DoD Public Key Infrastructure

(PKI) Partner PKI Interoperability Test Plan

15 November 2010

Version 2.0

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
11/15/2010	2.0	Version 2.0

Contents

Introduction

This document provides guidance and steps necessary to conduct Public Key enabled application interoperability testing of partner Public Key Infrastructures (PKIs) with which the 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 interoperability. As a result of Federal and DoD secure information sharing initiatives, DoD and its partners are required to establish and maintain secure PKI interoperability. DoD Instruction 8520.2 is the governing policy document for DoD PKI and DoD relying party responsibilities and the DoD PKI External Interoperability Plan describes categories and requirements for approval of external PKIs. In addition to the requirements specified in the aforementioned documents, each intended external PKI must be tested and evaluated by JITC to prove they are technically interoperable prior to approval for use in DoD.

Scope of Test Plan

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

Purpose of Testing

The purpose of this testing is to analyze and validate the PKIs of DoD partners. Validating the PKIs involves ensuring DoD systems are capable of seamlessly interoperating with the agencies PKIs from a technical standpoint.

Preliminary Actions

Before testing begins, testers must gather all required information and materials from the intended partner PKI. This information will facilitate testing.

Obtain Required Materials

The DoD test team must obtain the following test materials from the intended partner:

- Partner Root Certificate Authority (CA) certificate(s)
- Partner Intermediate/Subordinate CA certificate(s)
- A valid set of ALL the certificates on the end-user's card (i.e. ID or PIV(I) Auth Cert, Signature Cert, Encryption Cert, Card Auth Cert)
- At least one revoked end-user certificate (Revoked certificates should be from the same issuing CA as the valid set of Certificates)

These materials should be obtained via a digitally signed e-mail from the intended partner. The partner should label each end-user certificate with the usage and the revocation status. For example the following name conventions can be used for a certificate that will be used for E-mail signing and Smart Card Logon:

Valid_Sign_SCL.cer or *Revoked_Sign_SCL.cer*

Once all preliminary actions are completed proceed to testing described in the next section.

Operating System Requirements

The following are requirements for the operating system that will be used for testing.

- Windows XP SP3, Windows Vista SP2, or Windows 7 or above. Testing should be done on the pre-configured Virtual Machines (VMs) provided by the DoD PKE team. VM should be loaded with either VMware Server 2.0. Tester should take snapshots as specified in the procedures. This allows the tester to simple "revert to snapshot" to return the box back to its clean state and thus avoiding contaminated results. In VMware Server 2 in the options panel on the right-hand side of the "Summary" tab.
- The latest version of PITT installed. Pre-configured VMs from the DoD PKE team will have this installed but it is necessary to verify PITT is the latest version at the time of testing. This tool can be downloaded here: http://pkif.sourceforge.net/pitt.html. The download for PITT is located in the ***Downloads*** section of the PKIF webpage. Be sure to choose the ***.msi*** file for Windows machines. Once installed, the PITT application along with a PITT user guide will be in the ***Start→Programs***.

  NOTE: The latest version of PITT is currently 1.2. Although newer versions of the tool will be released, not all new releases will require partner re-testing. Re-testing will only be required when requirements change and thus notification will be sent to the appropriate JITC contacts.

- Wireshark (Pre-Configured VMs will have this installed)
- Turn off Automatic Root Certificates Update.
    - 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`".
- Turn Name Constraints off (**For Windows XP Only**)
    - Click **Start**, and **Run**. Type "**Regedit"** to edit the registry.
    - Navigate to the following registry key and add the following:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\root\ProtectedRoots\Flags]
      "***bitmask"=dword:0x20***

        a. Right-Click on **"Root"** and select **"New"**, then select **"Key"**
        b. Name the Key **"ProtectedRoots"**
        c. Right-Click on **"ProtectedRoots"** select **"New"**, then select **"DWORD Value"**
        d. Name the DWORD Value **"Flags"**
        e. Right-Click the DWORD Value and select **"Modify"**
        f. Enter **"20"** as the value and click **"OK"**
        g. Close regedit - No restart of the operating system is required

Testing Overview

Interoperability testing will validate the use of other partner approved PKIs on DoD systems. Testing will be conducted by the DoD Joint Interoperability Test Command (JITC). Testers will use the PKI Interoperability Test Tool (PITT) to inspect and validate all the required elements/attributes of the approved partner PKI.

Objectives

The primary objectives of this testing are listed as follows:

A. Trust partner root certificate either directly or through cross-certification
B. Validate partner certificates as applicable (Cross/Subordinate CA/End Entity certificates)
C. Check availability and performance of all partner URIs in certificate extensions
D. Ensure partner's revoked certificates are properly rejected

About PITT

The PITT tool path processing element is based on the RFC 5280 path processing algorithm. This algorithm is described in detail in **Section 6** of the RFC 5280 which can be found here: http://www.ietf.org/rfc/rfc5280.txt

Testing: Direct Trust Interoperability

The direct trust model requires the DoD to directly trust the target PKI trust anchor (self-signed Root certificate). In a production environment, the DoD public key enabled application will be required to trust the root certificates and have access to the revocation information of the target PKI in order to determine the validity of the target PKI certificates. While the direct trust test method can be used for any DoD partner PKI whether a federal bridge partner or not, reliance on direct trust to establish interoperability should be avoided except in extraordinary circumstance. DoD Policy and business needs will determine when direct trust may be used.

Direct Trust Test Plan

The DoD JITC Test team will use the latest version of the PKI Interoperability Test Tool (PITT).

Each end-user certificate (i.e. Signature, Encryption, PIV Auth, and ID) must be tested with the PITT tool. The PITT tool will build and validate certificate paths. PITT has the ability to leverage two certification path processing engines:

-Microsoft Crypto API (CAPI)
-PKI Framework (PKIF)

These implementations can use trust anchors stored in one of the two trust anchor stores:

-CAPI store configuration
-PITT custom "simple store" configuration

These configurations allow simulation of the path processing behavior of the commonly used applications in the DoD. Each configuration will be a use case which uses the respective Partner's Root certificates as Trust Anchors. For this testing, a partner end-user certificate will be validated with several use cases. If all statuses are "ok" (see next section for details), and all Universal Resource Identifiers (URIs) are resolvable then the intended partner certificate and infrastructure has passed the Direct Trust Interoperability test.

