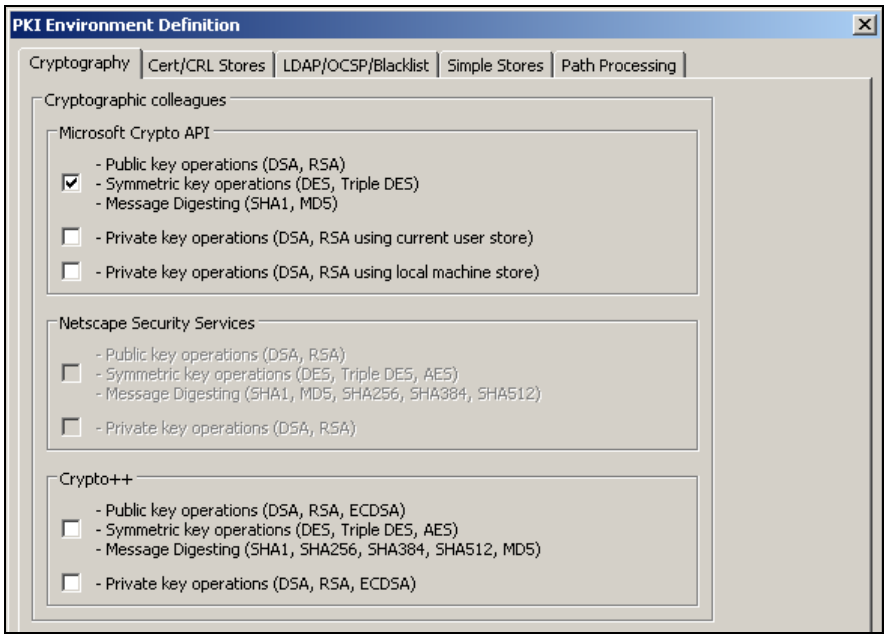
Cross-Certificate Trust Test Procedures

NOTE: These steps should be repeated on all 3 operating systems (XP, Vista, and Windows 7) for each end-entity certificate that was obtained in the Preliminary Actions including the revoked certificate.

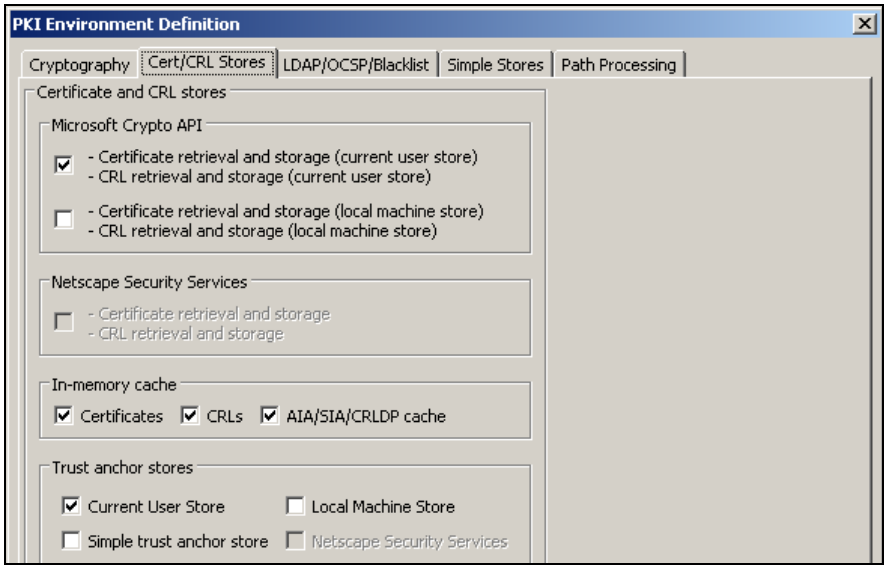
Cross-Certificate Trust Test Case #1: CAPI Path Processing

NOTE: Use of the self-signed **CCEB IRCA1** certificate as the trust anchor is the primary change from the procedure steps for the Direct Trust test. Intermediate CA certificates are also not loaded into CAPI.

1. Revert to the clean snapshot of the VM.
2. Update the Windows Certificate Store with the **CCEB IRCA1** certificate. By default the **Current User** store will be used. The certificates should be placed under **Trusted Root Certification Authorities**.
3. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
4. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:

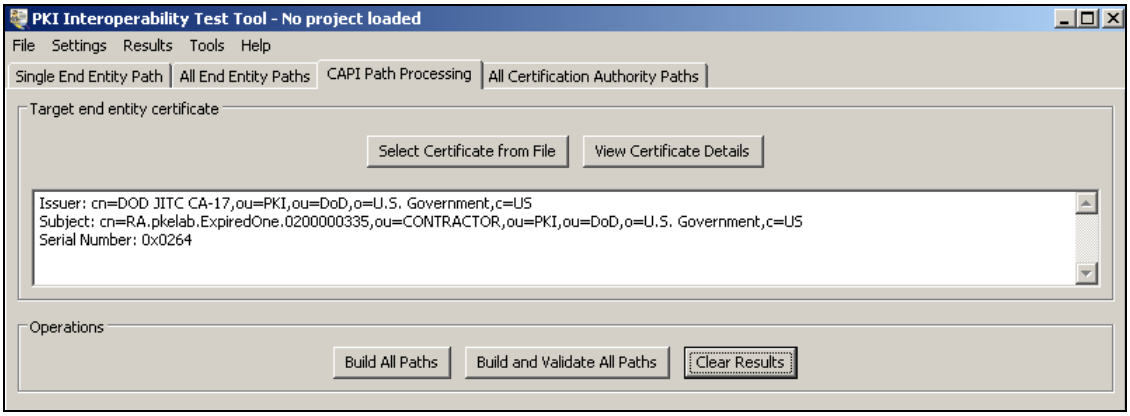


5. Select the **Cert/CRL Stores** tab and verify that the following options are set:



6. Click **OK** to close the **PKI Environment Definition** window and then click **Close** to go back to the PITT main window.

