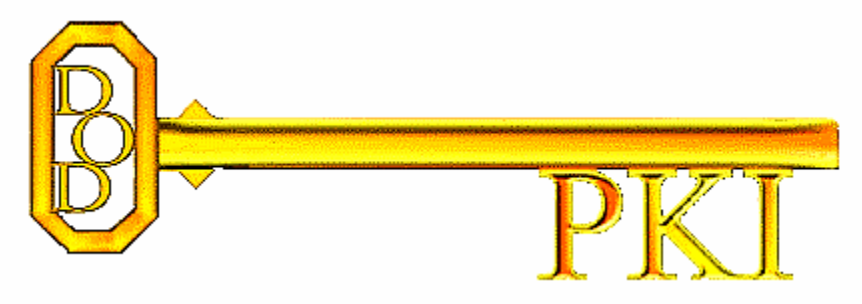
Test Plan

for

Department of Defense (DoD) Public Key Infrastructure (PKI) Interagency/Partner Interoperability

Version 1.0.3



Prepared for:
Department of Defense (DoD) PKI

August 27, 2008

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Curt Spann	6/12/08	Initial Release Candidate Draft	1.0
Curt Spann	6/18/08	Updated title page, added partner specific appendix, and incorporated Mr. Santosh Chokhani comments	1.0.1
Curt Spann	7/31/08	Added manual testing process for cross certificate section	1.0.2
Curt Spann	8/27/08	Removed CP and CPS review requirements	1.0.3

1 Overview

Secure information sharing among the United States (US) Department of Defense (DoD), US Federal Agencies, Non-Federal Agencies (e.g., State and Local Agencies, and Foreign, Allied or Coalition Partners requires that the PKIs used by these organization interoperate. Currently, each organization has its own, mature PKI.

The US Federal Bridge Certification Authority (FBCA) is an attempt to harmonize the security and provide for interoperability among these PKIs. Figure 1-1, "The DoD PKI External Interoperability Landscape" provides a notional view of the trust relationships established between the various PKIs.

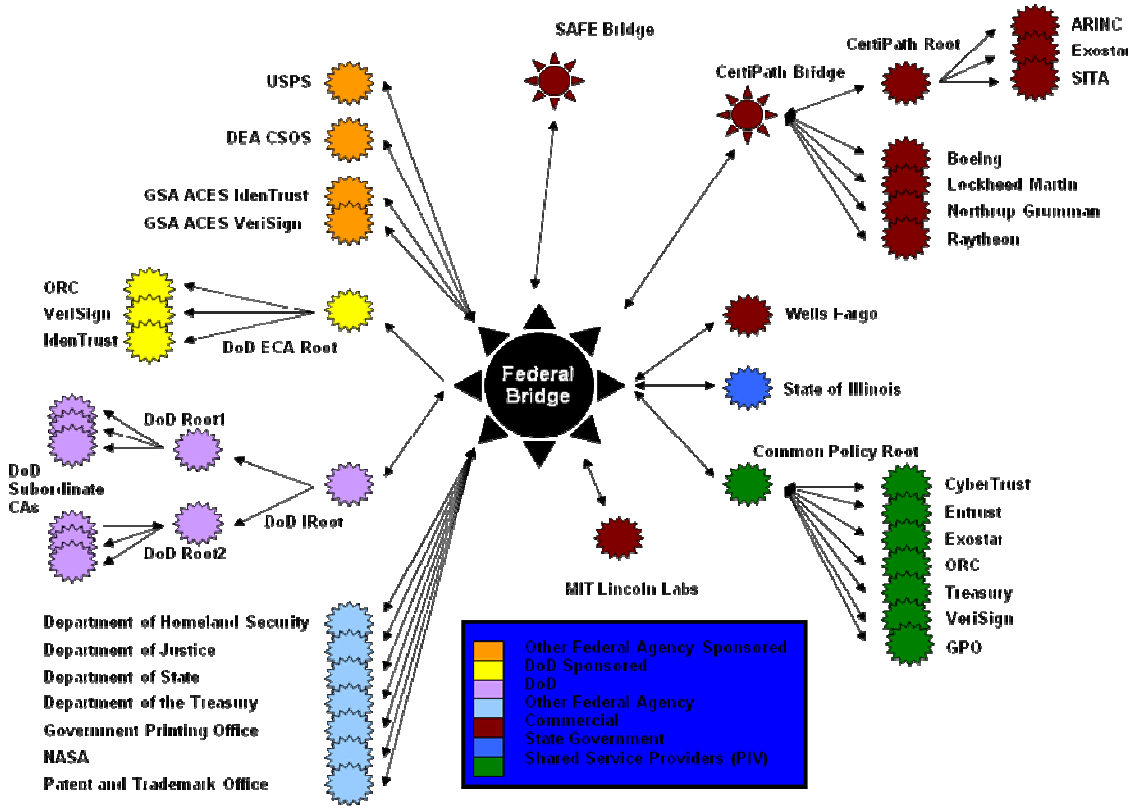


Figure 1-1 DoD PKI External Interoperability Landscape

PKI interoperability is defined as inter-organization applications that were interoperating without PKI-based security services (e.g., e-mail; Web ;etc.) continue to interoperate securely with applicable (i.e., authentication, integrity, confidentiality, and/or non-repudiation) when PK enabled.

Recent deployments of PKIs in each of these organizations and the introduction of the Federal Bridge Certification Authority (FBCA) have led to different

interoperability approaches. The goal of complete interoperability is challenging due to the following factors:

- Each organization is at different stage of technological readiness and sophistication;
- Commercial support for PK enabling applications varies from vendor to vendor;
- A wide range of PK enabled applications require interoperation; and
- Each PKI is at a different level of maturity in terms of development and/or deployment.

The PKI interoperability challenge requires using more than one approach. This document provides guidelines for conducting interoperability testing for the following approaches[1]:

I. Direct Trust – Under the direct trust approach, two or more organizations desiring PKI interoperability, install each others' trust anchors (generally distributed in the form of self-signed root certificates).

II. Bridge – Under the Bridge approach, several organizations cross certifiy with a Bridge. This concept can be used recursively (i.e., Bridges cross certifying Bridges) to provide Global PKI interoperability. Testing for approach includes utilizing cross certificates established with the FBCA or other partner PKI to validate PK enabled application interoperability. Thus, the testing under this approach covers both the cross certification with Bridge and direct organization ←→ cross certification.

The long term success of PKI interoperability will require partners to notify each other of changes in their PKI that can impact interoperability. Examples of these changes are certificate and CRL formats; OCSP request and response formats; and how these PKI objects are made available to the relying party applications of the peer organizations with which an organization wishes to interoperate.

1.1 Purpose

The purpose of this document is to provide an understanding to the DoD for system, application and portal owners, the risks inherent in implementing trust across the PKI landscape of Figure 1-1. Another purpose of this document is to provide the DoD application owners the various trust paths possible through the PKI landscape and the security ramifications of these trust paths.

This document provides the PKI interoperability testing approach through the use of common Internet-based applications (Email and Web Authentication). This document also contains the lessons learned to date in testing PKI interoperability using these applications with various PKIs. This document provides a set of pre-test setup and test cases to facilitate PK enabled application interoperability testing. This document also provides a framework for understanding the implications of implementation of the

[1] This document also uses the term "model" for the trust approaches.

Approval of External Public Key Infrastructures (PKI) Policy Memorandum and guidance on how certificates from US Federal Agencies and Non-Federal Agencies can be used on DoD systems and applications.

1.2 Scope

This document provides guidance and steps necessary to conduct PK enabled application interoperability testing through direct trust model and the cross certification model through the FBCA and with other partners. This version of the test plan limits PK enabled application interoperability testing to client authentication to Web Site (also known as certificate-based SSL client authentication) and secure email (digital signature and encryption). Other applications (smart card logon, desktops and laptops sign-on, virtual private network (VPN), mobile applications, network logon, code signing) may be expanded on by this test plan at a later date when requested by the External Interoperability Working Group (EIWG).

1.3 Participants

Name	Organization	Contact Info
DoD POCs	DoD PKI PMO (North - NSA)	Ms. Deborah M. Mitchell dmmitc3@missi.ncsc.mil
	DoD PKI PMO (South - DISA)	Ms. Jackie Villasenor Jackie.Villasenor@disa.mil
Agency/Partner POCs (TBD)		

1.4 Organizational PKI Usages

Partner usage or planned usage of PKI determines the level of interoperability to be achieved. Mission needs determine the PK enabled applications that require interoperability. Partners must agree on needs and evaluate current/planned capabilities.

1) Certain interoperability requirement questions must be answered to begin testing:
   - Is interoperability needed for access to Web servers?
   - Is interoperability needed for secure e-mail? If yes, which security services are required: signature, encryption, or both.
   - Is interoperability needed for encrypted files?
   - Is interoperability needed for other uses (smart card logon, desktops and laptops sign-on, code signing, VPNs, Personal Digital Assistants (PDAs), etc)?