Direct Trust Test Procedures

The following are the testing procedures for each configuration use case. After running the PITT tool, testers will be able to determine a Pass or Fail result from the PITT Results Report. After determining the results, testers will use PITT to generate a Summary Report.

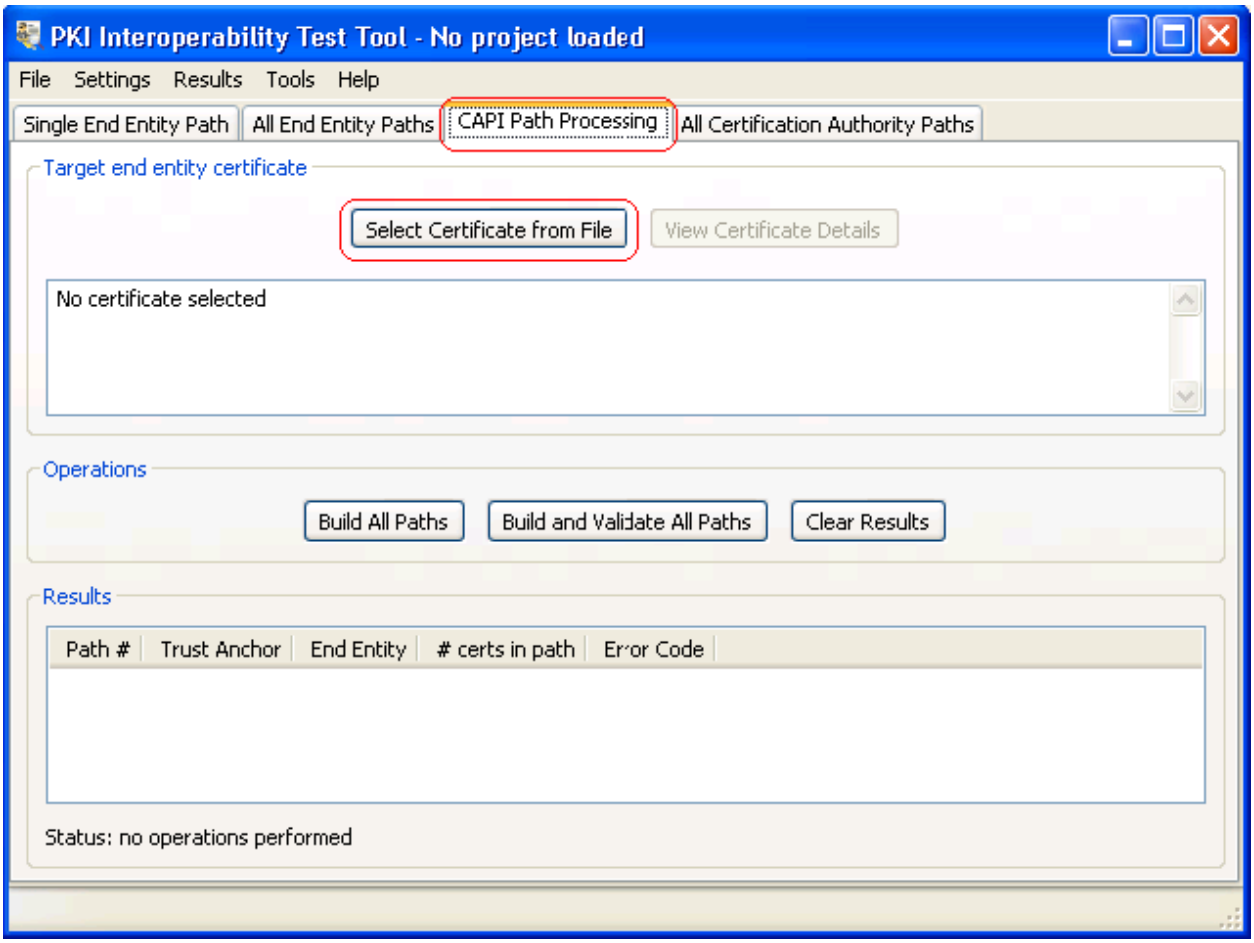
NOTE: These steps should be completed on all 3 operating systems (XP, Vista, and Windows 7) for each partner end-entity certificate that was obtained in the preliminary actions including the revoked certificate.

DT Use Case #1: CAPI Store Configuration (Using Microsoft CAPI Path Processing)

1. Take a snapshot of the VM at a clean state (no partner certificates installed) before beginning testing. This allows for testers to revert back to a clean state before completing each section of testing.

2. Update the CAPI Computer store with the root and intermediate/subordinate CA certificates of the partner PKI.
   For Windows XP: Right-click the certificate and select ***Install Certificate***. For testing installing the certificate into the Current User store is ok, in this case just select all default options in the wizard.
   For Windows Vista/7: Right-click the certificate and select ***Install Certificate***. Click ***Open***. Click ***Next.*** Select "**Place all Certificates in the following store"** and select the **"Trusted Root Certification Authorities"** for the Root Certificate, and **"Intermediate Certification Authorities"** for the Sub-CA certificates.

3. Launch the **PITT.exe** tool.
4. Select ***Settings→Edit PITT Settings***.
5. Check the box ***Check URIs during path processing***. Click ***Ok***.
6. Now in the ***CAPI Path Processing*** tab under the ***Target End Entity Certificate*** click ***Select Certificate from File***.