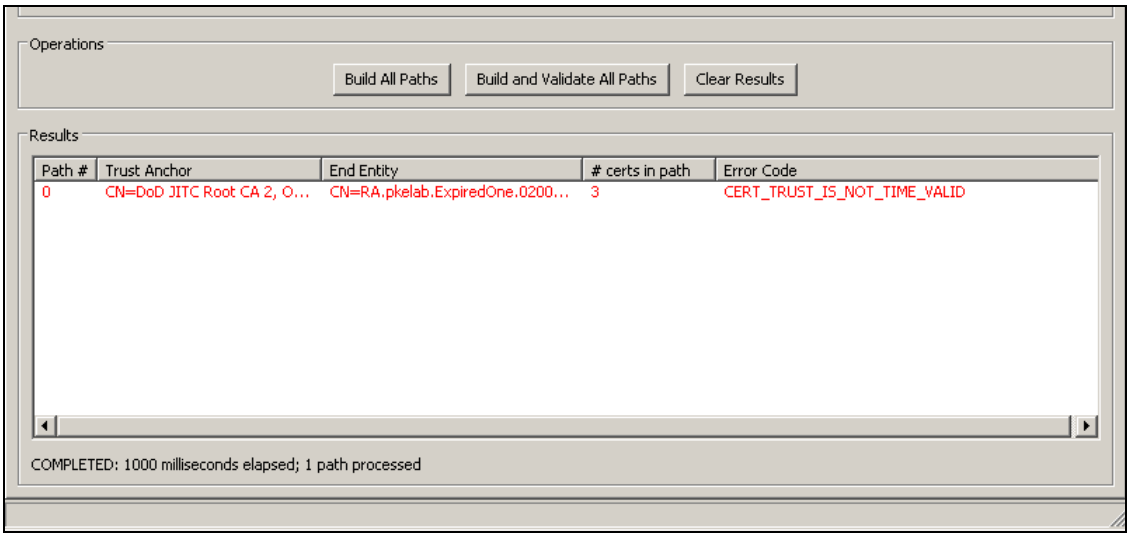
7. From the PITT main window, select the **CAPI Path Processing** tab. Click **Select Certificate from File** and load the end entity certificate to be tested.



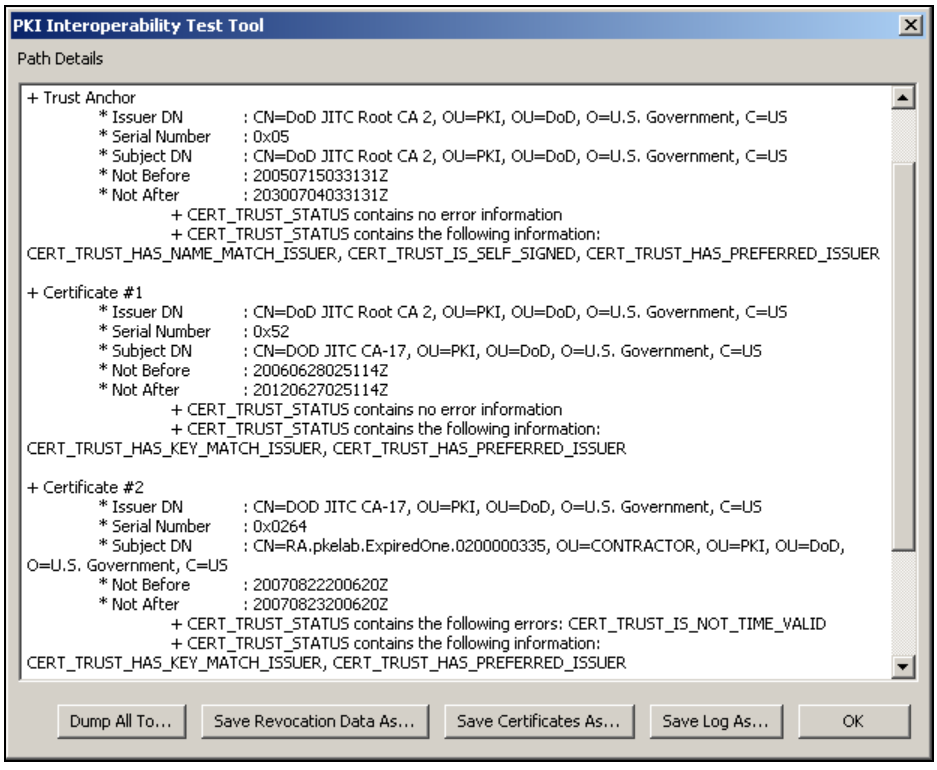
8. Once the certificate is loaded start an interface capture in **Wireshark.**

9. Return to PITT and in the **CAPI Path Processing** tab click **Build and Validate All Paths**.

10. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.