- Which protocols will be used for access to PKI objects such as certificates, CRLs, OCSP requests and responses, etc.?

STEP I: Identify Usage (or Planned Usage) of PKI within Agency	
DoD Use	Agency/Partner Use (To be filled out before JITC test)
• Email Signature (send/ receive) • Email Encryption (send/receive) • Web server client authentication • Mobile Devices (BlackBerry S/MIME)	• TBD [Section filled out for Partner/Agency in Appendix A]

**STEP 1 Provides DoD list of common capabilities that could be considered for testing.

Based on the mission needs and capabilities, the partners should identify applications and systems that need to be tested.

2) Which common platforms need interoperability testing?

STEP 2: Identify Common Platforms between DoD and Agency/Partner		
Use - Application	DoD	Agency/Partner
Web application – IIS Windows 2003	X	
Web application – Apache Linux	X	
Web application – Other	X	
Email sign/encrypt – Outlook XP	X	
Email sign/encrypt – Outlook 2003	X	
Email sign/encrypt – Outlook 2007		
Email sign/encrypt – Mozilla Thunderbird		
Email sign/encrypt – Novell Mail		
Email sign/encrypt – Lotus Notes		
Email sign/encrypt – Web mail		
Email sign/encrypt – Other		
Remote Access VPN - Cisco	X	
Remote Access VPN – Microsoft		

Remote Access VPN - Other		
Mobile Application BlackBerry - S/MIME	X	
Mobile Application Windows Mobile		
Mobile Application Other		
Network Logon – XP	X	
Network Logon – Vista		
Network Logon – Linux/Mac		
Code Signing		
		[Section filled out for Partner/Agency in Appendix A]

**STEP 2 identifies common platforms that could be considered for interoperability. Also provides shareable lessons learned with partnering agencies PKI implementations.

1.5 Organizational PKI Architectures

Overview of partnering agencies PKI is extremely important to establishing interoperability. Access to root certificates, certificate status information and certficates are critical for PK enabled application interoperability.

3) Architecture Information the agency or partner needs to provide are:

1) What is the Agency PKI Hierarchy, including the root CA(s) and CA(s) under the Root?
2) Which of the CAs are signed by the Federal Bridge?
3) What is the largest CRL size?
4) How often are the CRL(s) generated?
5) How long are the CRL(s) valid for?
6) What is the maximum time the agency has to revoke known-compromised certificates?
7) Does the Agency/Partner provide an Online Certificate Status Protocol (OCSP) service? If yes,
    a. What is the OCSP trust model: direct trust; CA signed; or delegated
    b. Is the OCSP identified in AIA?
    c. Does the OCSP support pre-signed responses?
    d. Does the OCSP support nonce responses?
8) What are the certificate life times of the various types of CAs?
9) How often are the CAs added/removed in the infrastructure?
10) What are the Agency/Partner CAs intended use, what type of certificates are issued (e.g. email signature, email encryption, Web server, Windows domain controller, etc.)? What is the validity period for the various types of certificates.
11) What protocols are used to access the certificates and CRLs (e.g. HTTP, HTTPS, LDAP, LDAPS, etc.)?
12) Is there a repository for user certificates to obtain the public keys (e.g. email integration to an LDAP, email integration to HTTP, use of a LDAP proxy, etc.)?

13) Does the Agency/Partner run a test PKI environment? If so is it accessible to the internet?
14) Which certificate policy assurance levels will be tested?
15) Will HSPD-12 PIV authentication certificates be tested?
16) What key sizes and algorithms are used to sign:
    a. certificates
    b. CRLs
    c. OCSP responses

**STEP 3 provides the DoD test team the ability to determine what components of the Agency/Partners PKI are to be tested using a direct trust vice cross certificate test methods. These answers will also identify what external access is available to the DoD for testing.

STEP III: Answers to Agency/Partner Architecture	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
[Section filled out for Patner/Agency in Appendix A]	

2 Testing Overview

Interoperability testing will validate the use of other agency/partner approved PKIs on DoD systems. Testing will be conducted at the DoD Joint Interoperability Test Command (JITC). Testers will load required CA certificates into a public key enabled (PK-enabled) applications that are commonly found within the DoD.

1) Primary Objectives:
    a. Trust agency/partner root certificate either directly or through cross certification
    b. Validate agency/partner certificates as applicable (Cross/Subordinate CA/End Entity certificates)
    c. Prove ability to accept agency/partner's certificate for access to a DoD PK-enabled Web server
    d. Prove ability to trust email signed using agency/partner's certificate
    e. Prove ability for a DoD user to encrypt using agency/partner's encryption certificate
    f. Reject a agency/partner's revoked certificate
    g. Reject a agency/partner's expired certificate

2) Optional Objectives:
    a. Trust and validate signatures on mobile code signed by a agency/partner's code signing certificate
    b. Utilize agency/partner OCSP responder, if provided
    c. Verify interoperability with device applications (domain controllers, desktops and laptops, VPNs, mobile applications, network logon)

Required Items:

Agency/Partner issued

- Agency/Partner Root CA certificate
- Agency/Partner Cross-certificate, when applicable
- Agency/Partner Subordinate CA certificates, when applicable
- Agency/Partner Identity certificate
- Agency/Partner Email Signature certificate when applicable
- Agency/Partner Email Encryption certificate
- Agency/Partner Root CA CRL
- Agency/Partner Subordinate CA CRLs
- Agency/Partner End Entity revoked certificate
- Agency/Partner End Entity expired certificate

DoD-issued (JITC Equivalent)

- DoD Root CA certificate
- DoD Cross-certificate, when applicable
- DoD Subordinate CA certificates
- DoD Identity certificate
- DoD Email Signature certificate
- DoD Email Encryption certificate
- DoD Root CA CRL
- DoD Subordinate CA CRLs
- DoD End Entity revoked certificate
- DoD End Entity expired certificate
- DoD PK-enabled Web server

Optional:

- Agency/Partner PK-enabled Web server

Optional:

- Mobile code signed by DoD certificate

- Mobile code signed by Agency/Partner certificate
- Device applications – TBD
- OCSP responder testing
- Device applications – TBD

3 Testing Direct Trust Interoperability

The direct trust model requires the DoD to directly trust the root certificates of the target PKI. 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. The direct trust test method can be used for any DoD partner PKI whether a federal bridge partner or not. DoD Policy and business needs will determine when direct trust may be used.

3.1 High Level Direct Trust Interoperability Test Plan

With the data collected in section 1, the DoD should be able to determine which DoD environments need to be tested to ensure a basic level of interoperability. Lessons learned from this testing will be documented and provided to the DISA DoD PKE support team DoD applications that have unique configurations will be able to use these lessons learned.

Application Platforms to be tested	[Filled out in Appendix A based on Partner/Agency findings]
Windows 2003 IIS Web application – DoD PK-Enabled	
Linux Apache Web server – DoD PK-Enabled	
Outlook 2003/IE7 on Windows XP – DoD PK-Enabled	
Other – TBD (Firefox browser perhaps)	

3.2 Detailed Direct Trust Application Testing

The following procedures validate agency/partner PKI interoperability with DoD PK-enabled applications utilizing findings from section 1. If uni-directional trust is being tested, the tests below need to be performed with only one party. If bi-directional trust is being tested, the tests below need to be performed with both parties.

3.2.1 Non-DoD Root CA Self-Signed Certificate

a. Objective. To determine if a Non-DoD root CA self-signed certificate will load into a DoD PK-enabled platform's trust list.
b. Criterion. Platform shall trust the Non-DoD root CA self-signed certificate.
c. Test Procedures. Testers will invoke the functionality of the PK-enabled. Platform to trust the Non-DoD root CA self-signed certificate. Testers will:

(1) Load the Non-DoD root CA self-signed certificate.

(2) Verify that the DoD PK-enabled platform can accept the Non-DoD root CA self-signed certificate**.**

d. Criterion-related Data Requirements.

1) Non-DoD root CA self-signed certificate.
2) Configured DoD PK-enabled platform. (see below)

Windows 2003 IIS Web Server	Pass / Fail
Procedure:	
Findings /Comments:	
Linux Apache Web Server	Pass / Fail
Procedure:	
Findings/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Findings/Comments:	

3.2.2 Non-DoD Subordinate CA Certificate

a. Objective. To determine if a Non-DoD subordinate CA certificate will load into a DoD PK-enabled platform .

b. Criterion. Platform shall validate a Non-DoD subordinate CA certificate.

c. Test Procedures. Testers will:

(1) Load the Non-DoD root CA self-signed certificate into application.

(2) Load the Non-DoD subordinate CA certificate.

(3) Verify that the platform validates the Non-DoD subordinate CA certificate.

d. Criterion-related Data Requirements.