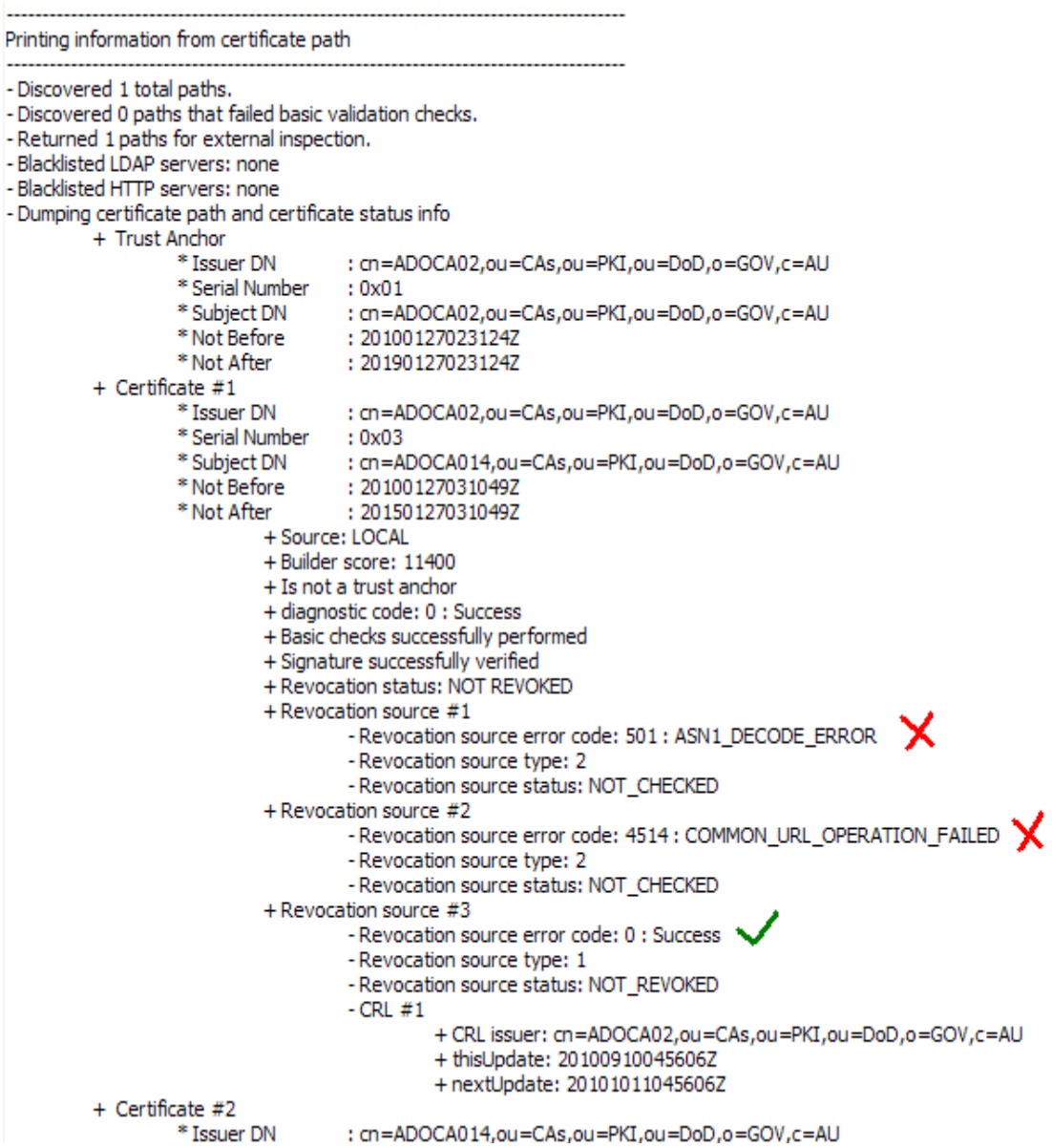


7. Browse to a partner end-user certificate and select it.
8. Once the certificate is selected start an interface capture in **Wireshark.**
9. Click ***Build and Validate Path***.

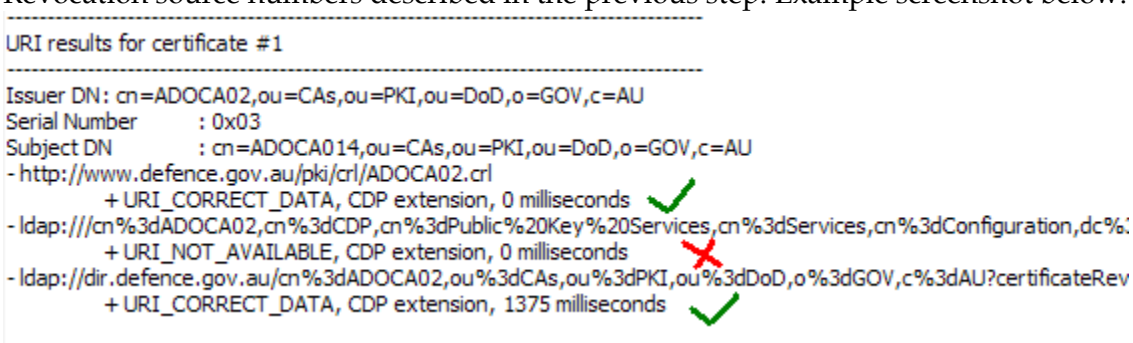
10. PITT will attempt to build and validate all elements and then display a detailed report of each element of the certificate path.
11. When PITT has completed validation, stop **Wireshark** capture and save the .pcap file to a "*Results_Data_Partner_X"* folder created for this partner.
12. **Overall Validation Result checks** -- Under the "***Printing information from path validation results***" verify all checks were a success and the "***Most severe revocation status***" is not revoked. Should look similar to following screenshot (policy identifiers may vary):