11. For each path listed, right-click on it and select **View Path Processing Results.**



12. Record the structure of the trust path in **Section 3-A** of the **Cross-Certificate CAPI Path Processing Results** table. List the type, certificate name (Common Name), and serial number of each certificate in the path, from the trust anchor to the end entity certificate.

Example:

Type	Certificate Name	Serial Number
Trust Anchor	DoD CCEB Interoperability CA 1	0x06
Certificate 1	DoD JITC CA-17	0x52
Certificate 2	RA.pkelab.ExpiredOne	0x0264

13. The top of the results log will display "*Chain contains no error*" if the path is valid, or "*Chain contains the following errors*" followed by the error code[6] if the path is invalid. Record any chain error code in **Section 3-B** as a critical finding, or *"pass"* if no error is shown.

14. For each certificate listed in the results logs, if no error was encountered the line "*CERT_TRUST_STATUS contains no error information*" will be shown. Otherwise the line *"CERT_TRUST_STATUS contains the following errors"* will be shown, followed by error code(s). Record any certificate error code in **Section 3-C** as a critical finding, or *"pass"* if no error is shown. Example:

Certificate Name	Error Code(s)	Severity
DoD CCEB Interoperability CA 1		Pass
DoD JITC CA-17		Pass
RA.pkelab.ExpiredOne	CERT_TRUST_IS_NOT_TIME_VALID	Critical

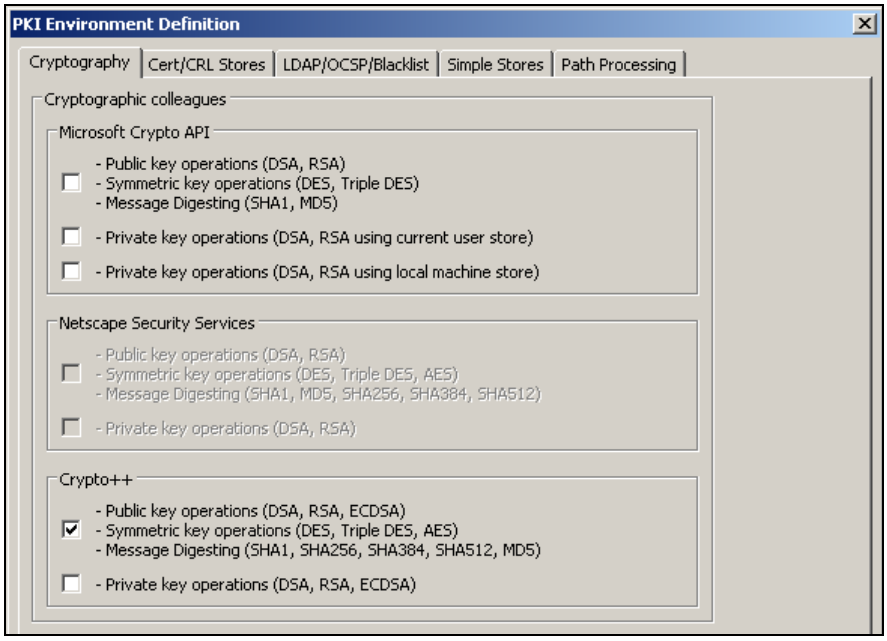
NOTE: For the revoked end entity certificate, error code *"CERT_TRUST_IS_REVOKED"* should be treated as *"pass"*.

3. Click **Dump All To…** to save a copy of the results.

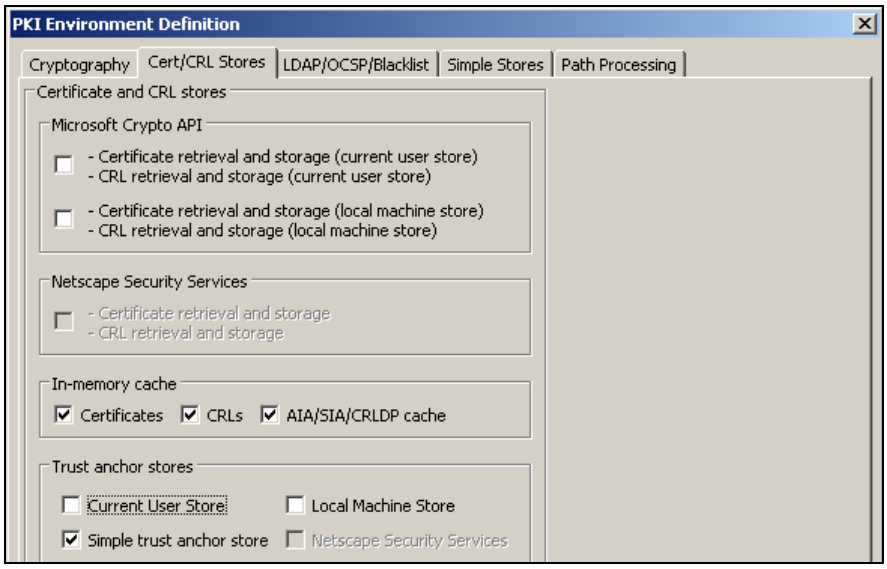
[6] Full list of *CERT_TRUST_STATUS* error codes and their explanation can be found at http://msdn.microsoft.com/en-us/library/aa377590%28VS.85%29.aspx.