1) Non-DoD Self signed Root CA certificate.
2) Non-DoD subordinate CA certificate.
3) DoD PK-enabled platform. (see below)

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.3 Non-DoD Root CA CRL

a. Objective. To determine if a PK-enabled platform can use the Non-DoD Root CA CRL to retrieve accurate revocation information.

b. Criterion. Application shall use the Non-DoD Root CA CRL to check the status of a Non-DoD subordinate CA certificate.

c. Test Procedures. Testers will:

(1) Load the Non-DoD root CA CRL into the application.

(2) Verify that the application can use the Non-DoD Root CA CRL to check the status of a Non-DoD subordinate CA certificate. (Also performed in subsequent tests)

d. Criteria-related Data Requirements.

1) Non-DoD Root CA CRL
2) Non-DoD Subordinate CA Certificate
3) PK-enabled Web platform. (see below)

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.4 Non-DoD Subordinate CA CRL

a. Objective. To determine if a PK-enabled platform can use a Non-DoD subordinate CA CRL to retrieve accurate revocation information.

b. Criterion. Application shall use a Non-DoD subordinate CA CRL to check the status of a Non-DoD identity certificate.

c. Test Procedures. Testers will:

(1) Load a Non-DoD subordinate CA CRL into application.

(2) Verify that the application can use the Non-DoD subordinate CA CRL to check the status of a Non-DoD identity certificate. (Also performed in subsequent tests)

d. Criteria-related Data Requirements.

1) Non-DoD Subordinate CA CRL

2) Non-DoD identity certificate
3) PK-enabled Web platform. (see below)

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.5 Non-DoD Identity Certificate

a. Objective. To determine if a DoD PK-enabled Web platform can authenticate users using a Non-DoD identity certificate.

b. Criterion. Application shall use a Non-DoD identity certificate to authenticate users.

c. Test Procedures. Testers will:

(1) Load a Non-DoD identity certificate and associated prvate key into client side browser application

(2) Verify that the DoD Web Server application validates a Non-DoD identity certificate

(3) Verify that the Non-DoD client validates the DoD Web Server

d. Criterion-related Data Requirements.

1) Client loaded with Non-DoD identity certificate and associated private key
2) DoD PK-enabled Web platform. (see below)
3) DoD PK-enabled Web platform has both the DoD and Non-DoD Roots.
4) DoD PK-enabled Web platform has the DoD Web Server certificate and associated private key
5) Client loaded with Non-DoD Root

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	

XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.6 Revoked Non-DoD Identity Certificate

a. Objective. To determine if a PK-enabled Web Platform rejects a revoked Non-DoD identity certificate.

b. Criterion. Web Server shall reject a revoked Non-DoD identity certificate.

c. Test Procedures. Testers will:

(1) Load a revoked Non-DoD identity certificate and associated private key into client side browser application.

(2) Verify that the application rejects a revoked Non-DoD identity certificate.

d. Criterion-related Data Requirements.

1) Client loaded with Revoked Non-DoD identity certificate and associated private key
2) DoD PK-enabled Web server.
3) Access to current CRL from CAs in the trust path for the client certificate
4) DoD PK-enabled Web platform has both the DoD and Non-DoD Roots
5) DoD PK-enabled Web platform has the DoD Web Server certificate and associated private key
6) Client loaded with Non-DoD Root

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.7 Expired Non-DoD Identity Certificate

a. Objective. To determine if a PK-enabled Web platform rejects an expired Non-DoD identity certificate.

b. Criterion. Web Server shall reject an expired Non-DoD identity certificate.

c. Test Procedures. Testers will:

(1) Load an expired Non-DoD identity certificate and associated prvate key into client side browser application.

(2) Verify that the DoD Web Server rejects an expired Non-DoD identity certificate.

d. Criterion-related Data Requirements.

1) Client loaded with Expired Non-DoD identity certificate and associated private key.

2) DoD PK-enabled Web server. (see below)

3) DoD PK-enabled Web platform has both the DoD and Non-DoD Roots

4) DoD PK-enabled Web platform has the DoD Web Server certificate and associated private key

5) Client loaded with Non-DoD Root

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.8 Use of a valid Non-DoD Signature and Encryption Certificate

a. Objective. To determine if a DoD PK-enabled email application can receive signed and encrypted mail using the Non-DoD signature certificate. The DoD PK-enabled mail application should also be able to send encrypted email using the Non-DoD encryption certificate.

b. Criterion. The DoD PK-enabled email client shall be able to receive signed mail, decrypt incoming messages and send encrypted using a Non-DoD signing and encryption certificate.

c. Test Procedures. Testers will:

1) Send email signed and encrypted e-mail. The e-mail is signed using a Non-DoD signature certificate into the DoD PK-enabled email client.

2) Verify the signature on the e-mail.
3) Decrypt the e-mail successfully.
4) Verify that the email application can encrypt a test message with a document attachment using a Non-DoD encryption certificate.
5) Verify that the application can decrypt a test email.

d. Criterion-related Data Requirements.

1) DoD PK-enabled email.
2) Non-DoD CAs.

Windows 2003 IIS Web Application	N/A
Procedure:	
Finding/Comments:	
Linux Apache Web Application	N/A
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.9 Revoked Non-DoD Signature Certificate

a. Objective. To determine if a DoD PK-enabled email application rejects a revoked Non-DoD signature certificate.

b. Criterion. Application shall reject a revoked Non-DoD signature certificate.

c. Test Procedures. Testers will:

(1) Load a current Non-DoD CRL into DoD email application.
(2) Send email signed with a revoked Non-DoD signature certificate into the DoD PK-enabled email client.
(2) Verify that the application rejects a revoked Non-DoD signature certificate.

d. Criterion-related Data Requirements.

1) Current Non-DoD CRL.
3) DoD PK-enabled email client loaded with DoD and Non-DoD roots, and a DoD user e-mail certificates and associated private keys.

Windows 2003 IIS Web Application	N/A
Procedure:	
Finding/Comments:	
Linux Apache Web Application	N/A
Procedure:	
Finding/Comments:	

XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.10 Expired Non-DoD Signature Certificate

a. Objective. To determine if a PK-enabled e-mail application rejects an expired Non-DoD signature certificate.

b. Criterion. DoD PK-enabled email application shall reject an expired Non-DoD signature certificate.

c. Test Procedures. Testers will:

(1) Send signed email using an expired Non-DoD signing certificate to the DoD PK-enabled email application.

(2) Verify that the e-mail application rejects an expired Non-DoD signing certificate.

d. Criterion-related Data Requirements.

1) Expired Non-DoD signature certificate.

2) DoD PK-enabled e-mail client loaded with DoD and Non-DoD roots, and a DoD user e-mail certificates and associated private keys.

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.11 Non-DoD OSCP Responder (Optional)

a. Objective. Use Non-DoD OCSP responder to validate Non-DoD certificates.

b. Criterion. A DoD PK-enabled platform configured with an OCSP client shall be able to connect to a Non-DoD OCSP responder to validate Non-DoD certificates.

c. Test Procedures. Testers will:

(1) Configure DoD PK-enabled Web Server's and e-mail client's OSCP client to use Non-DoD component OCSP service.

(2) Verify that a DoD PK-enabled Web server validates a Non-DoD Web client certificate using OSCP request and response.

(3) Verify that a DoD PK-enabled email client can validate a Non-DoD user certificate using OSCP request and response.

d. Criteria-related Data Requirements.

1) Non-DoD identity certificate
2) Non-DoD signature certificate,
3) Revoked Non-DoD identity certificate,
4) Expired Non-DoD identity certificate.
5) Revoked Non-DoD identity certificate,
6) Expired Non-DoD identity certificate
7) Non-DoD OCSP Service configuration
8) DoD PK-enabled Web Server and e-mail client platforms with DoD approved OSCP client.

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.12 Non-DoD Code Signing Certificate (Optional)

a. Objective. To determine if a Non-DoD code signing certificate validates signatures on mobile code.

b. Criterion. Application shall validate signature on mobile code using a Non-DoD code signing certificate.

c. Test Procedures. Testers will:

(1) Load a Non-DoD code signing certificate into application.

(2) Validate a signature on mobile code signed by a Non-DoD code signing certificate.

d. Criterion-related Data Requirements. Non-DoD code signing certificate and Non DoD Root.

Windows 2003 IIS Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
Linux Apache Web Application	Pass / Fail
Procedure:	
Finding/Comments:	
XP/IE7/Outlook 2003 Client	Pass / Fail
Procedure:	
Finding/Comments:	

3.2.13 Device Applications (Optional) - TBD

4 Testing Cross Certification Interoperability

In the cross-certification or mesh trust model, each CA issues a certificate to each other CA that it trusts. If two CAs trust each other and issue certificates to each other. 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.