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
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
                * 2.5.29.32.0
                * 2.16.840.1.101.2.1.11.19
                * 2.16.840.1.101.2.1.11.19
- User constrained policy set
        + 2.16.840.1.101.2.1.11.9
        + 2.16.840.1.101.2.1.11.19
- Authority constrained policy set
        + 2.16.840.1.101.2.1.11.9
        + 2.16.840.1.101.2.1.11.19
```

13. **Certificate Path checks** -- Under "Printing information from certificate path" verify each certificate (marked with +) has performed all checks successfully and there are no error messages. Details of each certificate will be listed under the certificate as shown in the screen shot below. Testers should review all the details listed for the certificate and check for any abnormalities. Verify the ***"Revocation source error code"*** for each Revocation source. The following screenshot is an example of a certificate that has two bad ***Revocation sources*** and one good source:



14. **URI checks** -- Verify URIs. The information under the URIs marked with a + will indicate the state of that URI. The URIs are in order (1, 2, 3, e.t.c) corresponding with the Revocation source numbers described in the previous step. Example screenshot below:



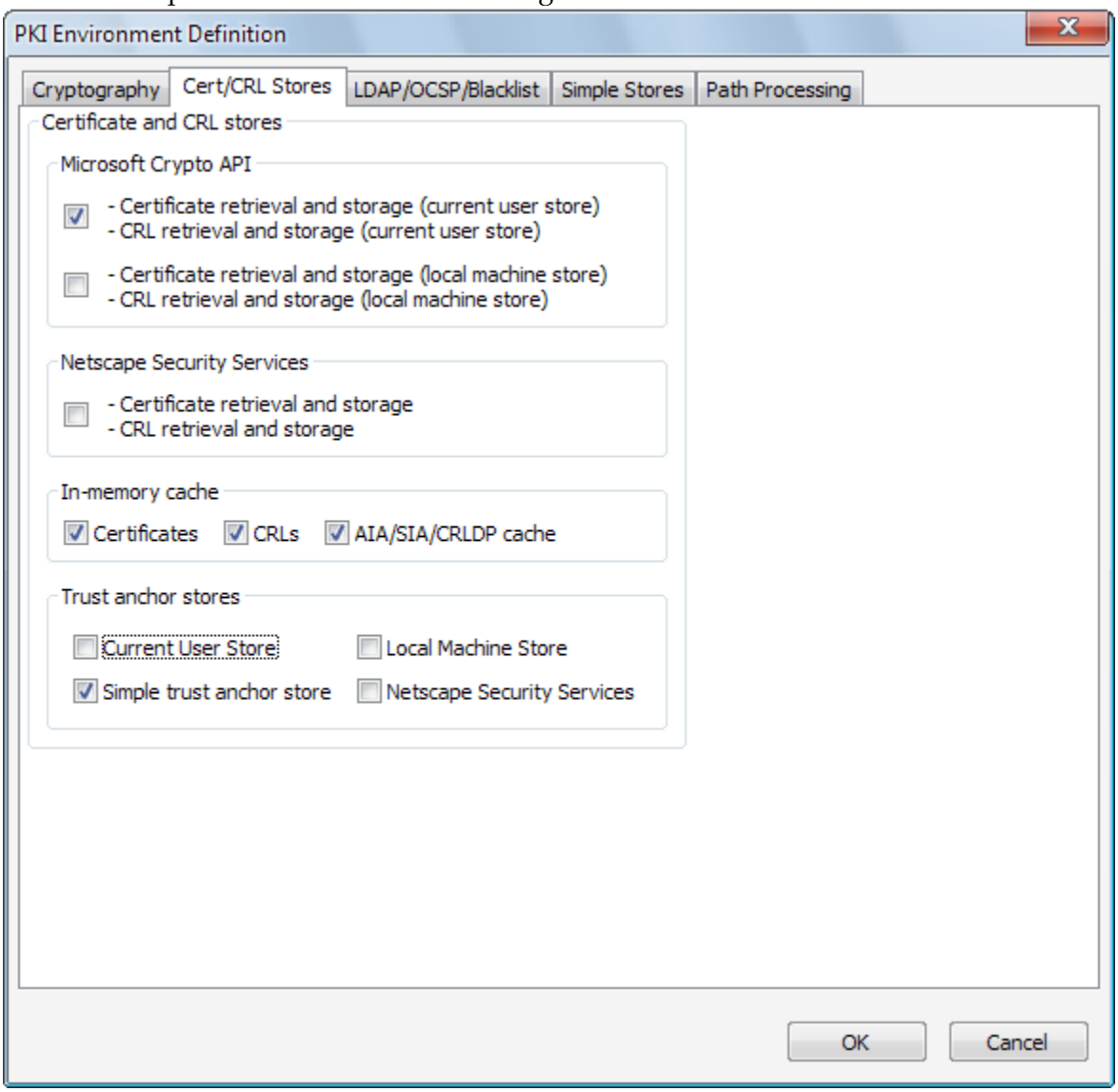
15. Record Results. Perform the following checks:

✓ From **Step 12(Overall Validation Result checks):** i. If there are NO red messages, there is a revocation status, AND all checks were a success → Record **Good**. ii. If there is a problem → Note the problem in comments section, record **Bad**, and move to the next check (Tester want to report ALL issues with the Partner PKI)**.**	Good / Bad *Findings/Comments:*
✓ From **Step 13 (Certificate Path checks):** i. If all is successful → Record **Good**. ii. If there are any unsuccessful/failed checks or bad Revocation sources → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
✓ From **Step 14 (URI checks):** i. If the URI is successful → Record **Good**. ii. If there are any bad URIs → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
DT - Use Case #1: CAPI Store Configuration - **All** "Goods" indicate the partner has passed. - Otherwise the partner has failed.	Pass / Fail
Findings/Comments:	

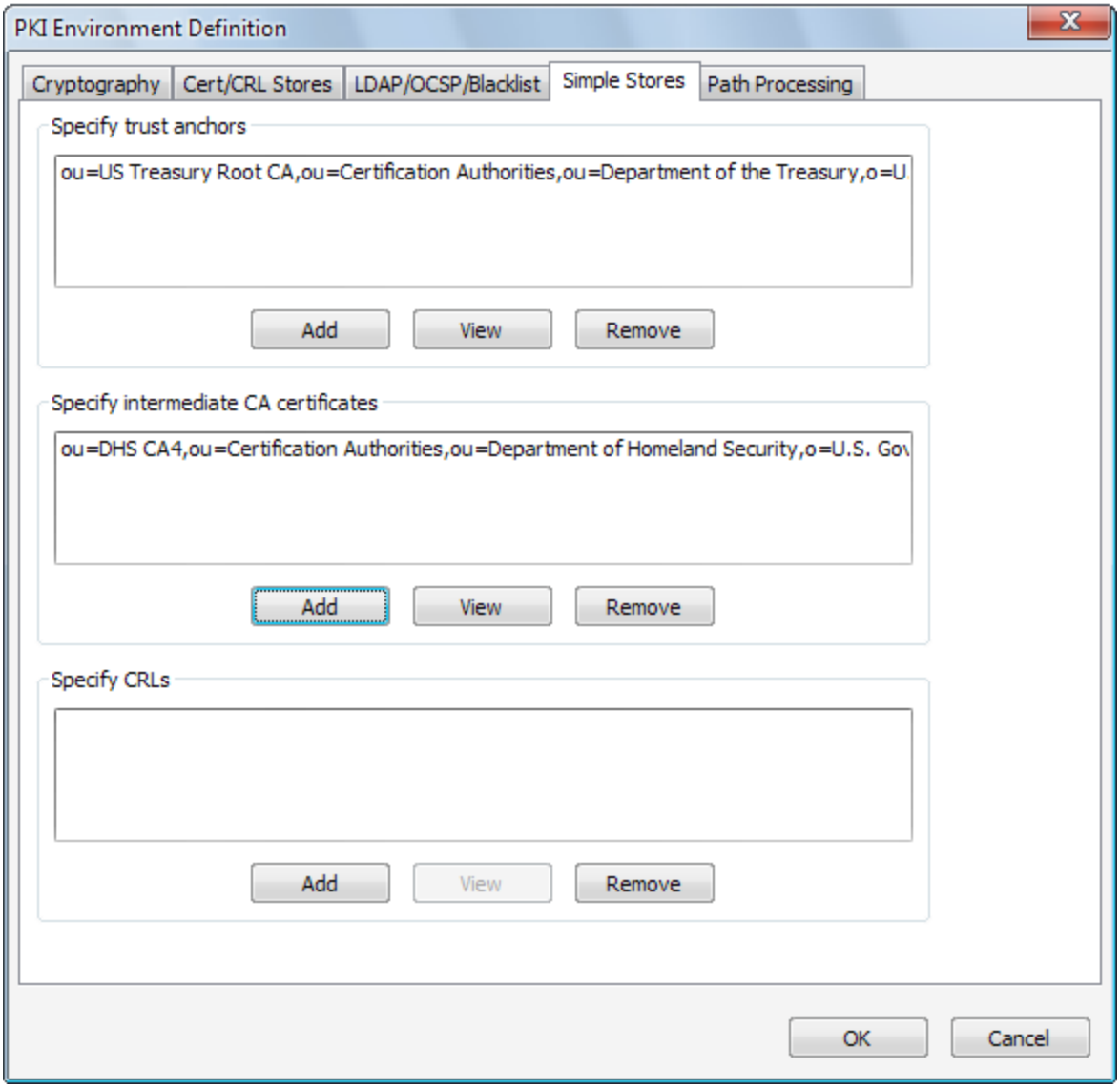
16. Copy and Paste the Results report into a file. Save the report for the corresponding partner in the "*Results_Data_Partner_X"* folder.
17. Revert to the clean snap-shot.

DT Use Case #2: PITT Custom Simple Store Configuration (Using PKIF path processing)

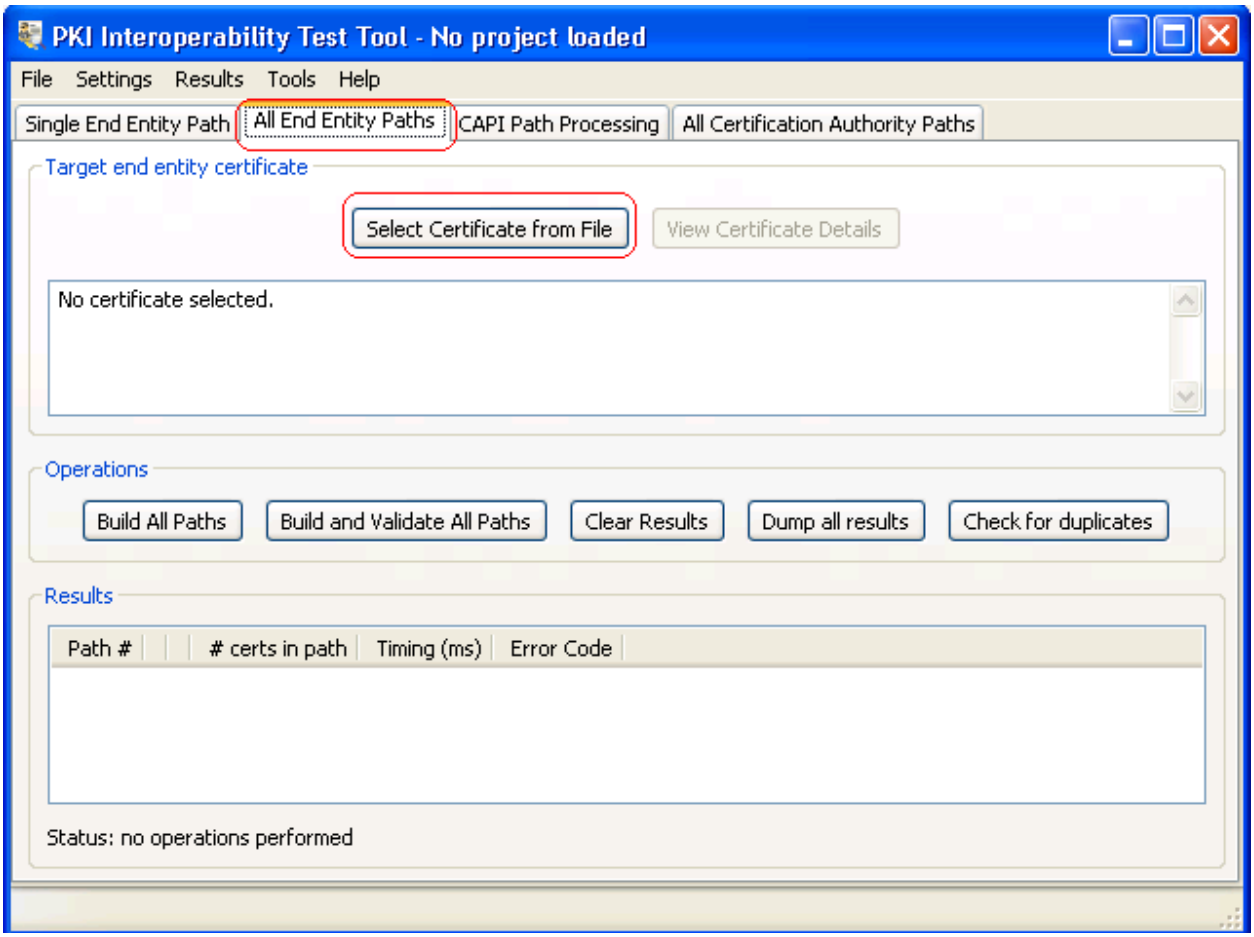
1. Launch the **PITT.exe** tool.
2. Select ***Settings→Edit Default PKI Settings***.
3. Select ***Define PKI Environment***.
4. In the PKI Environment Definition window select the ***Cert/CRL Stores*** tab.
5. Select same options selected in the following screenshot:



6. In the PKI Environment Definition window select the ***Simple Stores*** tab.
7. The partner Root CA certificate and Sub-ordinate CA certificate(s) must be added to the simple store. Click ***Add*** and browse to the certificate.



8. After certificates have been added select ***OK***.
9. Select ***Define Path Settings***. Check the box ***Initial explicit policy indicator***.
10. *Click* **Ok** and ***Close.***
11. Select ***Settings→Edit PITT Settings***.
12. Check the box ***Check URIs during path processing***. Click ***Ok***.
13. Now in the ***All End Entity Paths*** tab under the ***Target End Entity Certificate*** click ***Select Certificate from File***.



14. Browse to the partner end-user certificate and select it.
15. Once the certificate is selected start a interface capture with **Wireshark.**
16. Click ***Build and Validate Path***.