Cross-Certificate Trust Test Case #2: PKIF Path Processing

1. Revert to the clean snapshot of the VM.
2. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
3. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:



4. Select the **Cert/CRL Stores** tab and verify that the following options are set:



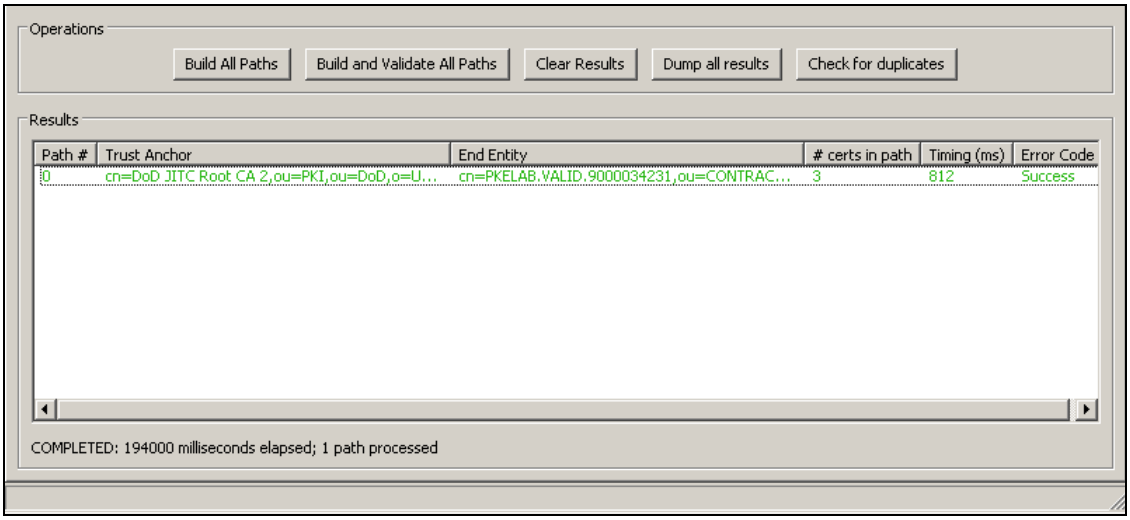
5. Select the **Simple Stores** tab and use the **Add** button to load the **CCEB IRCA1** certificate into the **Specify trust anchor** panel.

6. From the PITT main window, select the **All End Entity Paths** tab. Click **Select Certificate from File** and load the end entity certificate to be tested.

7. Once the certificate is loaded start an interface capture in **Wireshark.**

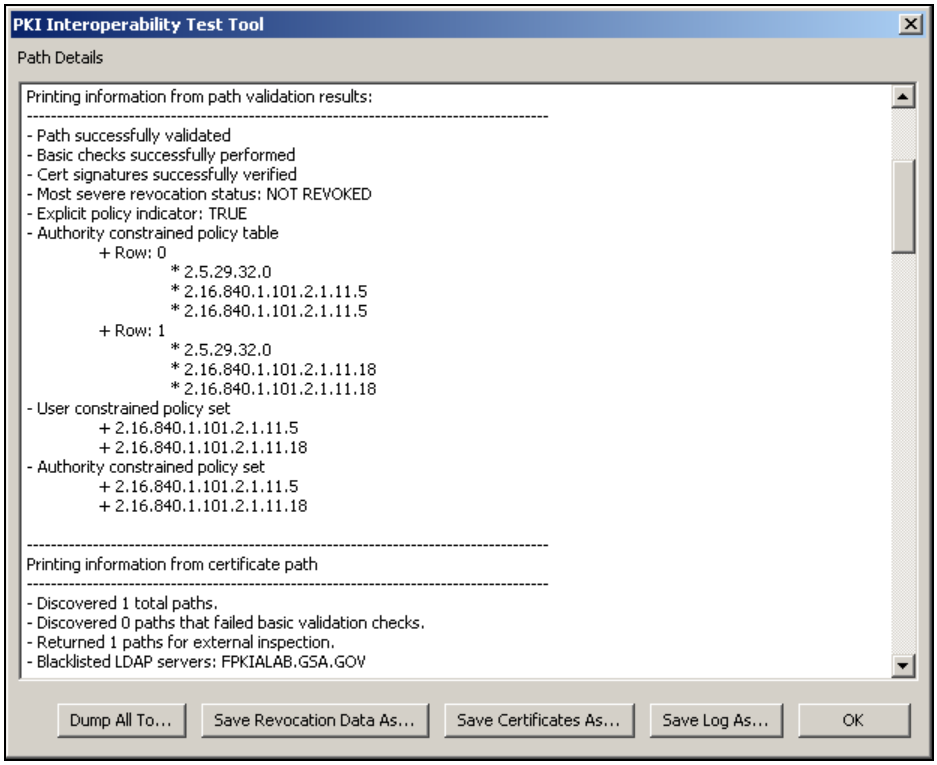
8. Return to PITT and in the **All End Entity Paths** tab click **Build and Validate All Paths**.

9. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.