High Level Policy and Interoperability Steps prior to testing:

1. Development of proper governing documents (e.g. Memorandum Of Agreement), will require meetings between prospective PKI governing bodies.
2. Discuss how PKI operational information and issues are communicated between the partners (e.g. how new systems are advertised, how revocations are requested/handled, how certificates and revocation status are obtained by the relying parties)
3. Develop PKI Interface Specification that includes certificate profiles, methods and procedures for issuing and delivering cross-certificates, certificates and CRLs.

Test Environment Configurations:

Prior to conducting the tests, the settings indicated below must be implemented to enable correct path processing on the targeted Operating System (OS). Additionally, any applications used during the testing will need to be configured following the guidance in this section.

Microsoft OS settings (Windows 2000, XP, Server 2003)

By default, Microsoft (MS) Cryptographic Application Programming Interface (CAPI) rejects the name types not defined in the Name Constraint field. In order to facilitate RFC-3280-compliant certificate validation in regards to processing of Name Constraints, the following registry key must be set on all machines:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
SystemCertificates\Root\ProtectedRoots\Flags, Type REG_DWORD, Value 0x20
```

Microsoft Internet Explorer settings

The Microsoft Internet Explorer client will need to be configured to allow for the selection of the certificate when accessing the DoD PKI web site. To enable this feature, the following settings must be configured:

To enable certificate selection in Internet Explorer (IE), launch IE and select “Tools” then “Internet Options…”, click on the “Security” tab. Ensure “Internet” is selected, then click on “Custom Level…”. scroll down to the “Miscellaneous” section and ensure “Don’t prompt for client certificate selection when no certificates or only one certificate exists” is set to “Disable”.

Microsoft Outlook Client settings (Outlook 2003)

The Microsoft Outlook client will need to be configured to check the validation of certificates. To enable this feature, the following registry key must be set while logged on as the user conducting the test:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security]
"UseCRLChasing"=dword:00000001
```

The next step is to configure the Outlook client to utilize the correct certificates for signing e-mails. To configure the certificates in Outlook, click the "Tools" menu, then select "Options…". Next click on the "Security" tab. Under the "Encrypted email" section, ensure "Send clear text signed message when sending signed messages" is checked. Next click on the "Settings…" button to select the certificates used for signed and encrypted e-mail.

Microsoft Web Server settings (IIS 6.0)

In order to conduct the cross certified tests, a DoD PKI issued SSL certificates must be installed and configured as the Server Certificate on the Microsoft IIS server hosting the DoD PKI Web Site. This site will be configured to allow "Anonymous" authentication, "Require secure channel (SSL)", "Require 128-bit encryption" and "Require client certificate". To ensure IIS is performing certificate validation the following command must be run on the IIS server:

```
adsutil.vbs SET w3svc/NUM/CertCheckMode 0
```

(Note: *NUM* is the value of the Identifier assigned to the DoD PKI web site visible through the IIS Manager) With those configuration in place, the DoD PKI web site will require a client certificate that is trusted and validated in order to access the site.

By default, Microsoft's Internet Information Services (IIS) 6.0 does not attempt to download intermediate certificates to build a path when validating a client certificate. In order to force Authority Information Access (AIA) chasing, the following registry setting must be applied:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTPFilter\Parameters]

"ServiceDll"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,\0
0,74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,\77,0
0,33,00,73,00,73,00,6c,00,2e,00,64,00,6c,00,6c,00,00,00

"ServiceMain"="HTTPFilterServiceMain"

"CurrentMode"=dword:00000000

"CertChainCacheOnlyUrlRetrieval"=dword:00000000
```

By default, IIS 6.0 sends the client browser a 'Root Hint List' of root certificates that it is configured to trust. The client browser then allows the user to select a certificate to present for authentication. However, if the Root Hint List is present, the user can only choose a certificate that chains to one of the roots therein. The following registry settings

disable the 'Root Hint List' behavior and enable the user to present any certificate to the Web server, which in turn performs the path validation:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
]

"EventLogging"=dword:00000001

"SendTrustedIssuerList"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\DES 56/56]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\NULL]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\RC2 128/128]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\RC2 40/128]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\RC4 128/128]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\RC4 40/128]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\RC4 56/128]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Ciphers\Triple DES 168/168]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Hashes]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Hashes\MD5]
```

Linux Web Server settings (Apache)
(configuration instructions for Apache web server go here)

4.1 Manual Path Processing Testing

Path Processing Tool
In order to perform the manual path processing for a cross certified PKI, a path processing tool is used to expidite the discovery of the correct certificate path. Below is the output generated by the tool when attempting to process the cross certified path for the target PKI.

< Path Processing Tool certificate path output >

Once the correct path is discovered using the tool, use the steps below to manually process the path and record the outcome.

Target PKI Manual Testing Steps	Pass/Fail
1. Check end-entity certificate attributes (certificate 6) Open the Target PKI end-entity certificate on a Microsoft Windows platform. For steps 1.1 and 1.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
1.1. CDP: CDP(2):	
1.2. AIA: AIA(2):	
2. Test end-entity certificate attributes (certificate 6)	
2.1. Using the CDP URL(s) from step 1.1 download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
2.2. Using the AIA URL(s) from step 1.2 download the end-entity issuer certificate. This test will determine if the issuer's certificate data is available. If the requested data is unavailable, this is a failure.	
3. Check issuer certificate attributes (certificate 5) Open the issuer certificate on a Microsoft Windows platform. For steps 3.1 and 3.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
3.1. CDP: CDP(2):	
3.2. AIA: AIA(2):	
4. Test issuer certificate attributes (certificate 5)	
4.1. Using the CDP URL(s) from step 3.1 download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
4.2. Using the AIA URL(s) from step 3.2 download the end-entity issuer certificate. This test will determine if the next issuer certificate data is available. If the requested data is unavailable, this is a failure.	
5. Check next issuer certificate attributes (certificate 4) Open the next issuer certificate on a Microsoft Windows platform. For steps 5.1 and 5.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
5.1. CDP: CDP(2):	
5.2. AIA: AIA(2):	
6. Test next issuer certificate attributes (certificate 4)	
6.1. Using the CDP URL(s) from step 5.1 download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
6.2. Using the AIA URL(s) from step 5.2 download the end-entity issuer certificate. This test will determine if the next issuer certificate data is available. If the requested data is unavailable, this is a failure.	
7. Check next issuer certificate attributes (certificate 3) Open the next issuer certificate on a Microsoft Windows platform. For steps 7.1 and 7.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
7.1. CDP: CDP(2):	
7.2. AIA: AIA(2):	
8. Test next issuer certificate attributes (certificate 3)	
8.1. Using the CDP URL(s) from step 7.1 download the CRL. This test will determine if the	

certificate revocation data is available. If the requested data is unavailable, this is a failure.	
8.2. Using the AIA URL(s) from step 7.2 download the end-entity issuer certificate. This test will determine if the next issuer certificate data is available. If the requested data is unavailable, this is a failure.	
9. Check next issuer certificate attributes (certificate 2) Open the next issuer certificate on a Microsoft Windows platform. For steps 9.1 and 9.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
9.1. CDP: CDP(2):	
9.2. AIA: AIA(2):	
10. Test next issuer certificate attributes (certificate 2)	
10.1. Using the CDP URL(s) from step 9.1 download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
10.2. Using the AIA URL(s) from step 9.2 download the end-entity issuer certificate. This test will determine if the next issuer certificate data is available. If the requested data is unavailable, this is a failure.	
11. Check next issuer certificate attributes (certificate 1) Open the next issuer certificate on a Microsoft Windows platform. For steps 11.1 and 11.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
11.1. CDP: CDP(2):	
11.2. AIA: AIA(2):	
12. Test next issuer certificate attributes (certificate 1)	
12.1. Using the CDP URL from step 5.1.1. download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
12.2. Using the AIA URL from step 5.1.2. download the end-entity issuer certificate. This test will determine if the next issuer certificate data is available. If the requested data is unavailable, this is a failure.	
This process will repeat until the trust anchor certificate has been reached. In the DoD community, the trust anchor will be the DoD Interoperability Root CA-1. If the certificate path contains more than the above number of certificates, repeat the steps above until the complete certificate path has been traversed.	
***X* Check next issuer certificate attributes (certificate *X*)** Open the next issuer certificate on a Microsoft Windows platform. For steps *X*.1 and *X*.2 record the data for the attributes below. If the attribute does not exist, this is a failure.	
X.1 CDP: CDP(2):	
X.2 AIA: AIA(2):	
***Z*. Test next issuer certificate attributes (certificate *X*)**	
Z.1 Using the CDP URL(s) from step *X*.1 download the CRL. This test will determine if the certificate revocation data is available. If the requested data is unavailable, this is a failure.	
Z.1 Using the AIA URL(s) from step *X*.2 download the end-entity issuer certificate. This test will determine if the issuer's certificate data is available. If the requested data is unavailable, this is a failure.	