17. PITT will attempt to build and validate all elements and then display a detailed report of each element of the certificate path.
18. When PITT has completed validation, stop **Wireshark** capture and save the .pcap file to a "*Results_Data_Partner_X"* folder created for this partner.
19. **Overall Validation Result checks** -- Under the "***Printing information from path validation results***" verify all checks were a success and the "***Most severe revocation status***" is not revoked.
20. **Certificate Path checks** -- Under "Printing information from certificate path" verify each certificate (marked with +) has performed all checks successfully and there are no error messages. Details of each certificate will be listed under the certificate as shown in the screen shot below. Testers should review all the details listed for the certificate and check for any abnormalities. Verify the ***"Revocation source error code"*** for each Revocation source.
21. **URI checks** -- Verify URIs. The information under the URIs marked with a + will indicate the state of that URI. The URIs are in order (1, 2, 3, e.t.c) corresponding with the Revocation source numbers described in the previous step.
22. Record Results. Perform the following checks:

a. From **Step 19(Overall Validation Result checks):** i. If there are NO red messages, there is a revocation status, AND all checks were a success → Record **Good**. ii. If there is a problem → Note the problem in comments section, record **Bad**, and move to the next check (Tester want to report ALL issues with the Partner PKI)**.**	Good / Bad *Findings/Comments:*
b. From **Step 20 (Certificate Path checks):** i. If all is successful → Record **Good**. ii. If there are any unsuccessful/failed checks or bad Revocation sources → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
c. From **Step 21 (URI checks):** i. If the URI is successful → Record **Good**. ii. If there are any bad URIs → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
DT - Use Case #2: PKIF Simple Store Configuration - **All** "Goods" indicate the partner has passed. - Otherwise the partner has failed.	Pass / Fail
Findings/Comments:	

23. Copy and Paste the Results report into a file. Save the report for the corresponding partner in the "*Results_Data_Partner_X*" folder for the partner.
24. After this test is complete revert to snap-shot.

Direct Trust Test Results

Summarize the results in the following table:

DT - Use Case #1: CAPI Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the Microsoft CAPI Store with the Partner Root and Intermediate CA certificates installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	
DT - Use Case #2: PKIF Simple Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the PITT Custom Simple Store with the Partner Root and Intermediate CA certificates installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	

Testing: Cross-Certificate Trust Interoperability

In the cross-certification trust model, each CA issues a certificate to another CA that it trusts. The two certificates become a cross-certificate pair providing 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 user will trust the Interoperability Root CA (IRCA) self-signed certificate which allows for establishing partner trust through path-processing.

Cross-Certificate Trust Test Plan

The DoD JITC Test team will use the latest version of the PKI Interoperability Test Tool (PITT). This tool can be downloaded here: http://pkif.sourceforge.net/pitt.html.

Each end-user certificate (i.e. Signature, Encryption, PIV Auth, and ID) must be tested with the PITT tool. For Cross-Certificate testing, the PITT tool will build and validate certificate paths leveraging these two configurations:

-CAPI store configuration
-PITT custom "simple store" configuration