10. For each path listed, right-click on it and select **View Path Processing Results.**

    Sample output:



11. Record the structure of the trust path in **Section 4-A** of the **Direct Trust PKIF Path Processing Results** table. List the type, Common Name (CN), and serial number of each certificate in the path, from the trust anchor to the end entity certificate. Example:

Type	**Common Name**	**Serial Number**
Trust Anchor	DoD CCEB Interoperability CA 1	0x06
Certificate 1	DoD JITC CA-17	0x52
Certificate 2	RA.pkelab.ExpiredOne	0x0264

12. **Overall Validation Check** – If the path is valid, *"NOT REVOKED"* will be shown under *"Most severe revocation status"*. Otherwise an error condition will be shown. Record the error condition in **Section 4-B** as a critical finding, or *"pass"* if no error.

    NOTE: For the revoked end entity certificate, a revoked status should be treated as *"pass"*.

13. **Certificate Path Check –** Under "*Printing information from certificate path*", for each certificate, record the status of the following checks:

    a. Record the "*diagnostic code*". This will be *"0 : Success"* if all checks were successful, which should be classified as *"pass"*. If any check has failed, an error code will be displayed. Record the error code in **Section 4-C** as a critical finding.

    NOTE: For the revoked end entity certificate a diagnostic code of *"PATH_VALIDITY_PERIOD_VIOLATION"* should be treated as *"pass"*.

    b. For each "*Revocation source*" listed, record the "*Revocation source type*" (1 = CRL, 2 = OCSP) and the "*Revocation source error code*", which will be *"0 : Success"* if a revocation source has no error. Record this as *"pass"* in **Section 4-C**. If any other error code is displayed, record it as a critical finding.

Example:

Certificate Name:	DoD CCEB Interoperability CA 1			**Severity**
Diagnostic Code:	0 : Success			Pass
Certificate Name:	DoD JITC CA-17			
Diagnostic Code:	0 : Success			Pass
Revocation Type:	OCSP	**Revocation Source Error Code:**	0 : Success	Pass
Certificate Name:	RA.pkelab.ExpiredOne			
Diagnostic Code:	PATH_VALIDITY_PERIOD_VIOLATION			Critical
Revocation Type:	OCSP	**Revocation Source Error Code:**	OCSP_PATH_FAILED	Critical
Revocation Type:	CRL	**Revocation Source Error Code:**	0 : Success	Pass

14. **URI Check –** Each certificate will have a "*URI results*" section listing all URIs found in the certificate and their status. Record the certificate extension the URI belongs to, its access protocol, and the URI's status, which can be one of the following:

    a. *"URI_CORRECT_DATA"* indicates a correct and accessible URI. Record this as *"pass"* in **Section 4-D**.

    b. *"URI_INCORRECT_DATA"* indicates that the URI contains incorrect information or lacks required information. Record this as a critical finding in **Section 4-D**.

    c. *"URI_NOT_AVAILABLE"* indicates an inaccessible URI. Record this as a critical finding in **Section 4-D**.

    d. *"URI_WARNING"* indicates the presence of a self-signed certificate in the URI. Record this as a non-critical finding in **Section 4-D**.

Example:

Certificate Name:	DoD CCEB Interoperability CA 1					**Severity**
Extension:	SIA	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Extension:	SIA	**Protocol:**	LDAP	**Status:**	URI_NOT_AVAILABLE	Critical
Certificate Name:	DoD JITC CA-17					
Extension:	AIA	**Protocol:**	HTTP	**Status:**	URI_WARNING	Non-Critical
Extension:	SIA	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Extension:	CDP	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass
Certificate Name:	RA.pkelab.ExpiredOne					
Extension:	AIA	**Protocol:**	LDAP	**Status:**	URI_WARNING	Non-Critical
Extension:	AIA	**Protocol:**	HTTP	**Status:**	URI_INCORRECT_DATA	Critical
Extension:	CDP	**Protocol:**	HTTP	**Status:**	URI_CORRECT_DATA	Pass

15. Click **Dump All To…** to save a copy of the results.

Cross-Certificate Trust Test Results

Summarize the results in the following table. Use one set of tables for each trust path.

Cross-Certificate Trust CAPI Path Processing Results

3-A. Trust Path Information (CAPI Test Procedure #12)		
Type	**Common Name**	**Serial Number**

3-B. Chain Error Code (CAPI Test Procedure #13)	**Severity (Critical, Non-Critical, or Pass)**

3-C. Certificate Error Code (CAPI Test Procedure #14)		
Certificate Name	**Error Code(s)**	**Severity**
	Number of Critical Findings:	
	Number of Non-Critical Findings:	

Cross-Certificate Trust PKIF Path Processing Results

4-A. Trust Path Information (PKIF Test Procedure #11)		
Type	**Common Name**	**Serial Number**

4-B. Overall Validation Check (PKIF Test Procedure #12)	**Severity (Critical, Non-Critical, or Pass)**

4-C. Certificate Path Check (PKIF Test Procedure #13)				
Certificate Name:				**Severity**
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		
Certificate Name:				
Diagnostic Code:				
Revocation Type:		**Revocation Source Error Code:**		
Revocation Type:		**Revocation Source Error Code:**		

Cross-Certificate Trust PKIF Path Processing Results (continued)

4-D. URI Check (PITT Test Procedure #14)						
Certificate Name:						**Severity**
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Certificate Name:						
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
Extension:		**Protocol:**		**Status:**		
					Number of Critical Findings:	
					Number of Non-Critical Findings:	

Summary of Test Results

Data Summary

At the completion of all tests summarize the results in the following table. List the name of each end entity certificate tested and whether it failed or passed each of the four test cases.