4.2 FBCA Cross Certified Trust Application Testing

Valid Certificate Testing Steps:

FBCA Target PKI Valid Certificate	Pass/Fail

1. Cross Certified Certificate	
1.1. Load/Trust necessary root CA certificate (e.g. DoD Interoperability Root CA-1, CCEB Roots) Application/OS is able to load/trust the necessary root CA certificate for cross certified testing **Pass/Fail Criteria:** If both 1.1.1 and 1.1.2 pass = Pass, If either 1.1.1 or 1.1.2 fail = Fail	
1.1.1. Windows XP SP2/Windows Server 2003 (IE, Outlook and IIS) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
1.1.2. Linux (Apache) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
2. Logical Access (CRL validation)	
2.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.1.1, 2.1.2, 2.1.3 and 2.1.4 pass = Pass, If 2.1.1, 2.1.2, 2.1.3 or 2.1.4 fail = Fail	
2.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.1.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
2.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.2.1, 2.2.2, 2.2.3 and 2.2.4 pass = Pass, If 2.2.1, 2.2.2, 2.2.3 or 2.2.4 fail = Fail	
2.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.2.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
3. Logical Access (OCSP validation) – Optional	
3.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.1.1, 3.1.2, 3.1.3 and 3.1.4 pass = Pass, If 3.1.1, 3.1.2, 3.1.3 or 3.1.4 fail = Fail	
3.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.1.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
3.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the	

Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.2.1, 3.2.2, 3.2.3 and 3.2.4 pass = Pass, If 3.2.1, 3.2.2, 3.2.3 or 3.2.4 fail = Fail	
3.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.2.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
4. Signed E-mail (CRL validation)	
4.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.2.1, 4.2.2 and 4.2.3 pass = Pass, If 4.2.1, 4.2.2 or 4.2.3 fail = Fail	
4.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
4.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using CRLs	
4.2.3. DoD PKI user's system validates Target PKI end-entity certificate certification path and displays the digitally signed e-mail	
4.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.4.1, 4.4.2 and 4.4.3 pass = Pass, If 4.4.1, 4.4.2 or 4.4.3 fail = Fail	
4.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
4.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using CRL	
4.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays the digitally signed e-mail	
5. Signed E-mail (OCSP validation) – Optional	
5.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.2.1, 5.2.2 and 5.2.3 pass = Pass, If 5.2.1, 5.2.2 or 5.2.3 fail = Fail	
5.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	

5.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using OCSP, where appropriate	
5.2.3. DoD PKI user's system validates Target PKI end-entity certificate via OCSP and displays the digitally signed e-mail	
5.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.4.1, 5.4.2 and 5.4.3 pass = Pass, If 5.4.1, 5.4.2 or 5.4.3 fail = Fail	
5.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
5.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using OCSP	
5.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays the digitally signed e-mail	

Revoked Certificate Testing Steps:

FBCA Target PKI Revoked Certificate	Pass/Fail
1. Cross Certified Certificate	
1.1. Load/Trust necessary root CA certificate (e.g. DoD Interoperability Root CA-1, CCEB Roots) Application/OS is able to load/trust the necessary root CA certificate for cross certified testing **Pass/Fail Criteria:** If both 1.1.1 and 1.1.2 pass = Pass, If either 1.1.1 or 1.1.2 fail = Fail	
1.1.1. Windows XP SP2/Windows Server 2003 (IE, Outlook and IIS) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
1.1.2. Linux (Apache) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
2. Logical Access (CRL validation)	
2.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.1.1, 2.1.2, 2.1.3 and 2.1.4 pass = Pass, If 2.1.1, 2.1.2, 2.1.3 or 2.1.4 fail = Fail	
2.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.1.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
2.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.2.1, 2.2.2, 2.2.3 and 2.2.4 pass = Pass, If 2.2.1, 2.2.2, 2.2.3 or 2.2.4 fail = Fail	

2.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.2.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
3. Logical Access (OCSP validation) – Optional	
3.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.1.1, 3.1.2, 3.1.3 and 3.1.4 pass = Pass, If 3.1.1, 3.1.2, 3.1.3 or 3.1.4 fail = Fail	
3.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.1.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
3.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate **Pass/Fail Criteria:** If 3.2.1, 3.2.2, 3.2.3 and 3.2.4 pass = Pass, If 3.2.1, 3.2.2, 3.2.3 or 3.2.4 fail = Fail	
3.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.2.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
4. Signed E-mail (CRL validation)	
4.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.2.1, 4.2.2 and 4.2.3 pass = Pass, If 4.2.1, 4.2.2 or 4.2.3 fail = Fail	
4.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
4.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using CRLs	
4.2.3. DoD PKI user's system validates Target PKI end-entity certificate certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
4.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	

4.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.4.1, 4.4.2 and 4.4.3 pass = Pass, If 4.4.1, 4.4.2 or 4.4.3 fail = Fail	
4.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
4.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using CRL	
4.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
5. Signed E-mail (OCSP validation) – Optional	
5.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.2.1, 5.2.2 and 5.2.3 pass = Pass, If 5.2.1, 5.2.2 or 5.2.3 fail = Fail	
5.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
5.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using OCSP, where appropriate	
5.2.3. DoD PKI user's system validates Target PKI end-entity certificate via OCSP and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
5.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.4.1, 5.4.2 and 5.4.3 pass = Pass, If 5.4.1, 5.4.2 or 5.4.3 fail = Fail	
5.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
5.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using OCSP	
5.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	

4.3 Non-FBCA Cross Certified Trust Application Testing

Valid Certificate Testing Steps:

Non-FBCA Target PKI Valid Certificates	Pass/Fail
1. Cross Certified Certificate	
1.1. Load/Trust necessary root CA certificate Application/OS is able to load/trust the necessary root CA certificate for cross certified testing **Pass/Fail Criteria:** If both 1.1.1 and 1.1.2 pass = Pass, If either 1.1.1 or 1.1.2 fail = Fail	
1.1.1. Windows XP SP2/Windows Server 2003 (IE, Outlook and IIS) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	

1.1.2. Linux (Apache) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
2. Logical Access (CRL validation)	
2.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.1.1, 2.1.2, 2.1.3 and 2.1.4 pass = Pass, If 2.1.1, 2.1.2, 2.1.3 or 2.1.4 fail = Fail	
2.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.1.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
2.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.2.1, 2.2.2, 2.2.3 and 2.2.4 pass = Pass, If 2.2.1, 2.2.2, 2.2.3 or 2.2.4 fail = Fail	
2.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.2.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
3. Logical Access (OCSP validation) – Optional	
3.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.1.1, 3.1.2, 3.1.3 and 3.1.4 pass = Pass, If 3.1.1, 3.1.2, 3.1.3 or 3.1.4 fail = Fail	
3.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.1.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
3.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.2.1, 3.2.2, 3.2.3 and 3.2.4 pass = Pass, If 3.2.1, 3.2.2, 3.2.3 or 3.2.4 fail = Fail	
3.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for	

CA certificates.	
3.2.4. DoD PKI Web Site server allows Target PKI end-entity user access to the web site	
4. Signed E-mail (CRL validation)	
4.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.2.1, 4.2.2 and 4.2.3 pass = Pass, If 4.2.1, 4.2.2 or 4.2.3 fail = Fail	
4.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
4.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using CRLs	
4.2.3. DoD PKI user's system validates Target PKI end-entity certificate certification path and displays the digitally signed e-mail	
4.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.4.1, 4.4.2 and 4.4.3 pass = Pass, If 4.4.1, 4.4.2 or 4.4.3 fail = Fail	
4.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
4.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using CRL	
4.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays the digitally signed e-mail	
5. Signed E-mail (OCSP validation) – Optional	
5.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.2.1, 5.2.2 and 5.2.3 pass = Pass, If 5.2.1, 5.2.2 or 5.2.3 fail = Fail	
5.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
5.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using OCSP, where appropriate	
5.2.3. DoD PKI user's system validates Target PKI end-entity certificate via OCSP and displays the digitally signed e-mail	
5.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent	

from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.4.1, 5.4.2 and 5.4.3 pass = Pass, If 5.4.1, 5.4.2 or 5.4.3 fail = Fail	
5.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
5.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using OCSP	
5.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays the digitally signed e-mail	

Revoked Certificate Testing Steps:

Non-FBCA Target PKI Revoked Certificates	Pass/Fail
1. Cross Certified Certificate	
1.1. Load/Trust necessary root CA certificate Application/OS is able to load/trust the necessary root CA certificate for cross certified testing **Pass/Fail Criteria:** If both 1.1.1 and 1.1.2 pass = Pass, If either 1.1.1 or 1.1.2 fail = Fail	
1.1.1. Windows XP SP2/Windows Server 2003 (IE, Outlook and IIS) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
1.1.2. Linux (Apache) Install the Target PKI Cross Certified Root CA Self-Signed Certificate. Ensure the certificate is loaded into the proper certificate store.	
2. Logical Access (CRL validation)	
2.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.1.1, 2.1.2, 2.1.3 and 2.1.4 pass = Pass, If 2.1.1, 2.1.2, 2.1.3 or 2.1.4 fail = Fail	
2.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.1.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
2.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 2.2.1, 2.2.2, 2.2.3 and 2.2.4 pass = Pass, If 2.2.1, 2.2.2, 2.2.3 or 2.2.4 fail = Fail	
2.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
2.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
2.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280	
2.2.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
3. Logical Access (OCSP validation) – Optional	
3.1. Access DoD PKI Web Site (IIS) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.1.1, 3.1.2, 3.1.3 and 3.1.4 pass = Pass, If 3.1.1, 3.1.2, 3.1.3 or 3.1.4 fail = Fail	

3.1.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.1.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.1.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.1.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
3.2. Access DoD PKI Web Site (Apache) via Target PKI end-entity certificate In this test the Target PKI end-entity user will attempt to access the DoD PKI Web Site via the Target PKI end-entity certificate. On the client, launch IE and attempt to access the DoD PKI Web Site. **Pass/Fail Criteria:** If 3.2.1, 3.2.2, 3.2.3 and 3.2.4 pass = Pass, If 3.2.1, 3.2.2, 3.2.3 or 3.2.4 fail = Fail	
3.2.1. Target PKI end-entity user is able to select their certificate in the Certificate Selection dialog box	
3.2.2. DoD PKI Web Site server developed the Target PKI subscriber certification path via path processing	
3.2.3. DoD PKI Web Site server validates Target PKI subscriber certification path, including revocation checking and extension constraints processing per RFC 5280. Note: It is possible that the Target PKI provides OCSP responses only of end certificates and not for CA certificates.	
3.2.4. DoD PKI Web Site server denies Target PKI end-entity user access to the web site	
4. Signed E-mail (CRL validation)	
4.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.2.1, 4.2.2 and 4.2.3 pass = Pass, If 4.2.1, 4.2.2 or 4.2.3 fail = Fail	
4.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
4.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using CRLs	
4.2.3. DoD PKI user's system validates Target PKI end-entity certificate certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
4.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
4.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 4.4.1, 4.4.2 and 4.4.3 pass = Pass, If 4.4.1, 4.4.2 or 4.4.3 fail = Fail	
4.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
4.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using CRL	
4.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
5. Signed E-mail (OCSP validation) – Optional	

5.1. Target PKI user sends signed e-mail to DoD PKI user In this test the Target PKI user will attempt to send a digitally signed e-mail to the DoD PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the DoD PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.2. DoD PKI user is able to open signed e-mail sent from Target PKI user In this test the DoD PKI user will attempt to open and validate a digitally signed e-mail sent from the Target PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.2.1, 5.2.2 and 5.2.3 pass = Pass, If 5.2.1, 5.2.2 or 5.2.3 fail = Fail	
5.2.1. DoD PKI user's system is able to develop the Target PKI subscriber certification path	
5.2.2. DoD PKI user's system checks the revocation status of the certificates in the certification path using OCSP, where appropriate	
5.2.3. DoD PKI user's system validates Target PKI end-entity certificate via OCSP and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	
5.3. DoD PKI user sends signed e-mail to Target PKI user In this test the DoD PKI user will attempt to send a digitally signed e-mail to the Target PKI user via Outlook. On the client, launch Outlook and create a new e-mail message to be sent to the Target PKI user. Click the icon to digitally sign the e-mail, then click send. **Pass/Fail Criteria:** Signed e-mail is successfully sent = Pass, Signed e-mail is unsuccessfully sent = Fail	
5.4. Target PKI user is able to open signed e-mail sent from DoD PKI user In this test the Target PKI user will attempt to open and validate a digitally signed e-mail sent from the DoD PKI user. On the client, launch Outlook and attempt to open the digitally signed e-mail. **Pass/Fail Criteria:** If 5.4.1, 5.4.2 and 5.4.3 pass = Pass, If 5.4.1, 5.4.2 or 5.4.3 fail = Fail	
5.4.1. Target PKI user's system is able to develop the DoD PKI subscriber certification path	
5.4.2. Target PKI user's system checks the revocation status of the certificates in the certification path using OCSP	
5.4.3. Target PKI user's system validates DoD PKI end-entity certification path and displays a message indicating that the certificate used to digitally sign the e-mail is revoked	

5 Summary

This section will provide a summary of the testing results.

6 Glossary of Terms

Authentication	A security measure designed to establish the identity of originator of a transmission or message, or a means of verifying an individual's identity. An example is client-side authentication to a Web Server to facilitate Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
Certificate Revocation Lists (CRLs)	A list published and maintained by each Certification Authority (CA) listing all of its revoked certificates that are still within their validity dates. When a CA revokes a certificate, the CA administrator (CAA) prepares a new CRL and posts it to the directory server (DS). (1)
Direct Trust	Trust done by directly trusting the CA as apposed to Cross Certified Trust where the trust is created by trusting a cross certified CA..
Federal Bridge Certification Authority (FBCA)	Supports interoperability among PKI domains with disparate policies in a peer to peer fashion, and the Common Policy Root CA, which manages a hierarchical PKI.
Online Certificate Status Protocol (OCSP)	Internet protocol used for obtaining the revocation status of an X.509 digital certificate created as an alternative to CRLs. OCSP responses are much smaller, require less bandwidth and can be deployed to provide revocation status as fresh or fresher (even near real-time) than CRL. Note: In the DoD PKI, OCSP response has about the same freshness as the CRL since OCSP responses are derived from published CRLs.
Path Validation	Ability to discover and validate all of the certification paths at the Rudimentary and Basic levels within the Directory based PKI architecture from the end entity certificate to the trust anchor. Relying parties are obligated to ensure all certificates within the trusted path are trusted by the DoD PKI and/or DoD Approved PKIs. This is defined in RFC 5280.
Root Certification Authority	A self-signed certificate. A root certificate is part of a public key infrastructure scheme. A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is the top-most certificate of the tree. All certificates below the root certificate inherit the trustworthiness of the root certificate.
DoD	Agencies, Services, COCOMs …
Homeland Security Presidential Directive (HSPD-12)	This standard, signed by the President on August 27, 2004, established the requirements for a common identification standard for identification credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. This standard also defines the authentication mechanisms offering varying degrees of security. (4)
Personal Identity Verification (PIV)	
Cross Certificate Pair	An attribute of a PKI directory schema that contains the issuedByThisCA and issuedToThisCA elements which is used to store all, except self-issued certificate issued to a CA or a subset of

	certificates issued from this CA
issuedByThisCA	An optional element of the of the CrossCertificatePair attribute of a CA's crossCertificatePair attribute that contains a subset of certificates issued from a CA
issuedToThisCA	An element of the of the CrossCertificatePair attribute of a CA's crossCertificatePair attribute that contains a subset of certificates issuedToThisCA
Component certificate	
OIDs	Object Identifier
Certificate Policy (CP)	The Certificate Policy (CP) governs the operation of a Public Key Infrastructure (PKI), consisting of products and services that provide and manage X.509 certificates for public key cryptography. (2)
Certification Practice Statement (CPS)	A document that establishes the proofing requirements for identifying a private key owner that must be satisfied before creating a certificate. (1)
SCVP	Server-based Certificate Validation Protocol
Lightweight Directory Access Protocol (LDAP)	An application protocol for querying and modifying directory services running over TCP/IP. (3)
ISS	
OWA	Outlook Web Access
Hypertext transfer Protocol (HTTP)	A communications protocol for the transfer of information on the intranet and the World Wide Web. (3)
Certification Authority (CA)	The PKI entity that digitally signs certificates and Certificate Revocation Lists. The CA generates some certificate information but is mainly responsible for collecting information from authorized sources and correctly entering that information into a certificate. The CA digitally signs a subscriber's certificate when authorized by the appropriate trusted person. It must include only valid and appropriate information and maintain evidence that due diligence was exercised in confirming the information. (1)
Assurance Levels	The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys (and thereby the private keys). The processes and controls employed in the operation of the PKI, the methods used to protect the private keys, and the strength of the cryptographic algorithms used all serve a role in determining the assurance level of the PKI. There are three levels of assurance: Standard, Medium, and Medium Hardware. The applicability of the different assurance levels is determined by the value of the information being protected and the threat environment. Standard assurance is intended for applications handling unclassified information of low value in a Minimally or Moderately Protected Environment. Medium assurance is intended for applications handling unclassified medium value information in Moderately Protected Environments, unclassified high value information in Highly Protected Environments, and discretionary access control of classified information in Highly Protected Environments. Medium Hardware assurance is intended for all applications operating in environments appropriate for Medium Assurance but which require a higher degree

	of assurance and technical non-repudiation and for applications performing contracting and contract modifications. (1)
Virtual Private Network (VPN)	Protected information system link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the impression of a dedicated line. (1)
Subordinate Certification Authority	A certificate authority created from and signed by a root certificate. In the case of DoD, Subordinate or (Intermediate) CAs issue certificates to users and devices.
Agency PKI	
Agency CA	
Bi-lateral Trust	
Bridge	Tests utilizing cross certificates established with the FBCA or other partner PKI to validate end-to-end interoperability.
Certificate	A data file that binds the identity of an entity to a public key. Certificates contain the user's identification and a signature from an issuing authority. Also referred to as a digital certificate, an X.509 certificate, or a public key certificate. (1)
Code Signing	
Code Signing Certificate	
CRL Distribution Point (CRLDP)	A CRLDP allows revocation information within a single CA domain to be posted in multiple CRLs. (5)
Cross Certificate	
Cross Certified Federal Bridge	
Cryptography	An encoding scheme, also known as asymmetric cryptography, that uses separate keys for encryption and decryption. The two keys are generated at the same time and have two properties. First, whichever key is used to encrypt the data, the other key must be used to decrypt it. Second, knowledge of one of the keys, called the public key, is not sufficient to determine the other key, called the private key. Public key cryptography is a critical element of the Department of Defense net centric goals as well as Information Assurance (IA) Defense-in-Depth technical strategy. (1)
Digital Signature	An electronic code that can be attached to data that identifies the signer of the data and associates the signer with the data being signed. Digital signatures allow the recipient to verify the identity of the signer and that the data has not been modified. (1)
Direct Trust	A direct trust interoperability sharing roots and revocation information to validate certificate trusts without taking advantage of interoperability through bridge mechanisms.
DoD External Certification Authority (ECA)	A mechanism for external entities and organizations to obtain certificates that have been approved by the DoD as meeting the required assurance levels for binding the identity of the named certificate holder to the public key contained in the certificate. ECA certificates can be issued for a validity period of up to 3 years. (1)
Department of	Refers to the core framework and services that provide for the

Defense Public Key Infrastructure (DoD PKI)	generation, production, distribution, control, revocation, recovery, and tracking of digital certificates and their corresponding public and private keys for DoD entities. (1)
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called cipher to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. (3)
Encryption Certificate	
Expired Certificate	
Expired Site	
External PKI Partner	
FBCA Partner	
Foreign, Allied or Coalition Partner PKI	
Good Certificate	
Good Site	
Identity Certificate	
Mobile Code	Software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. (3)
Non-FBCA Partner	
Non-Federal Agency PKI	
Online Certificate Status Protocol (OCSP) Client	
Online Certificate Status Protocol (OCSP) Responder	
Online Certificate Status Protocol (OCSP) Response	
Partner Certification Authority (CA)	
Partner PKI	
Partnering Agency	
Public Key Cryptography	An encoding scheme, also known as asymmetric cryptography, that uses separate keys for encryption and decryption. The two keys are generated at the same time and have two properties. First, whichever key is used to encrypt the data, the other key must be used to decrypt it. Second, knowledge of one of the keys, called the public key, is not sufficient to determine the other key, called the private key. Public key cryptography is a critical element of the Department of Defense net centric goals as well as Information Assurance (IA) Defense-in-Depth technical strategy. (1)

Public Key (PK)-Enabled Application	Applications that use both public key cryptography and the PKI to provide public key-based security services. These applications directly interface to the cryptography to sign data, verify signatures, and encrypt and decrypt data. However, PK-enabled applications are not considered to be part of the PKI itself. (1)
Public Key Infrastructure	Refer to DoD PKI above.
Relying Party	Entities that use digital certificates to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding of the subscriber's name to the public key contained in the certificate. Relying parties may themselves also be subscribers. (1)
Revoked Certificate	
Revoked Site	
Root Certificate	
Root Certification Authority (CA)	The Root CA is the trust anchor for all certificates issued by the PKI. It generates and signs its own certificate. It also signs certificates for Subordinate CAs. (1)
Self-signed Certificate	
Signature Certificate	
Subordinate Agency	
Subordinate Certification Authority	Subordinate CAs issue certificates and CRLs for users, including human and non-human subscribers and relying parties. Subordinate CAs interface with RAs for issuance and revocation. (1)
Subordinate Partner	
Trust Agency	
Trust Partner	
Uni-Directional Trust	
US Federal Agency PKI	

Footnote of Referenced Documents
(1) United States Department of Defense Coalition Public Key Infrastructure Concept of Operations, December 7, 2007 Version 1
(2) Certificate Policy for the Coalition Public Key Infrastructure, 4 May 2008, Draft Version 0.8
(3) Wikipedia (www.wikipedia.org)
(4) FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
(5) Understanding Public-Key Infrastructure Concepts, Standards, and Deployment Considerations, authored by Carlisle Adams and Steve Lloyd, 1999

Appendix A – Partner/Agency Specific Information

1) Certain interoperability requirement questions must be answered to begin testing:
   - Is interoperability needed for access to Web servers?
   - Is interoperability needed for secure e-mail? If yes, which security services are required: signature, encryption, or both.
   - Is interoperability needed for encrypted files?
   - Is interoperability needed for other uses (smart card logon, desktops and laptops sign-on, code signing, VPNs, Personal Digital Assistants (PDAs), etc)?
   - Which protocols will be used for access to PKI objects such as certificates, CRLs, OCSP requests and responses, etc.?

STEP 1: Identify Usage (or Planned Usage) of PKI within Agency	
DoD Use	DoS Use (To be filled out before JITC test)
• Email Signature (send/ receive) • Email Encryption (send/receive) • Web server client authentication • Mobile Devices (BlackBerry S/MIME)	• Email Signature (send/ receive) • Email Encryption (send/receive) • Web server client authentication • TBD [Section filled out for DoS]

**STEP 1 Provides DoD list of common capabilities that could be considered for testing.

Based on the mission needs and capabilities, the partners should identify applications and systems that need to be tested.

2) Which common platforms need interoperability testing?

STEP 2: Identify Common Platforms between DoD and DoS		
Use – Application	DoD	DoS
Web application – IIS Windows 2003	X	X
Web application – Apache Linux	X	X
Web application – Other	X	
Email sign/encrypt – Outlook XP	X	

Email sign/encrypt – Outlook 2003	X	X
Email sign/encrypt – Outlook 2007		
Email sign/encrypt – Mozilla Thunderbird		
Email sign/encrypt – Novell Mail		
Email sign/encrypt – Lotus Notes		
Email sign/encrypt – Web mail		
Email sign/encrypt – Other		
Remote Access VPN – Cisco	X	
Remote Access VPN – Microsoft		
Remote Access VPN – Other		
Mobile Application BlackBerry - S/MIME	X	
Mobile Application Windows Mobile		
Mobile Application Other		
Network Logon – XP	X	X
Network Logon – Vista		
Network Logon – Linux/Mac		
Code Signing		
		[Section filled out for DoS]

**STEP 2 identifies common platforms that could be considered for interoperability. Also provides shareable lessons learned with partnering agencies PKI implementations.

3) Architecture Information the agency or partner needs to provide are:

    1) What is the Hierarchy and quantity of CA certificates?
    2) Are the CAs signed by the Federal Bridge?
    3) How many Certificate Revocation Lists (CRLs) and what are their sizes?
    4) How often are the CRL(s) generated?
    5) How long are the CRL(s) valid for?
    6) What is the maximum time the agency has to revoke known-compromised certificates?
    7) Does the Agency/Partner provide an Online Certificate Status Protocol (OCSP) service?
    8) How often are the CAs added/removed in the infrastructure?
    9) What are the Agency/Partner CAs intended use, what type of certificates are issued (e.g. email signature, email encryption, Web server, Windows domain controller, etc.)?
    10) What protocols are used to access the CA and CRL repository (e.g. HTTP, HTTPS, LDAP, LDAPS, etc.)?
    11) Is there a repository for user certificates to obtain the public keys (e.g. email integration to an LDAP, email integration to HTTP, use of a LDAP proxy, etc.)?
    12) Does the Agency/Partner run a test PKI environment? If so is it accessible to the internet?
    13) Which certificate policy assurance levels will be tested?
    14) Will HSPD-12 PIV compliance certificates be tested?

15) What key sizes and algorithms are you signing certificates with?
16) What Certificate Management Software are you using?

**STEP 3 provides the DoD test team the ability to determine what components of the Agency/Partners PKI are to be tested using a direct trust vice cross certificate test methods. These answers will also identify what external access is available to the DoD for testing.

STEP 3: Answers to DoS Architecture	
1	5 CAs in the Department of State (DoS) infrastructure. 2 Root and 3 Subordinate CAs. 1 Root and 1 Subordinate CAs to be retired (FADS), New Root High Assurance (HA) Active Directory (AD) has 2 Subordinate CAs for issuing credentials AD HA CA and PIV CA.
2	New CAs AD and PIV are not yet signed by Fed bridge (in the queue). FADS Root was signed by Fed bridge. (No longer issuing User Certificates from FADS ??? – DOS confirm)
3	Largest CRL size is 70 KB (AD HA CA) – All CRLs are available from LDAP and HTTP.
4	Unknown
5	Effective 25 Hours
6	No OCSP
7	AD Root issued June 23, 2004 and valid for 30 years, AD HA CA issued June 30, 2004 and valid for 10 years PIV CA issued Aug 31, 2006 and valid for 6 years Not aware of other CAs.
8	AD HA CA and PIV issue user certificates, AD HA CA issues certificates for Sign and Encrypt mail, also can be used for SCL and Web authentication
9	CRLs available from LDAP or HTTP, Root CAs are accessible via LDAP (Softerra). Add links
10	External directory is not available for User Public keys.
11	Has a Test lab that resembles AD Root and AD subordinate CAs – It is not accessible to DoD from internet. CA, CRLs and user certificates have to be emailed or hand carried.
12	Certificates are at three assurance levels (Basic, Medium and High) ???
13	Unknown
[Section filled out for DoS]	

With the data collected in section 1, the DoD should be able to determine which DoD environments need to be tested to ensure a basic level of interoperability. Lessons learned from this testing will be documented as provided to the DISA DoD PKE support team

Specific DoD applications that have unique configurations will be able to used these lessons learned to configure their applications (per policy).

Application Platforms to be tested	[based on DoS findings]
Windows 2003 IIS Web application – DoD PK-Enabled	
Linux Apache Web server – DoD PK-Enabled	
Outlook 2003/IE7 on Windows XP – DoD PK-Enabled	
Other – TBD (Firefox browser perhaps)	

Appendix B – DoD Environment

DoD PKI consists of two distinct environments, each employing a tiered hierarchy of specialized root CAs designed for interoperability with other PKIs , one or more root CAs, subordinate and intermediate certificate authorities, and end entities. The environments are:

- Production DoD PKI Environment - The production PKI consists of many systems located on both Unclassified (NIPRNET) and Secret (SIPRNET) networks.
    - The current root CA (cn=DoD Root CA 2, ou=PKI, ou=DoD, o=U.S. Government, c=US) is an off-line system located and operated in a physically secure location. This single root CA is used to sign subordinate and intermediate CAs on both network classifications. This root CA private key is RSA 2048.
    - The older root CA (cn = DoD CLASS 3 Root CA, ou = PKI, ou = DoD, o = U.S. Government, c = US) is collocated with the new system, but is currently in maintenance mode until all of its subordinates have expired (09/15/2009). This root CA private key is RSA 1024.
    - Subordinate CAs are regularly deployed for technical refreshes and new capabilities, using identical technologies located at two Defense Enterprise Computing Centers (DECCs) in Chambersburg, PA and Denver, CO. Note: Oklahoma City will eventually replace the Denver location. Some of these CAs issue only token-based certificates for the DoD Common Access Card (CAC) and others issue software user certificates, server certificates, and CAC certificates.
    - Intermediate (Non-Person Entity) CA systems issue CA certificates to C/S/A Microsoft CAs, whose sole function is to issue only domain controller certificates within a Microsoft Active Directory environment.
    - A specialized interoperability root CA ([cn=US DoD CCEB Interoperability Root CA 1, ou=PKI, o=U.S. Government, c=US] cn=DoD Interoperability Root CA 1, ou=PKI, o=U.S. Government, c=US) is used to facilitate interoperability with CCEB nations. This root CA private key is RSA 2048. Note that this Root is not currently operational.
    - A specialized interoperability root CA (cn=DoD Interoperability Root CA 1, ou=PKI, o=U.S. Government, c=US) is used to facilitate interoperability with partners of the FBCA. This root CA private key is RSA 2048. This root CA has issued certificates to both the Root 2 and Root 1 described previously.
    - The Robust Certificate Validation System (RCVS) is a high-availability OCSP responder service (http://ocsp.disa.mil) which hosts all CRLs associated with the DoD PKI. Currently, the RCVS system uses a self-signed OCSP Responder certificate, however DoD plans to migrate to a delegated trust model (DTM) in the near future.
    - Full CRLs and CA certificates are available for download via a secure DISA Web server (https://crl.gds.disa.mil).

  - A robust, searchable directory service known as *DoD 411* provides user certificate information via a secure DISA Web page (https://dod411.gds.disa.mil).

- Test DoD PKI Environment - JITC is located at Ft. Huachuca, AZ and runs the test environment for the DoD PKI. This environment is online and identical to unclassified production system minus the redundancy See http://jitc.fhu.disa.mil/pki/ for more information and test URLs.

Appendix C – Federal Bridge Certification Authority

The Federal Bridge Certification Authority (FBCA) and the DoD Interoperability Root CA-1 have issued cross certificates to each other. FBCA has bi-directional cross certificates with Non-Federal Agency PKIs and U.S. Federal Agency Partner PKIs.

Below is a list of the current Organizations Cross-Certified with the FBCA obtained from the Federal PKI Architecture site (see http://www.cio.gov/fpkia/crosscert.htm for the most current list):

Cross-Certified Entity	FBCA Assurance Level	Cross-Certified Date
NASA	Medium	September 18, 2002
Department of Defense	Medium	* September 18, 2002
Department of the Treasury	High	September 18, 2002
	Medium	September 18, 2002
	Medium Hardware	** August 14, 2007
Department of State	High	January 21, 2004
State of Illinois	Medium	January 21, 2004
	Basic	** March 8, 2005
	Medium	February 11, 2004
DoD External CA	Medium	* February 8, 2005
ACES/ORC, Inc.	Medium	** February 8, 2005
US Patent and Trademark Office	Medium	June 1, 2005
Department of Homeland Security	Medium	June 1, 2005
	High	June 1, 2005
	Basic	June 1, 2005
	Basic	** October 4, 2006
Government Printing Office	Medium	** December 13, 2005
	Medium Hardware	** February 12, 2008
	High	** December 15, 2005
CertiPath Bridge	Medium	** May 9, 2006
	Medium CBP	** May 9, 2006
	Medium Hardware	** May 9, 2006
	Medium Hardware CBP	** May 9, 2006
	Medium	* June 13, 2006
United States Postal Service	Medium	** October 20, 2006
	Medium Hardware	** February 12, 2008
MIT Lincoln Laboratory	Medium	** July 10, 2007
	Medium Hardware	** July 10, 2007
	Medium Hardware	** July 10, 2007
SAFE Bridge	Medium CBP	** February 12, 2008
	Medium Hardware CBP	** February 12, 2008

* FBCA issued cross-certificate allowing one-way trust
** This was the date the Federal PKI Policy Authority voted on and approved issuing a FBCA cross-certificate

Last Updated: 3 March 2008

Appendix D – Acronyms

Acronym	Definition
ACES	Access Certificates for Electronic Services
AD	Active Directory
AIA	Authority Information Access
ARL	Authority Revocation List
CA	Certification Authority
CAPI	Cryptographic Application Programming Interface
CCA	Cross Certificate Agreement
CCEB	Combined Communications – Electronics Board
CN	Common Name
CO	Colorado
COCOM	Combatant Command
CP	Certificate Policy
CPB	CertiPath Bridge
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution List
C/S/A	Commands, Services and Agencies
DECC	Defense Enterprise Computing Centers
DISA	Defense Information Systems Agency
DN	Distinguished Name
DNS	Domain Name Service
DoD	Department of Defense
DOS	Department of State
DTM	Delegated Trust Model
EIWG	External Interoperability Working Group
FADS	???
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
HA	High Assurance
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IE	Internet Explorer
IIS	Internet Information Services
JITC	Joint Interoperability Test Command
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
MIT	Massachusetts Institute of Technology
MOA	Memorandum Of Agreement

MS	Microsoft
NASA	National Aeronautics and Space Administration
NIPRNet	Non-Secure Internet Protocol Router Network
NSA	National Security Agency
ORC	Operational Research Consultants
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Pennsylvania
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 (certificates)
PIV	Personal Identity Verification
PMO	Program Management Office
POC	Point Of Contact
RCVS	Robust Certificate Validation System
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman
SAFE	Signature and Authentication For Everyone
SCVP	Server-Based Certificate Validation Protocol
SHA	Secure Hash Algorithm
SIA	Subject Information Access
SIPRNet	Secret Internet Protocol Router Network
S/MIME	Secure/Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Universal Resource Locator
US	United States
VPN	Virtual Private Network