These two configurations allow simulation of the path processing behavior of the commonly used applications in the DoD. Each configuration will be a use case which uses the self-signed **Interoperability Root CA (IRCA)** as a common Trust Anchor for all Partners. For this testing, a partner end-user certificate will be validated with both use cases. If all statuses are "ok" (see next section for details), all Universal Resource Identifiers (URIs) are resolvable, **AND** the partner end-user certificate trust chain terminates at the **IRCA** certificate then the intended partner certificate and infrastructure has passed the Cross-Certificate Interoperability test.

Cross-Certificate Trust Test Procedures

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

NOTE: Use of the self-signed IRCA certificate as the Trust Anchor is the primary change from the procedure steps for the Direct Trust test.

The following are the testing procedures for each configuration use case. After running the PITT tool, testers will be able to determine a Pass or Fail result from the PITT Results Report. After determining the results, testers will use PITT to generate a Summary Report.

The first step is to download and install PITT from the URL above. The download for PITT is located in the ***Downloads*** section of the PKIF webpage. Be sure to choose the ***.msi*** file for

Windows machines. Once installed, the PITT application along with a PITT user guide will be in the ***Start→Programs***.

CC Trust - Use Case #1: CAPI Store Configuration (Using Microsoft CAPI Path processing)

1. Take a snapshot of the VM at a clean state (no partner certificates installed) before beginning testing. This allows for testers to revert back to a clean state before completing each section of testing.
2. Update the CAPI Current User store with the **IRCA self-signed root certificate**.

   For Windows XP: Right-click the certificate and select ***Install Certificate***. For testing installing the certificate into the Current User store is ok, in this case just select all default options in the wizard.
   For Windows Vista/7: Right-click the certificate and select ***Install Certificate***. Click ***Open***. Click ***Next.*** Select "**Place all Certificates in the following store"** and select the **"Trusted Root Certification Authorities"** for the Root Certificate.

3. Launch the **PITT.exe** tool.
4. Select ***Settings→Edit PITT Settings***.
5. Check the box ***Check URIs during path processing***. Click ***Ok***.
6. Now in the ***CAPI Path Processing*** tab under the ***Target End Entity Certificate*** click ***Select Certificate from File***.
7. Browse to a partner end-user certificate and select it.
8. Once the certificate is selected start an interface capture with **Wireshark.**
9. Click ***Build and Validate Path***.
10. PITT will attempt to build and validate all elements and then display a detailed report of each element of the certificate path.
11. When PITT has completed validation, stop **Wireshark** capture and save the .pcap file to a "*Results_Data_Partner_X"* folder created for this partner.
12. **Overall Validation Result checks** -- Under the "***Printing information from path validation results***" verify all checks were a success and the "***Most severe revocation status***" is not revoked.
13. **Certificate Path checks** -- Under "Printing information from certificate path" verify each certificate (marked with +) has performed all checks successfully and there are no error messages. Details of each certificate will be listed under the certificate as shown in the screen shot below. Testers should review all the details listed for the certificate and check for any abnormalities. Verify the ***"Revocation source error code"*** for each Revocation source.