End Entity Certificate	Direct Trust CAPI Path Processing	Direct Trust PKIF Path Processing	Cross-Certificate Trust CAPI Path Processing	Cross-Certificate Trust PKIF Path Processing

Determine Conclusion

All end entity certificates from the Partner PKI and the Third Party PKI must have passed all test cases in order to be approved for interoperability with the Host PKI. In the event of failure, provide the error information to the Partner PKI so the issues can be resolved.

Appendix A – Testing Transitive Trust

Transitive trust describes the situation where the Host PKI and the Partner PKI have a cross-certificate relationship, and the Partner PKI has a cross-certificate relationship with a Third Party PKI. The Host PKI needs to constrain path building in some way so that the cross-certification to the Third Party PKI is not unknowingly inherited, allowing unintended certificates to be successfully validated.

Transitive Trust Test Plan

JITC testers will use the latest version of PITT to test each end entity certificate supplied by the Third Party PKI. For each certificate two test cases will be used, each utilizing a different path processing engine and trusted certificate store. These are:

- Path processing using Crypto API (CAPI) engine and the Windows Certificate Store.
- Path processing using PKI Framework (PKIF) engine and the PITT Simple Store.

In each test case the trusted certificate store will contain the CCEB IRCA1 certificate as the trust anchor. The path processing engine will attempt to build and validate all possible trust paths from the end entity certificate to the trust anchor. The resulting log will be examined for errors and other information.

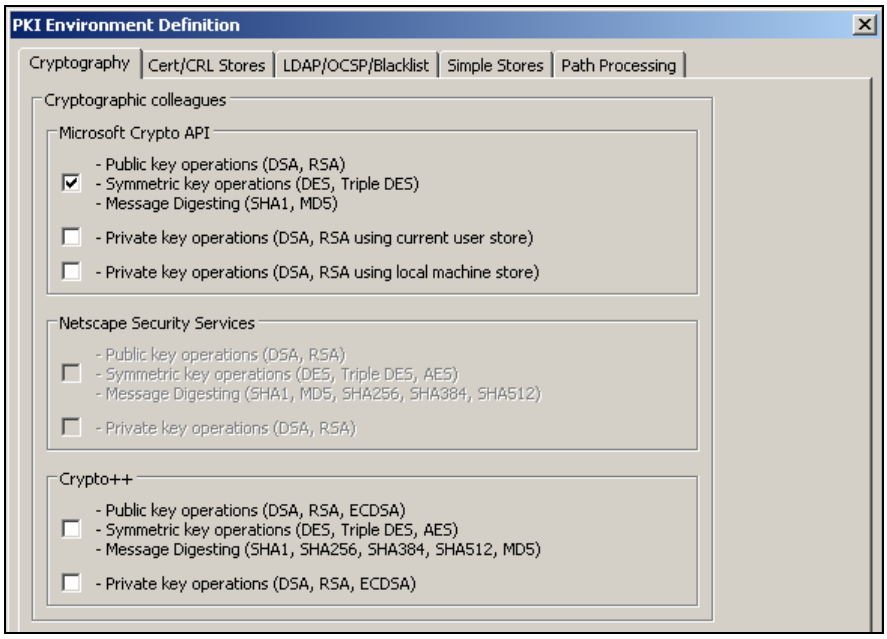
The Transitive Trust test is successful if both the PKIF and the CAPI test cases returned no valid trust path.

Transitive Trust Test Procedures

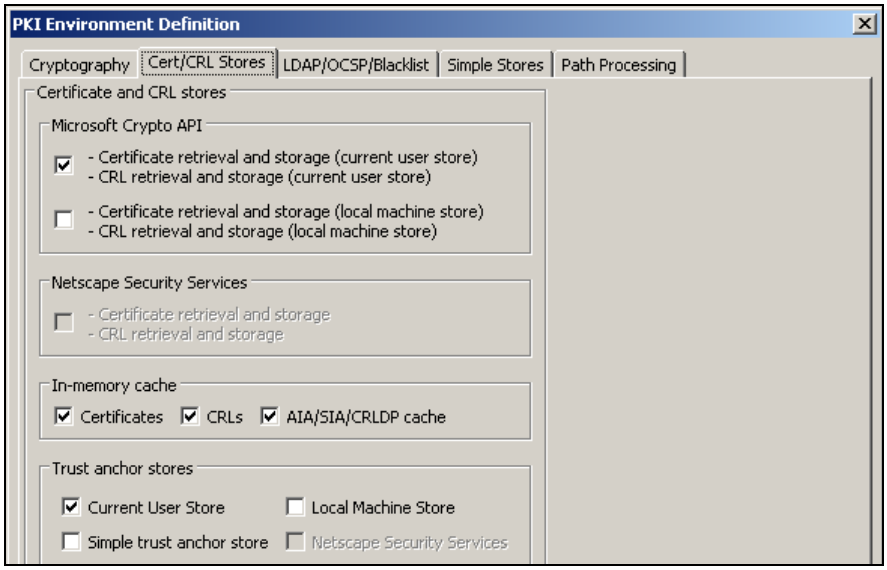
NOTE: These steps should be repeated on all 3 operating systems (XP, Vista, and Windows 7) for each Third Party PKI end-entity certificate that was obtained in the Preliminary Actions.

Transitive Trust Test Case #1: CAPI Path Processing

1. Revert to the clean snapshot of the VM.
2. Update the Windows Certificate Store with the **CCEB IRCA1** certificate. By default the **Current User** store will be used. The certificates should be placed under **Trusted Root Certification Authorities**.
3. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
4. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:

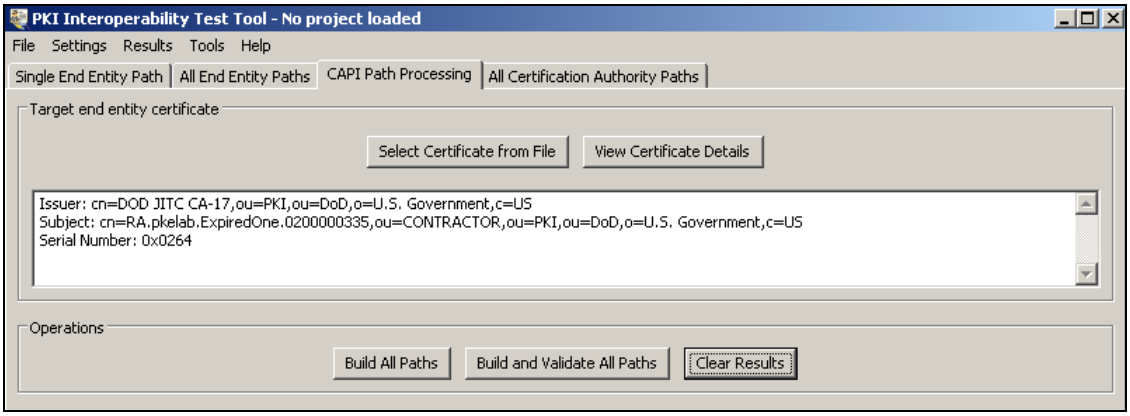


5. Select the **Cert/CRL Stores** tab and verify that the following options are set:



6. Click **OK** to close the **PKI Environment Definition** window and then click **Close** to go back to the PITT main window.

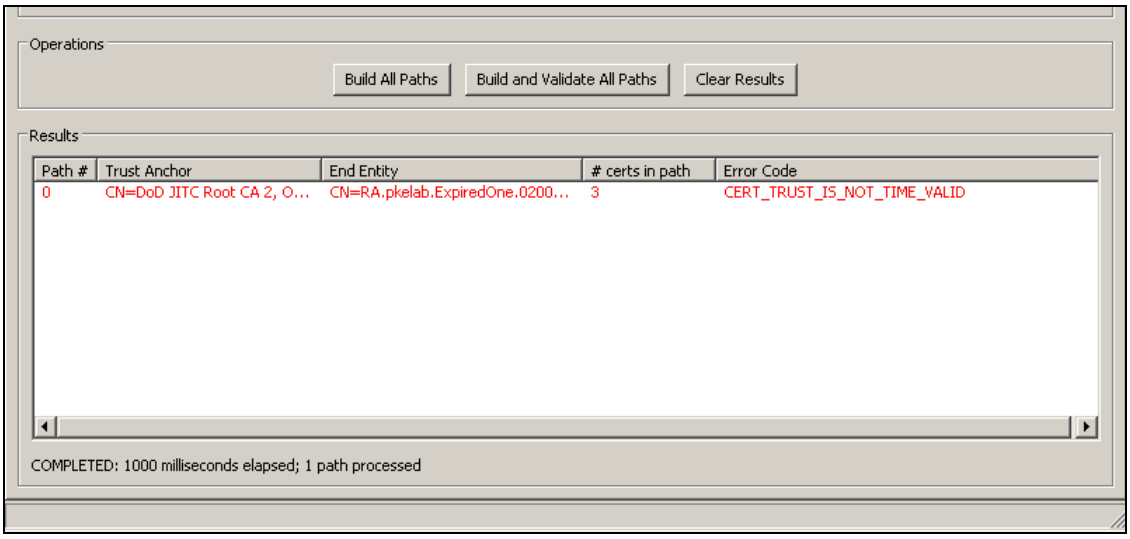
7. From the PITT main window, select the **CAPI Path Processing** tab. Click **Select Certificate from File** and load the Third Party PKI end entity certificate to be tested.



8. Once the certificate is loaded start an interface capture in **Wireshark.**

9. Return to PITT and in the **CAPI Path Processing** tab click **Build and Validate All Paths**.

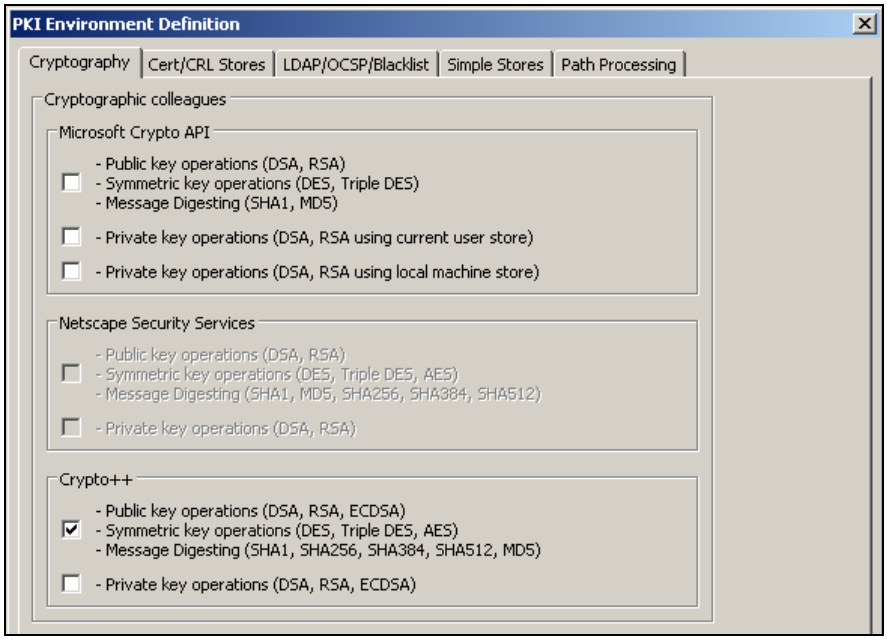
10. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.