14. **URI checks** -- Verify URIs. The information under the URIs marked with a + will indicate the state of that URI. The URIs are in order (1, 2, 3, e.t.c.) corresponding with the Revocation source numbers described in the previous step.
15. **Trust Anchor check –** Verify the Trust Anchor of the chain is the **IRCA** self-signed root certificate.
16. Record Results. Perform the following checks:

a. From **Step 12(Overall Validation Result checks):**	Good / Bad

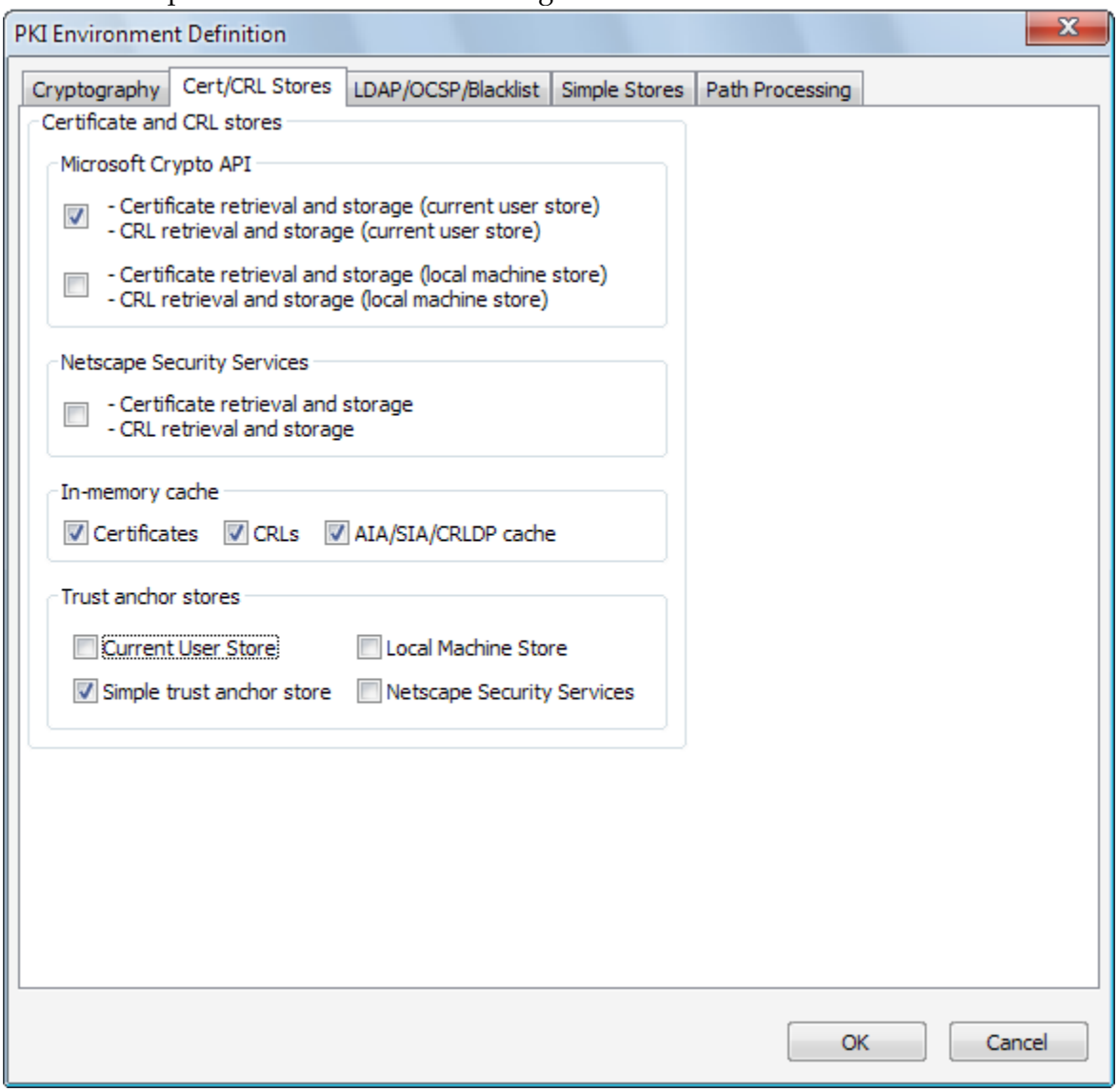
i. If there are NO red messages, there is a revocation status, AND all checks were a success → Record **Good**. ii. If there is a problem → Note the problem in comments section, record **Bad**, and move to the next check (Tester want to report ALL issues with the Partner PKI)**.**	*Findings/Comments:*
b. From **Step 13(Certificate Path checks):** i. If all is successful → Record **Good**. ii. If there are any unsuccessful/failed checks or bad Revocation sources → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
c. From **Step 14 (URI checks):** i. If the URI is successful → Record **Good**. ii. If there are any bad URIs → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
d. From **Step 15 (Trust Anchor Check)** i. If Trust Anchor is **IRCA** → Record **Good.** ii. If Trust Anchor is not **IRCA** → Record **Bad**.	Good / Bad *Findings/Comments:*
CC - Use Case #1: CAPI Store Configuration - **All** "Goods" indicate the partner has passed. - Otherwise the partner has failed.	Pass / Fail

Findings/Comments:

17. Copy and Paste the Results report into a file. Save the report for the corresponding partner into the *"Results_Data_Partner_X"* folder created for this partner.
18. After this test is complete revert to snap-shot.

CC Trust - Use Case #2: PITT Custom Simple Store Configuration

1. Launch the **PITT.exe** tool.
2. Select ***Settings→Edit Default PKI Settings***.
3. Select ***Define PKI Environment***.
4. In the PKI Environment Definition window select the ***Cert/CRL Stores*** tab.
5. Select same options selected in the following screenshot:



6. In the PKI Environment Definition window select the ***Simple Stores*** tab.
7. The self-signed IRCA certificate must be added to the Trust Root Anchor store. Click ***Add*** and browse to **IRCA** certificate.
8. After certificate has been added select ***OK***.
9. Select ***Define Path Settings***. Check the box ***Initial explicit policy indicator***.
10. *Click* **Ok** and ***Close.***
11. Select ***Settings→Edit PITT Settings***.
12. Check the box ***Check URIs during path processing***. Click ***Ok***.

13. Now in the ***All End Entity Paths*** tab under the ***Target End Entity Certificate*** click ***Select Certificate from File***.
14. Browse to a partner end-user certificate and select it.
15. Once the certificate is selected start an interface capture with **Wireshark.**
16. Click ***Build and Validate Path***.
17. PITT will attempt to build and validate all elements and then display a detailed report of each element of the certificate path.
18. When PITT has completed validation, stop **Wireshark** capture and save the .pcap file to a "*Results_Data_Partner_X"* folder created for this partner.
19. **Overall Validation Result checks** -- Under the "***Printing information from path validation results***" verify all checks were a success and the "***Most severe revocation status***" is not revoked.
20. **Certificate Path checks** -- Under "Printing information from certificate path" verify each certificate (marked with +) has performed all checks successfully and there are no error messages. Details of each certificate will be listed under the certificate as shown in the screen shot below. Testers should review all the details listed for the certificate and check for any abnormalities. Verify the ***"Revocation source error code"*** for each Revocation source.
21. **URI checks** -- Verify URIs. The information under the URIs marked with a + will indicate the state of that URI. The URIs are in order (1, 2, 3, e.t.c.) corresponding with the Revocation source numbers described in the previous step.
22. **Trust Anchor check –** Verify the Trust Anchor of the chain is the **IRCA** self-signed root certificate.
23. Record Results. Perform the following checks:

e. From **Step 19(Overall Validation Result checks):** i. If there are NO red messages, there is a revocation status, AND all checks were a success → Record **Good**. ii. If there is a problem → Note the problem in comments section, record **Bad**, and move to the next check (Tester want to report ALL issues with the Partner PKI)**.**	Good / Bad *Findings/Comments:*
f. From **Step 20 (Certificate Path checks):** i. If all is successful → Record **Good**. ii. If there are any unsuccessful/failed checks or	Good / Bad *Findings/Comments:*

bad Revocation sources → Note the error message and corresponding URI and Record **Bad**.	
g. From **Step 21 (URI checks):** i. If the URI is successful → Record **Good**. ii. If there are any bad URIs → Note the error message and corresponding URI and Record **Bad**.	Good / Bad *Findings/Comments:*
h. From **Step 22 (Trust Anchor Check)** i. If Trust Anchor is **IRCA** → Record **Good.** ii. If Trust Anchor is not **IRCA** → Record **Bad**.	Good / Bad *Findings/Comments:*
CC - Use Case #2: PKIF Simple Store Configuration - **All** "Goods" indicate the partner has passed. - Otherwise the partner has failed.	Pass / Fail
Findings/Comments:	

24. Copy and Paste the Results report into a file. Save the report for the corresponding partner to the "*Results_Data_Partner_X"* folder created for this partner.
25. After this test is complete revert to snap-shot.

Cross Certificate Trust Test Results

Summarize the results in the following table:

CC Trust - Use Case #1: CAPI Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the Microsoft CAPI Store with the IRCA certificate installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	
CC Trust - Use Case #2: PKIF Simple Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the PITT Custom Simple Store with IRCA certificate installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	

Summary of Testing Results

Data Summary

At the completion of testing testers should put together both tables of results as follows:

DT - Use Case #1: CAPI Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the Microsoft CAPI Store with the Partner Root and Intermediate CA certificates installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	
DT - Use Case #2: PKIF Simple Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the PITT Custom Simple Store with the Partner Root and Intermediate CA certificates installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	
CC Trust - Use Case #1: CAPI Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the Microsoft CAPI Store with the IRCA certificate installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	
CC Trust - Use Case #2: PKIF Simple Store Configuration	Pass / Fail
Procedure: *Use the PITT Tool to verify path building leveraging the PITT Custom Simple Store with IRCA certificate installed. Use PITT to validate partner end-user certificate attributes and elements.*	
Finding/Comments:	

Determine Conclusion

The intended partner must have passed all tests in order to be approved for Interoperability use. In the event a partner has failed any portion of the test, inform the partner of the results and the issues.

Appendix A – Contact Information

Website
Please visit the DoD PKE Interoperability Website URL below for additional information
https://www.us.army.mil/suite/page/571419

Technical Support
Contact technical support
PKE_Support@disa.mil

Appendix B – 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