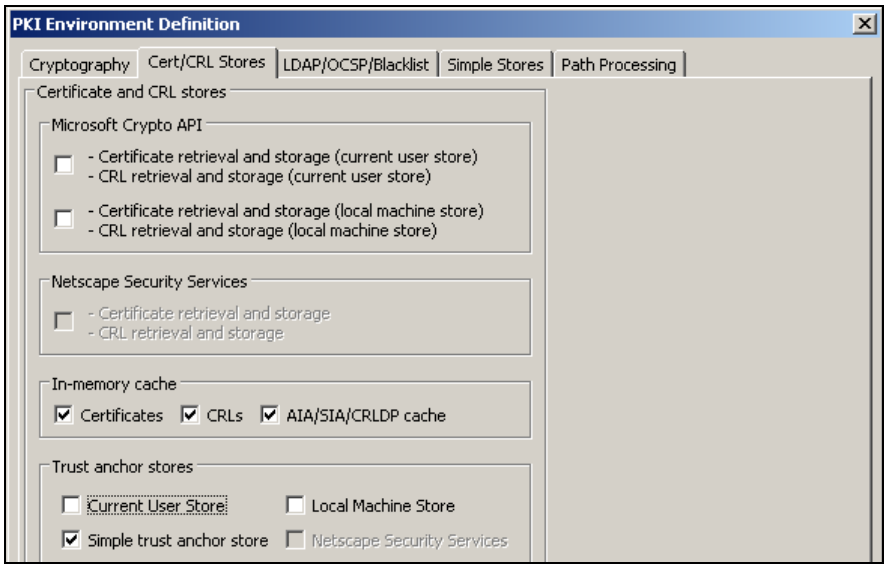
11. If any valid (green) path is found, record the structure of the trust path in **Section 5-A** of the **Transitive Trust CAPI Path Processing Results** table. List the type, Common Name (CN), and serial number of each certificate in the path, from the trust anchor to the end entity certificate. This is a critical finding.

Transitive Trust Test Case #2: PKIF Path Processing

1. Revert to the clean snapshot of the VM.
2. In the PITT menu bar select **Settings → Edit Default PKI Settings**, then in the **Default Settings** window click **Define PKI Environment**.
3. In the **PKI Environment Definition** window, select the **Cryptography** tab and verify that the following options are set:



4. Select the **Cert/CRL Stores** tab and verify that the following options are set:



5. Select the **Simple Stores** tab and use the **Add** button to load the **CCEB IRCA1** certificate into the **Specify trust anchor** panel.

6. From the PITT main window, select the **All End Entity Paths** tab. Click **Select Certificate from File** and load the Third Party PKI end entity certificate to be tested.

7. Once the certificate is loaded start an interface capture in **Wireshark.**

8. Return to PITT and in the **All End Entity Paths** tab click **Build and Validate All Paths**.

9. The bottom of the **Results** panel will display "COMPLETED" once all paths have been discovered. Valid paths are shown in green while invalid ones are shown in red. At this point stop the **Wireshark** capture and save the .pcap file.

10. If any valid (green) path is found, record the structure of the trust path in **Section 6-A** of the **Transitive Trust PKIF Path Processing Results** table. List the type, Common Name (CN), and serial number of each certificate in the path, from the trust anchor to the end entity certificate. This is a critical finding.

Transitive Trust Test Results

Summarize the results in the following table. Use one set of tables for each trust path.

Transitive Trust CAPI Path Processing Results

5-A. Trust Path Information (CAPI Test Procedure #11)		
Type	**Common Name**	**Serial Number**

Transitive Trust PKIF Path Processing Results

6-A. Trust Path Information (PKIF Test Procedure #10)		
Type	**Common Name**	**Serial Number**

Appendix B – Contact Information

Website
Please visit the DoD PKE Interoperability Website URL below for additional information
https://powhatan.iiie.disa.mil/pki-pke/interoperability.html

Technical Support
Contact technical support
PKE_Support@disa.mil

Appendix C – References

[1] DoD Chief Information Officer (CIO) Memorandum, "Approval of External Public Key Infrastructures". July 2008.
http://jitc.fhu.disa.mil/pki/documents/20080722_dod_external_pki_memo.pdf

[2] Department of Defense PKI External Interoperability Plan (EIP). March 2009. Prepared by External Interoperability Working Group.
http://jitc.fhu.disa.mil/pki/documents/dod_external_interoperability_plan_aug_2010.pdf

[3] Department of Defense Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling". May 2011. http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf