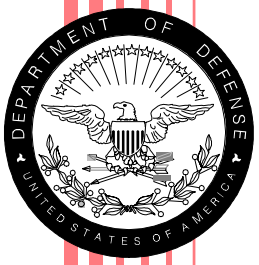


DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE INTEROPERABILITY MASTER TEST PLAN VERSION 1.2

NOVEMBER 2001

DEPARTMENT OF DEFENSE
PUBLIC KEY INFRASTRUCTURE
INTEROPERABILITY
MASTER TEST PLAN
VERSION 1.2

NOVEMBER 2001

Submitted by: **Ross Romeo**
LTC, USA
Chief
Networks and Integration Branch

Approved by: _____

LESLIE F. CLAUDIO
Chief
Networks, Transmission and Intelligence Division

Prepared Under the Direction of:

Cammie Webster
Joint Interoperability Test Command
Fort Huachuca, Arizona 85613-7020

(This page intentionally left blank.)

EXECUTIVE SUMMARY

Many programs supporting Department of Defense (DOD) missions require security services, such as authentication, confidentiality, non-repudiation, and access control. To address these security requirements, DOD developed a Public Key Infrastructure (PKI) to provide products and services that enhance security of networked information systems and facilitate digital signatures. Four distinct security services offered by PKI are authentication, confidentiality, integrity, and non-repudiation.

Recognizing the need to verify that vendor applications are interoperable with the DOD PKI, the National Security Agency (NSA) tasked the Joint Interoperability Test Command (JITC) to test these applications.

This master test plan contains testing procedures for use when evaluating a Public Key-Enabled application's interoperability with the DOD PKI. The tests deemed necessary for an accurate and comprehensive evaluation will be augmented with application specific procedures. The testing outlined in this document will be performed and the results analyzed to determine if an application meets the interoperability requirements for the DOD PKI and will be certified by the JITC accordingly.

JITC will test (APPLICATION) by using certificates and Certificate Revocation Lists from the JITC PKI Test Certificate Authority and Directory Server. JITC will determine the extent (APPLICATION) interoperates with the DOD PKI in accordance with the Defense Information Systems Agency and NSA document, "Department of Defense Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," version 1.0, 13 July 2000. JITC will use the Cygnacom Solutions document, "Conformance Testing of Relying Party Client Certificate Path Processing Logic," version1.06, 6 November 2000, for the Path Processing and Development, and Certificate Status portion of the testing.

If applicable to the application, testing will include: generating, retrieving, importing, and exporting keys and certificates; storing keys and related certificates; storing trust points; verifying communication protocols; checking certificate status; retrieving certificates from the archive; path development and processing; verifying application configuration; and reviewing documentation.

JITC will test (APPLICATION) at its PKI laboratory at Fort Huachuca, Arizona, and/or at the vendor’s site, as applicable.

(This page intentionally left blank.)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

APPENDICES

SYSTEM FUNCTIONAL DESCRIPTION

a. Many programs supporting Department of Defense (DOD) missions require security services, such as authentication, confidentiality, non-repudiation, and access control. To address these security requirements, DOD developed a Public Key Infrastructure (PKI) to provide products and services that enhance security of networked information systems and facilitate digital signatures. Four distinct security services PKI offers are authentication, confidentiality, integrity, and non-repudiation. Key components of the PKI include hardware and software that:

- issue and manage X.509 certificates.
- identify and bind the client to a unique public/private key pair for cryptographic purposes.
- provide directory services for storage and archiving of certificates and certificate revocation lists.

b. Applications use PKI certificates to authenticate users and public key encryption to safeguard data during transmission. Applications store the certificates, including the private key, and must perform "relying" party certificate path processing to verify that the requested certificates are valid.

TEST BACKGROUND

DOD requested that (APPLICATION) be tested to verify it performed according to DOD requirements. The interoperability test requirements come from the Defense Information Systems Agency and National Security Agency document, "Department of Defense Class 3 Public Key Infrastructure (PKI) Public Key-Enabled (PKE) Application Requirements," version 1.0, 13 July 2000. [Reference I-1a in Appendix I] This document will hereafter be referred to as the DOD PKE Application Requirements document.

TEST PURPOSE

To determine the extent (APPLICATION) meets the requirements to interoperate with the DOD PKI.

REQUIREMENTS

Table 7, found in the DOD PKE Application Requirements document summarizes the interoperability requirements for DOD PKE Applications. Most interoperability requirements are derived from this table. Figure 1 shows a matrix with the types of requirements and the section in the DOD PKE Application Requirements document where related information can be found.

Figure 1. Requirements Matrix

SECTION	SECTION IN REQUIREMENTS DOCUMENT
Generating Key Pairs	4.3.1.1
Retrieving Certificates	4.3.2.3
Importing and Exporting Keys and Certificates	4.3.1.5
Storing Trust Points	4.3.1.3
Verifying Communication Protocols	4.3.2.1
Checking Certificates Status	4.3.2.4
Retrieving Certificates and CRLs from the Archive	4.3.2.5
Path Development and Processing	4.3.4
Application Configuration	4.4
Application Documentation	4.5

SCOPE

The Joint Interoperability Test Command (JITC) will assess the interoperability of (APPLICATION) with the DOD PKI using the JITC test Certificate Authority (CA) workstation and the Directory Server (DS). Testing to verify that (APPLICATION) meets the criteria for Path Development and Processing, and Checking Certificate Status will be determined through the use of tests found in the Cygnacom Solutions document, "Conformance Testing of Relying Party Client Certificate Path Processing Logic," 6 November 2000 [Reference I-2 in Appendix I, Section 3.] Testing will be performed onsite or at the JITC depending on the configuration and portability of (APPLICATION). Our test team will determine the location based on information gathered on (APPLICATION) or through direct contact with (APPLICATION) personnel. The JITC PKI Application Assessment Worksheet is used to assist the team in gathering information about an application. For more information and a copy of the Application Assessment Worksheet see Appendix G.

OBJECTIVES AND METHODOLOGY

The test will exercise (APPLICATION)'s ability to use client certificates issued from the JITC servers. JITC will verify that users with certificates are properly recognized. JITC will introduce valid, revoked, and expired certificates to verify (APPLICATION) complies with DOD PKI interoperability standards. JITC will conduct the test at its PKI laboratory at Fort Huachuca, Arizona, and/or at the vendor's site, as applicable.

Testers have four methods for verifying (APPLICATION) compliance to requirements: Analysis, Demonstration, Inspection, or Test. (See Table I-1, Application Verification Methods.) The method used to verify each criterion will be determined by the PKI test engineer.

Table 1. Application Verification Methods

METHOD	DEFINITION
Analysis	The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpolation, or extrapolation of test results.
Demonstration	The operation of the application, or a function of the application, that relies on observable functional operation not requiring the use of instrumentation or special test equipment.
Inspection	The visual examination of application components, documentation, etc.
Test	The operation of the application, or part of the application, using instrumentation or special test equipment to collect data for later analysis.

PRESENTATION OF RESULTS AND ANALYSIS PROCEDURES

Analysts will examine the Pass/Fail status of each test event to determine the extent (APPLICATION) complies with the requirements for each section. Analysts will then characterize (APPLICATION)'s performance and the results will be recorded in the test report.

(This page intentionally left blank.)

APPENDIX A

ACRONYMS

CA	Certificate Authority
CRL	Certificate Revocation List
DISA	Defense Information Systems Agency
DOD	Department of Defense
DS	Directory Server
DSA	Digital Signature Algorithm
HTTP	Hypertext Transmission Protocol
HTTPS	Hypertext Transmission Protocol over Secure Sockets Layer
JITC	Joint Interoperability Test Command
KEA	Key Exchange Algorithm
KRM	Key Recovery Manager
LRA	Local Registration Authority
LDAP	Lightweight Directory Access Protocol
NIPRNet	Unclassified by Sensitive Internet Protocol Router Network
NSA	National Security Agency
OSC	Online Status Check
OSCR	Online Status Check Responder
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PMO	Program Management Office
RA	Registration Authority
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm

(This page intentionally left blank.)

APPENDIX B

TEST CRITERIA, PROCEDURES, AND DATA REQUIRED

TABLE OF CONTENTS

GENERAL TEST INFORMATION

Test Procedures

a. Test Conduct. The testers will develop detailed test events based on methods developed for each of the appropriate criterion contained in the applicable sections. Testers will develop the detailed test events on their appropriate data collection form found in Appendix C. The testers will then execute each test event on the data collection form. The testers will determine a Pass/Fail status for each criterion. Test results for each test event will be recorded on the data collection form.

b. Data Collection. Testers will record the Pass/Fail status of each function on the data collection forms in Appendix C.

Supplemental Test Data

a. Test dates, location, and type of testing.

b. System hardware and operating systems for test workstations.

c. Internet communication link between the test workstations and the JITC PKI test lab.

d. Software versions for all applications.

e. Test certificates used (reference C-1 in Appendix D).

f. Test data file used.

Presentation of Results. The test report will present the Pass/Fail test results for this section and a conclusion in narrative text and in a table similar to Table C-1 in Appendix C.

Analysis and Discussion. Analysts will examine the Pass/Fail status of each test event to determine the extent (APPLICATION) complies with the requirements for this section. Analysts will then characterize (APPLICATION)'s performance and the results will be recorded in the test report.

1 GENERATING KEY PAIRS

1.1 Objective. To determine the extent (APPLICATION) uses prescribed methods to create DOD PKI key pairs and certificates for individuals. **Note:** This section applies to key pairs whose public key will be contained in a Department of Defense (DOD) Public Key Infrastructure (PKI) issued certificate and does not apply to key pairs whose public key will not be contained in a DOD PKI issued certificate.

1.2 Criteria

a. Subscriber Keys. (APPLICATION) shall generate keys, request new certificates, and obtain new certificates through interaction with the DOD PKI. [Reference I-1a in Appendix I, table 7, page 36.]

b. Generating Key Pairs. (APPLICATION) shall generate key pairs using one of the following algorithms: Rivest, Shamir, and Adleman (RSA), Digital Signature Algorithm (DSA), or Key Exchange Algorithm (KEA). [Reference I-1a in Appendix I, paragraph 4.3.1.1, page 21.]

c. Private Encryption Keys to DOD Key Recovery Manager (KRM). (APPLICATION) shall provide the private keys generated for actual or possible encryption use to the DOD KRM. [Reference I-1a in Appendix I, paragraph 4.3.1.1, page 22.]

1.3 Test Procedures

a. Requesting and Obtaining New Certificates. Ensure that (APPLICATION):

(1) requested a new certificate for a subscriber.

(2) sent the request to the Certificate Authority (CA).

(3) obtained a new certificate for a subscriber.

b. Generating Key Pairs. Verification of the algorithm (APPLICATION) uses to generate a certificate.

c. Private Encryption Keys to DOD KRM. Ensure that (APPLICATION):

(1) generated an encryption key.

(2) sent the encryption key to the KRM.

1.4 Criteria Related Data Requirements

a. Subscriber Keys. Generated key and new certificate.

b. Generating Key Pairs. Algorithm used.

c. Private Encryption Keys to DOD KRM. Generated encryption key.

2 RETRIEVING CERTIFICATES

2.1 Objective. To determine the extent (APPLICATION) follows approved DOD PKI procedures for retrieving new certificates.

2.2 Criterion. (APPLICATION) shall request and accept certificates from the DOD PKI unless the application provides alternative means. [Reference I-1a in Appendix I, paragraph 4.3.2.3, page 25.]

2.3 Test Procedures. Ensure that (APPLICATION):

a. requested a test certificate from the DOD PKI.

b. retrieved the test certificate.

2.4 Criteria Related Data Requirements. Retrieved certificate.

3 IMPORTING AND EXPORTING KEYS AND CERTIFICATES

3.1 Objective. To determine to what extent (APPLICATION) imports and exports DOD PKI keys and certificates.

3.2 Criteria

a. Importing Keys and Certificates. (APPLICATION) shall import keys associated with standard certificates for individuals. [Reference I-1a in Appendix I, table 7, page 36.]

b. Certificate Type. (APPLICATION) shall import at least one set of keys and certificates for each certificate type supported. [Reference I-1a in Appendix I, table 7, page 36.]

c. Exporting Keys and Certificates. (APPLICATION) shall export keys and certificates. [Reference I-1a in Appendix I, table 7, page 36.]

3.3 Test Procedures

a. Importing Keys and Certificates. Ensure that (APPLICATION) imported a key from the DOD CA.

b. Certificate Type. Ensure that (APPLICATION) imported one certificate for each certificate type supported.

c. Exporting Keys and Certificates. Ensure that (APPLICATION) correctly exported a key and certificate to a file.

3.4 Criteria Related Data Requirements

a. Importing Keys and Certificates. Imported key.

b. Certificate Type. Imported key and certificate for each type supported.

c. Exporting Keys and Certificates. Exported file.

4 STORING TRUST POINTS

4.1 Objective. To determine the extent (APPLICATION) stores DOD PKI trust points.

4.2 Criterion. (APPLICATION) shall store DOD PKI trust points. [Reference I-1a in Appendix I, table 7, page 36.]

4.3 Test Procedures. Ensure that (APPLICATION) stored a DOD PKI trust point in its trust point list.

4.4 Criteria Related Data Requirements. Stored DOD PKI trust point.

5 VERIFYING COMMUNICATION PROTOCOLS

5.1 Objective. To determine the extent (APPLICATION) uses the correct communication protocols to communicate with the DOD PKI.

5.2 Criterion. (APPLICATION) shall communicate with the DOD PKI using Lightweight Directory Access Protocol (LDAP) and, as necessary, Hypertext Transmission Protocol (HTTP) and Hypertext Transmission Protocol over Secure Sockets Layer (HTTPS). [Reference I-1a in Appendix I, paragraphs 4.3.2.1, page 24 and Reference I-1b in Appendix I, Section 4, page 27.]

5.3 Test Procedures. Ensure that (APPLICATION):

a. transmitted data using the LDAP protocol.

b. transmitted data using the HTTP protocol if applicable.

c. transmitted data using the HTTPS protocol if applicable.

5.4 Criteria Related Data Requirements. Data Transmission

6 CHECKING CERTIFICATE STATUS

6.1 Objective. To determine the extent (APPLICATION) resolves the status of DOD PKI certificates.

6.2 Criteria

a. Certificate Status. (APPLICATION) shall request and accept certificate status information. **Note:** Applications must be capable of requesting and accepting information regarding the status of certificates upon which the application relies. Applications may use Online Status Checks (OSCs) to check certificate status when the DOD PKI has operational Online Status Check Responders (OSCRs). [Reference I-1a in Appendix I, paragraph 4.3.2.4, page 25.]

(1) Retrieving Certificate Revocation Lists (CRLs). (APPLICATION) shall check certificate status using CRLs. [Reference I-1a in Appendix I, paragraph 4.3.2.4.1, page 25.]

(2) OSCR. (APPLICATION) shall retrieve an OSC response. [Reference I-1a in Appendix I, paragraph 4.3.2.4.2, page 26.]

b. All Needed CRLs. (APPLICATION) shall obtain all needed CRLs. [Reference I-1a in Appendix I, table 7, page 37.]

c. Response. (APPLICATION) shall respond appropriately to valid and revoked certificates. [Reference I-1a in Appendix I, table 7, page 37.]

6.3 Test Procedures. Testers will verify that (APPLICATION) meets the criteria for this section by using the revocation status-related tests found in "Conformance Testing of Relying Party Client Certificate Path Processing Logic". [Reference I-2 in Appendix I, Section 4.] The testers will execute each test event on the data collection form found in Appendix C. A Pass/Fail status for each test event will be determined by the testers and recorded on the data collection form as such. If (APPLICATION) passes all tests listed below, the requirements are met for criterion 7.2.a, criterion 7.2.a.1, criterion 7.2.b, and criterion 7.2.c. **Note:** The OSC Responder tests (criteria 7.2.a.2) will not be tested until the DOD PKI has operational OSCRs. Testers will ensure that (APPLICATION):

a. used CRLs as the revocation status mechanism. [Reference I-2 in Appendix I, assertion AS:RL.01.]

b. verified that the signature on each CRL in the certification path uses the same public key that was used to sign the certificates. [Reference I-2 in Appendix I, assertion AS:RL.02.]

c. verified that the issuer name in the certificate matches the issuer name in

the CRL. [Reference I-2 in Appendix I, assertion AS:RL.03.]

d. rejected the path if any certificate in the certificate path has been revoked. [Reference I-2 in Appendix I, assertion AS:RL.04.]

e. rejected the path if any certificate in the certificate path has been revoked regardless of whether there are unrecognized critical *crlEntryExtensions* present in the CRL. [Reference I-2 in Appendix I, assertion AS:RL.05.]

f. rejected the path if any certificate in the certificate path has been revoked regardless of whether there are unrecognized critical *crlExtensions* present in the CRL. [Reference I-2 in Appendix I, assertion AS:RL.06.]

g. considered a CRL invalid if the *nextUpdate* time in the certificate is earlier than the current time. [Reference I-2 in Appendix I, assertion AS:RL.07.]

h. ensured that the CRL does not contain the *deltaCRLIndicator* extension. [Reference I-2 in Appendix I, assertion AS:RL.08.]

i. ensured that the CRL does not contain the *issuingDistributionPoint* extension. [Reference I-2 in Appendix I, assertion AS:RL.09.]

6.4 Criteria Related Data Requirements. The expected results for tests outlined in this section can be found on the Checking Certificate Status Data Collection Form found in Appendix C.

7 RETRIEVING CERTIFICATES AND CRLs FROM THE ARCHIVE

7.1 Objective. To determine the extent (APPLICATION) retrieves old certificates and CRLs from the DOD PKI archive. **Note:** The DOD PKI does not currently have operational archive capabilities.

7.2 Criteria

a. Old certificates and CRLs. (APPLICATION) shall accept needed old certificates and CRLs. [Reference I-1a in Appendix I, paragraph 4.3.2.5, page 26.]

b. Encryption Key Recovery. (APPLICATION) shall recover an encryption key provided by the DOD PKI KRM. [Reference I-1a in Appendix I, table 7, page 36.]

7.3 Test Procedures

a. Old certificates and CRLs. Ensure that (APPLICATION):

(1) requested an old certificate from the DOD PKI archive.

(2) retrieved an old certificate from the DOD PKI archive.

(3) requested an old CRL from the DOD PKI archive.

(4) retrieved an old CRL from the DOD PKI archive.

b. Encryption Key Recovery. Ensure that (APPLICATION) recovered an encryption key from the DOD PKI KRM.

7.4 Criteria Related Data Requirements

a. Old certificates and CRLs. Retrieved old certificate and CRL.

b. Encryption Key Recovery. Recovered encryption key.

8 PATH DEVELOPMENT AND PROCESSING

8.1 Objective. To determine the extent (APPLICATION) develops a sequence of DOD PKI certificates and CRLs that relate a given end-entity to a trust point using path processing.

8.2 Criterion. (APPLICATION) shall process and develop a path of certificates and CRLs that relate a given end-entity to a trust point using path processing. [Reference I-1a in Appendix I, Section 4.3.4, page 29.]

8.3 Test Procedures. Testers will verify that (APPLICATION) meets the criterion for this section by using the Path Development and Processing related tests found in "Conformance Testing of Relying Party Client Certificate Path Processing Logic". [Reference I-2 in Appendix I, Section 3.] The testers will execute each test event on the data collection form found in Appendix C. A Pass/Fail status for each test event will be determined by the testers and recorded on the data collection form as such. Testers will ensure that (APPLICATION):

a. verified the digital signatures on each certificate in the certification path using the superior public key. [Reference I-2 in Appendix I, assertion AS:CP.01.]

b. ensured that the notBefore time of each certificate in the certification path was earlier than the current time. [Reference I-2 in Appendix I, assertion AS:CP.02.]

c. ensured that the notAfter time of each certificate in the certification path was later than the current time. [Reference I-2 in Appendix I, assertion AS:CP.03.]

d. checked that names chain correctly. [Reference I-2 in Appendix I, assertion AS:CP.04.]

e. retrieved valid revocation data for each certificate in the certificate path. [Reference I-2 in Appendix I, assertion AS:CP.05.]

f. rejected the certificate path if any certificate in the certificate path has been revoked. [Reference I-2 in Appendix I, assertion AS:CP.06.]

g. ensured that the basic constraints extension is present in every intermediate certificate in the certification path. [Reference I-2 in Appendix I, assertion AS:IC.01.]

h. ensured that every intermediate certificate in the certification path must have the basic constraints extension present, and the *cA* component set to true. [Reference I-2 in Appendix I, assertion AS:IC.02.]

i. rejected a certificate path if any intermediate certificate in the certification path violates path length constraints presented in the *pathLenConstraint* field of the basic constraints extension in a superior certificate. [Reference I-2 in Appendix I, assertion AS:IC.03.]

j. ensured that the certificate has the *cA* component of the basic constraints extension present and set to TRUE when it encounters an intermediate certificate in the certificate path that has the key usage extension present and marked critical with the *keyCertSign* bit set to true and the basic constraints present. [Reference I-2 in Appendix I, assertion AS:IC.04.]

k. ensured that every intermediate certificate in the certificate path that has the key usage extension present has the *keyCertSign* bit set to TRUE. [Reference I-2 in Appendix I, assertion AS:IC.05.]

l. ensured that every intermediate certificate in the certificate path containing the public key of a CRL signer which has the key usage extension present has the *cRLSign* bit set to TRUE. [Reference I-2 in Appendix I, assertion AS:IC.06.]

8.4 Criteria Related Data Requirements. The expected results for tests outlined in this section can be found on the Path Development and Processing Data Collection Form found in Appendix C.

9 APPLICATION CONFIGURATION

9.1 Objective. To determine the extent (APPLICATION) is capable of being configured for use with the DOD PKI.

9.2 Criterion. (APPLICATION) shall be capable of being configured to operate with the DOD PKI. [Reference I-1a in Appendix I, table 7, page 38.]

9.3 Test Procedures. Ensure that (APPLICATION):

a. was configured to operate with the DOD PKI.

b. identified the operating conditions required of (APPLICATION)'s operating environment.

c. identified all necessary conditions and dependencies for it to securely perform its functions.

d. was configured for secure operation in its intended environments.

e. provided automated features that satisfy DOD Minimum Requirements. When not possible, ensure that (APPLICATION) provided well documented and easily followed procedures and assurance that administrator and user training addressed the procedures to manually configure the application.

f. was capable of being configured to operate with only DOD PKI trust points.

9.4 Criteria Related Data Requirements

a. User and administrator manuals.

b. DOD PKI trust point.

10 APPLICATION DOCUMENTATION

10.1 Objective. To determine the extent (APPLICATION) includes user and administrator manuals on the use of the application.

10.2 Criterion.

a. User and Administrator Manuals. (APPLICATION) shall include user and administrator manuals (or electronic equivalents) that are adequate to instruct personnel unfamiliar with public key cryptography on the proper and secure configuration and use of the application. [Reference I-1a in Appendix I, paragraph 4.5, page 33.]

b. Configuration to Interoperate. (APPLICATION) shall include configuration instructions to interoperate with the DOD PKI. [Reference I-1a in Appendix I, paragraph 4.5, page 33.]

c. Responsibilities as PKI Users. (APPLICATION) documentation shall instruct users and administrators regarding their responsibilities as PKI users. [Reference I-1a in Appendix I, paragraph 4.5, page 33.]

10.3 Test Procedures

a. User and Administrator Manuals. Ensure that (APPLICATION) included user and administrator manuals (or electronic equivalents) that are adequate to instruct personnel unfamiliar with public key cryptography on the proper and secure configuration and use of the application. These instructions shall cover:

(1) Installing DOD PKI trust points.

(2) Removing non-DOD PKI trust points.

(3) Generating a key pair and requesting and obtaining certificates or importing existing keys and certificates.

(4) Installing Uniform Resource Indicators for DOD PKI services, such as obtaining certificates for other entities and performing status checking.

(5) Selecting encryption algorithms. Selections should indicate algorithms that must be used, may be used, or cannot be used.

(6) Configuring the application for Secure Sockets Layer access to the DOD PKI, if necessary.

b. Configuration to Interoperate. Ensure that (APPLICATION) included configuration instructions for it to interoperate with the DOD PKI.

c. Responsibilities as PKI Users. Ensure that (APPLICATION) documentation instructed users and administrators regarding their responsibilities as PKI users. The documents shall include:

(1) Instructions on technical and procedural measures to protect the private key against compromise and misuse.

(2) Guidance on the actions to take for a suspected key compromise (e.g., a token has been lost.)

10.4 Criteria Related Data Requirements. Visual inspection of the manuals and a demonstration that the application performs as documented when the configuration guidance is followed.

APPENDIX C

DATA COLLECTION FORMS

Form Name **Page**

Table C-1. (APPLICATION) Interoperability Test Results

CRITERIA	RESULT
GENERATING KEY PAIRS	
Subscriber Keys	
Generating Key Pairs	
Private Encryption Keys to Department of Defense (DOD) Key Recovery Manager	
RETRIEVING CERTIFICATES	
Retrieving Certificates	
IMPORTING AND EXPORTING KEYS AND CERTIFICATES	
Importing Keys and Certificates	
Certificate Type	
Exporting Keys and Certificates	
STORING TRUST POINTS	
Storing Trust Points	
VERIFYING COMMUNICATION PROTOCOLS	
Verifying Communication Protocols	
CHECKING CERTIFICATE STATUS	
Checking Certificate Status	
RETRIEVING CERTIFICATES AND CERTIFICATE REVOCATION LISTS (CRLs) FROM THE ARCHIVE	
Old certificates and CRLs	
Encryption Key Recovery	
PATH DEVELOPMENT AND PROCESSING	
Path Development and Processing	
APPLICATION CONFIGURATION	
Application Configuration	
APPLICATION DOCUMENTATION	
User and Administrator Manuals	
Configuration to Interoperate	
Responsibilities as Public Key Infrastructure (PKI) users	

DATA COLLECTION FORM – DETAILED INFORMATION FOR (APPLICATION) TESTING

Application Name: _____ Version: _____
Vendor: _____

Testers (Data Collectors/Operators): _____ _____ _____

Location(s) of testing: _____ Dates of testing: _____ to _____

COMMON TEST DATA

Hardware and operating system for all systems:

Software versions and patches for all applications:

Additional test equipment required:

IP addresses used:

Certificates used (Include certificate passwords):

Files used:

Passwords Used:

Comments/Notes:

Diagram of Test Network:

DATA COLLECTION FORM – GENERATING KEY PAIRS

Criterion: 1.2a Subscriber Keys.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – GENERATING KEY PAIRS

Criterion: 1.2b Generating Key Pairs.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – GENERATING KEY PAIRS

Criterion: 1.2c Private Encryption Keys to the DOD KRM.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – RETRIEVING CERTIFICATES

Criterion: 2.2 Retrieving Certificates.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – IMPORTING AND EXPORTING CERTIFICATES

Criterion: 3.2a Importing Keys and Certificates.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – IMPORTING AND EXPORTING CERTIFICATES

Criterion: 3.2b Certificate Type.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – IMPORTING AND EXPORTING CERTIFICATES

Criterion: 3.2c Exporting Keys and Certificates.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – STORING TRUST POINTS

Criterion: 4.2 Storing Trust Points.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – VERIFYING COMMUNICATION PROTOCOLS

Criterion: 5.2 Verifying Communication Protocols.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – CHECKING CERTIFICATE STATUS

Criterion: 6.2 Certificate Status.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

DESIGNATOR	EXPECTED VALIDATION RESULT	ACTUAL RESULT	COMMENTS	PASS or FAIL
		LEVEL 1 TESTS		
RL.02.01	FAILURE			
RL.03.01	FAILURE			
RL.05.01	FAILURE			
RL.06.01	FAILURE			
RL.07.01	FAILURE			
RL.08.01	FAILURE			
RL.09.01	FAILURE			
		LEVEL 2 TESTS		
RL.03.02	FAILURE			
RL.03.03	SUCESSFUL			
RL.05.02	FAILURE			
RL.06.02	FAILURE			
RL.07.02	FAILURE			
RL.07.03	SUCESSFUL			

DATA COLLECTION FORM – RETRIEVING CERTIFICATES AND CRLs FROM THE ARCHIVE

Criterion: 7.2a Retrieving Certificates and CRLs from the Archive.	**Result:** □ PASS □ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – RETRIEVING CERTIFICATES AND CRLs FROM THE ARCHIVE

Criterion: 7.2b Encryption Key Recovery.	**Result:** □ PASS □ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – PATH DEVELOPMENT AND PROCESSING

Criterion: 8.2 Path Development and Processing.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

DESIGNATOR	EXPECTED VALIDATION RESULT	ACTUAL RESULT	COMMENTS	PASS or FAIL
		LEVEL 1 TESTS		
CP.01.01	SUCESSFUL			
CP.01.02	FAILURE			
CP.01.03	FAILURE			
CP.02.01	SUCESSFUL			
CP.02.02	FAILURE			
CP.03.01	FAILURE			
CP.03.04	SUCESSFUL			
CP.04.01	FAILURE			
CP.04.02	FAILURE			
CP.04.03	SUCESSFUL			
CP.05.01	FAILURE			
CP.06.01	FAILURE			
CP.06.02	FAILURE			
IC.01.01	FAILURE			
IC.02.03	FAILURE			
IC.04.01	SUCESSFUL			
IC.05.02	FAILURE			
IC.06.02	FAILURE			

DATA COLLECTION FORM – PATH DEVELOPMENT AND PROCESSING (continued)

DESIGNATOR	EXPECTED VALIDATION RESULT	ACTUAL RESULT	COMMENTS	PASS or FAIL
PP.01.01	CONFIG DEPENDANT			
PP.01.02	CONFIG DEPENDANT			
PP.01.05	CONFIG DEPENDANT			
PP.01.06	CONFIG DEPENDANT			
PP.01.08	CONFIG DEPENDANT			
PP.06.02	CONFIG DEPENDANT			
PP.06.03	FAILURE			
PP.06.04	CONFIG DEPENDANT			
PP.06.05	FAILURE			
PL.01.01	FAILURE			
PL.01.04	SUCESSFUL			
LEVEL 2 TESTS				
CP.02.03	FAILURE			
CP.02.04	SUCESSFUL			
CP.02.05	FAILURE			
CP.03.02	FAILURE			
CP.03.03	FAILURE			
IC.02.01	FAILURE			
IC.05.01	FAILURE			
IC.06.01	FAILURE			
PP.01.03	CONFIG DEPENDANT			
PP.01.04	CONFIG DEPENDANT			
PP.01.07	CONFIG DEPENDANT			
PP.01.09	CONFIG DEPENDANT			
PL.01.02	FAILURE			
PL.01.03	SUCESSFUL			
PL.01.05	FAILURE			
PL.01.06	FAILURE			
PL.01.08	FAILURE			
PL.01.09	SUCESSFUL			
PL.01.10	SUCESSFUL			

DATA COLLECTION FORM – APPLICATION CONFIGURATION

Criterion: 9.2 Application Configuration.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:
Equipment used for test:
Certificates used (if applicable):
Files used (if applicable):
Anomalies:
Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS
1	Ensure (APPLICATION) is configured to operate with the DOD PKI.		
	Notes:		
2	Ensure (APPLICATION) has identified the operating conditions required of it's operating environment.		
	Notes:		
3	Ensure (APPLICATION) has identified all necessary conditions and dependencies for it to securely perform its functions.		
	Notes:		
4	Ensure (APPLICATION) is configured for secure operation in its intended environments.		
	Notes:		
5	Ensure (APPLICATION) provided automated features that satisfy DOD Minimum Requirements. When not possible, ensure that (APPLICATION) provided well documented and easily followed procedures and assurance that administrator and user training addressed the procedures to manually configure the application.		
	Notes:		
6	Ensure (APPLICATION) is capable of being configured to operate with only DOD PKI trust points.		
	Notes:		

DATA COLLECTION FORM – APPLICATION DOCUMENTATION

Criterion: 10.2a User and Administrator Manuals.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

Test Information:

Ensure that (APPLICATION) included user and administrator manuals (or electronic equivalents) that are adequate to instruct personnel unfamiliar with public key cryptography on the proper and secure configuration and use of the application.

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS
1	Instructions cover installing DOD PKI trust points.		
2	Instructions cover removing non-DOD PKI trust points.		
3	Instructions cover generating a key pair and requesting and obtaining certificates or importing existing keys and certificates.		
4	Instructions cover installing Uniform Resource Indicators for DOD PKI services, such as obtaining certificates for other entities and performing status checking.		
5	Instructions cover selecting encryption algorithms. Selections should indicate algorithms that must be used, may be used, or cannot be used.		
6	Instructions cover configuring the application for Secure Sockets Layer access to the DOD PKI, if necessary.		

DATA COLLECTION FORM – APPLICATION DOCUMENTATION

Criterion: 10.2b Configuration to Interoperate.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS

DATA COLLECTION FORM – APPLICATION DOCUMENTATION

Criterion: 10.2c Responsibilities as PKI users.	**Result:** ☐ PASS ☐ FAIL

Application name: _____ Tester(s) (Data Collector/Operator): _____ _____

Location: _____ Date: _____

SPECIFIC TEST DATA

Software used for test:

Equipment used for test:

Certificates used (if applicable):

Files used (if applicable):

Anomalies:

Results/Notes:

Test Information:

Ensure that (APPLICATION) documentation instructs users and administrators regarding their responsibilities as PKI users.

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS
1	(APPLICATION) documents include instructions on technical and procedural measures to protect the private key against compromise and misuse.		
2	(APPLICATION) documents include guidance on the actions to take for a suspected key compromise (e.g., a token has been lost.)		

DAILY TEST STATUS REPORT **DATE: __ / __ / ____**

Application Name: _____ Version: _____

Testers (Data Collectors/Operators): _____ _____ _____

Location(s) of testing: _____

Tests completed today:

Expected Tests to be completed tomorrow:

Anomalies:

Comments/Notes:

Report Information: Report Completed By: _____ Date: __ / __ / ____ Time: _____

EXAMPLE DETAILED INFORMATION FOR APPLICATION TESTING DATA COLLECTION FORM

Application Name: (APPLICATION) **Version:** 1.0
Vendor: PKI 123 Inc

Testers (Data Collectors/Operators): John Doe, Mike Doe
Location(s) of testing: JITC/Fort Huachuca, AZ Dates of testing: Jan 01, 2001 to Jan 14, 2001

COMMON TEST DATA

Hardware and operating system for all systems:
2 – Micron Pentium III 866 MHz, 256M RAM, Windows NT Workstation 4.0 with Service Pack 6a

Software versions and patches for all applications:
Netscape 4.76 Complete Install (128-Bit Encryption)
Internet Explorer 5.5 Complete

Additional test equipment required:
None

IP addresses used:
10.10.10.10
10.10.10.11

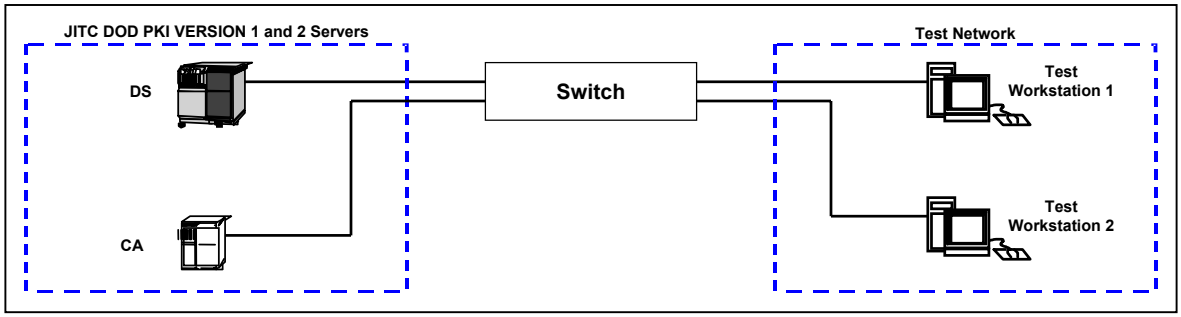
Certificates used (Include certificate passwords):
Path Processing Suite of Certificates (Password: *password*)
RA Cert 1, LRA Cert 2, Test Cert 7 (Password: *password*)

Files used:
test1.doc to test55.doc

Passwords Used:
Netscape Security: *5rE0QiPOd#* Profile: *default*
Windows NT: Login: *pkitest1* Password: Ne7#20)wLL

Comments/Notes:

Diagram of Test Network:



EXAMPLE DATA COLLECTION FORM

Criterion: 4.2. Storing Trust Points.	**Result:** ☒PASS ☐FAIL

Application name: (APPLICATION) Tester(s) (Data Collector/Operator): John Doe Mike Doe

Location: JITC/Fort Huachuca, AZ Date: Jan 02, 2001

SPECIFIC TEST DATA

Software used for test:
Netscape 4.76

Equipment used for test:
Test Workstation 1 and 2

Certificates used (if applicable):
JITC root CA certificate
Identity certificate 1

Files used (if applicable):
Test1.doc

Anomalies:

Results/Notes:

EVENT	TEST EVENT	DATA COLLECTOR ACTION	RESULTS
1	Install the JITC root CA certificate into the Netscape certificate trust point list.	Verify that the certificate is installed in the Netscape certificate trust point list.	**PASS**
2	Use (APPLICATION) and create a certificate profile for the JITC root CA certificate.	Verify that (APPLICATION) created a certificate profile that uses the JITC root CA certificate.	**PASS**
3	Use (APPLICATION) to add a digital signature to a test data file using a test identity certificate issued by the JITC root CA.	Verify that the digital signature on the test data file is trusted.	**PASS**
4	Remove trust for the JITC root CA certificate	Verify that the digital signature on the test data file is not trusted.	**PASS**

EXAMPLE DAILY TEST STATUS REPORT **DATE: 01 / 02 / 2001**

Application Name: (APPLICATION) **Version: 1.0**

Testers (Data Collectors/Operators): John Doe Mike Doe

Location(s) of testing: JITC/Fort Huachuca. AZ

Tests completed today:
Criteria 1.2a, Criteria 1.2b, Criteria 1.2c, Criteria 1.2d and Criteria 5.2.b.

Expected Tests to be completed tomorrow:
Criteria 3.2a, Criteria 3.2b and Criteria 3.2c.

Anomalies:
None

Comments/Notes:
Testing is on schedule and running smooth as planned.

Report Information: Report Completed By: John Doe **Date:** 01 / 02 / 2001 **Time:** 1630

(This page intentionally left blank.)

APPENDIX D

TEST CERTIFICATE PROFILES

D-1 Department of Defense (DOD) Certificate Profiles

a. DOD Public Key Infrastructure (PKI) Root Certificate Profile

Field	Critical Flag	Value	Comments
Certificate			
TbsCertificate			Fields to be signed.
Version		2	Integer Value of "2" for Version 3 certificate.
SerialNumber			
CertificateSerialNumber		1	
Signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
Algorithm		1:2:840:113549:1:1:5	Secure Hash Algorithm (SHA)-1 WithRSAEncryption
Parameters			(not populated)
Issuer			
Name		cn= DOD CLASS 3 Root CA, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the issuer of the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	
Validity			
NotBefore			
Time			
UtcTime			
UTCTime		980101120100Z	January 1, 1998, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
NotAfter			
Time			
UtcTime			
UTCTime		480101120100Z	January 1, 2048, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
Subject			
Name		cn=User1-CP.01.01, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the owner of the certificate.
RDNSequence			
RelativeDistinguishedName			

DOD Public Key Infrastructure (PKI) Root Certificate Profile (continued)

Field	Critical Flag	Value	Comments
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	
SubjectPublicKeyInfo			
Algorithm			
AlgorithmIdentifier			Public key algorithm used.
Algorithm		1:2:840:113549:1:1:1	RSA Encryption
parameters			(not populated)
subjectPublicKey		BIT STRING	Contains the subject public key
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	TRUE		this extension absent unless otherwise specified
cA		BOOLEAN	
pathLenConstraint		INTEGER	
keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		1	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		no policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		test-policy-1	id-test-certificate-policy-1
policyConstraints	FALSE		this extension absent unless otherwise specified
requireExplicitPolicy			
SkipCerts		INTEGER	
inhibitPolicyMapping			
SkipCerts		INTEGER	
algorithmIdentifier			
AlgorithmIdentifier			
algorithm		1:2:840:113549:1:1:5	SHA-1WithRSAEncryption
parameters			
encrypted			signature calculated

b. DOD PKI Identity Certificate Profile

Field	Critical Flag	Value	Comments
Certificate			
TbsCertificate			Fields to be signed.
Version		2	Integer Value of "2" for Version 3 certificate.
SerialNumber			
CertificateSerialNumber		1	
Signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
Algorithm		1:2:840:113549:1:1:5	SHA-1WithRSAEncryption
Parameters			(not populated)
Issuer			
Name		cn= DOD CLASS 3 Root CA, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the issuer of the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	
Validity			
NotBefore			
Time			
UtcTime			
UTCTime		980101120100Z	January 1, 1998, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
NotAfter			
Time			
UtcTime			
UTCTime		480101120100Z	January 1, 2048, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
Subject			
Name		cn=User1-CP.01.01, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the owner of the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	

DOD PKI Identity Certificate Profile (continued)

Field	Critical Flag	Value	Comments
SubjectPublicKeyInfo			
Algorithm			
AlgorithmIdentifier			Public key algorithm used.
Algorithm		1:2:840:113549:1:1:1	RSA Encryption
parameters			(not populated)
subjectPublicKey		BIT STRING	Contains the subject public key
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	TRUE		this extension absent unless otherwise specified
cA		BOOLEAN	
pathLenConstraint		INTEGER	
keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		1	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		no policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		test-policy-1	id-test-certificate-policy-1
policyConstraints	FALSE		this extension absent unless otherwise specified
requireExplicitPolicy			
SkipCerts		INTEGER	
inhibitPolicyMapping			
SkipCerts		INTEGER	
algorithmIdentifier			
AlgorithmIdentifier			
algorithm		1:2:840:113549:1:1:5	SHA-1WithRSAEncryption
parameters			
encrypted			signature calculated

c. DOD PKI E-mail Certificate Profile

Field	Critical Flag	Value	Comments
Certificate			
TbsCertificate			Fields to be signed.
Version		2	Integer Value of "2" for Version 3 certificate.
SerialNumber			
CertificateSerialNumber		1	
Signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
Algorithm		1:2:840:113549:1:1:5	SHA-1WithRSAEncryption
Parameters			(not populated)
Issuer			
Name		cn= DOD CLASS 3 Root CA, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the issuer of the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	
Validity			
NotBefore			
Time			
UtcTime			
UTCTime		980101120100Z	January 1, 1998, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
NotAfter			
Time			
UtcTime			
UTCTime		480101120100Z	January 1, 2048, 12:01:00 GMT
GeneralTime			
GeneralizedTime			Use for dates after 2049
Subject			
Name		cn=User1-CP.01.01, ou=Testing, ou=DOD, o=U.S. Government, c=US	X.500 Distinguished name of the owner of the certificate.
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	Reference X.520
AttributeValue		printableString	
SubjectPublicKeyInfo			
Algorithm			
AlgorithmIdentifier			Public key algorithm used.
Algorithm		1:2:840:113549:1:1:1	RSA Encryption
parameters			(not populated)
subjectPublicKey		BIT STRING	Contains the subject public key

DOD PKI E-mail Certificate Profile (continued)

Field	Critical Flag	Value	Comments
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	TRUE		this extension absent unless otherwise specified
cA		BOOLEAN	
pathLenConstraint		INTEGER	
keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		1	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		no policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		test-policy-1	id-test-certificate-policy-1
policyConstraints	FALSE		this extension absent unless otherwise specified
requireExplicitPolicy			
SkipCerts		INTEGER	
inhibitPolicyMapping			
SkipCerts		INTEGER	
algorithmIdentifier			
AlgorithmIdentifier			
algorithm		1:2:840:113549:1:1:5	SHA-1WithRSAEncryption
parameters			
encrypted			signature calculated

APPENDIX E

TEST RESOURCES

E-1 TEST SITES AND FACILITIES. Joint Interoperability Test Command (JITC) will test (APPLICATION) using the JITC Public Key Infrastructure (PKI) Test Certificate Authority and Directory Server at the JITC PKI laboratory at Fort Huachuca, Arizona, and/or at vendors site as applicable.

E-2 TEST EQUIPMENT/NETWORKS. (Test equipment and/or networks will vary depending on the application.) Figure D-1 depicts a Typical Test Configuration.

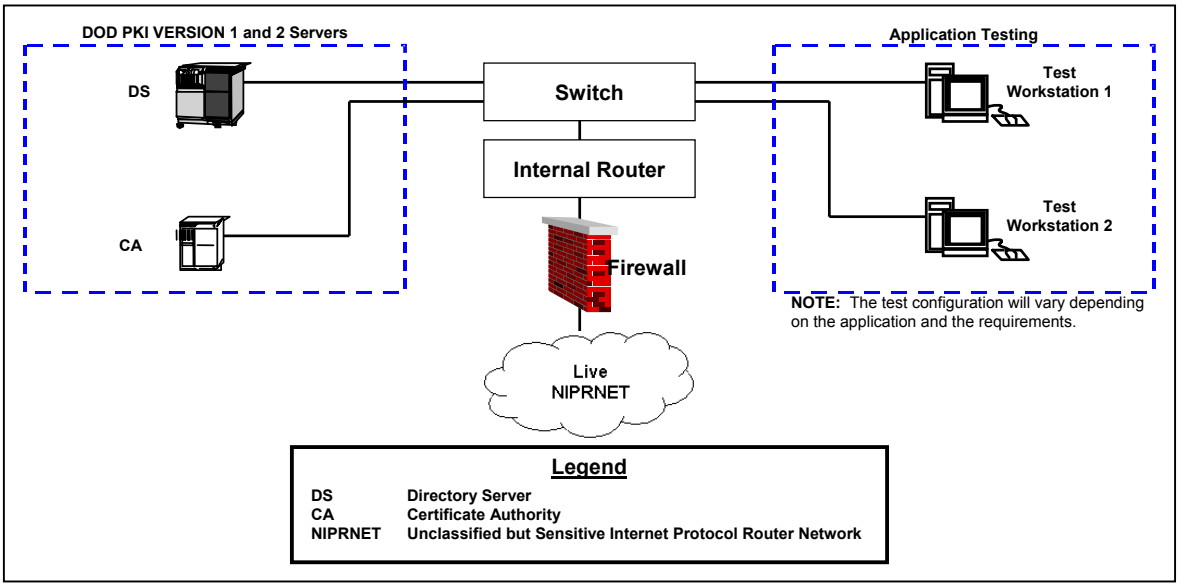


Figure E-1. Typical Test Configuration

E-3 REQUIREMENTS. JITC will determine the extent (APPLICATION) interoperates with the Department of Defense PKI in accordance with the Defense Information Systems Agency and the National Security Agency document, " Department of Defense Class 3 PKI Public Key-Enabled Application Requirements," version 1.0, 13 July 2000.

E-4 PERSONNEL REQUIREMENTS. The number of testers required depends on the test requirements and/or the test equipment/networks. Table D-1 depicts the personnel a typical test would require.

Table E -1. Personnel Requirements for a Typical Test

FUNCTION	NUMBER	SOURCE
Test Analyst/Data Collector	1	JITC
Operator	1	JITC

E-5 SOFTWARE DESCRIPTIONS. The test report will describe the testing software, version numbers, and any patches or upgrades.

APPENDIX F

JOINT INTEROPERABILITY TEST COMMAND (JITC) PUBLIC KEY INFRASTRUCTURE (PKI) SERVICES

F-1 JITC PKI VISION

- To be the premier Department of Defense (DOD) PKI test organization.
- To provide unequaled support to DOD and its commercial partners.
- To help deploy a fully interoperable PKI.

F-2 JITC PKI OVERVIEW

Many programs supporting the DOD missions require security services, such as authentication, confidentiality, non-repudiation, and access control. To help address these security problems, the DOD developed a PKI. The DOD provides products and services that enhance the security of networked information systems and facilitate digital signatures.

The JITC performs two major PKI services to ensure the long term success of the DOD PKI. These services are:

- Interoperability Certification of Public Key Enabled (PKE) applications.
- DOD PKI Test Certificate Services.

DOD is committed to using PKI. Services, agencies, and vendors must prepare for its deployment. The JITC PKI laboratory and PKI team are strategically positioned to provide the necessary services to DOD PKI customers, ensuring application interoperability within the infrastructure. The services offered by the JITC will do the following for your organization:

- Test compatibility and interoperability with the existing and planned PKI technologies and applications.
- Improve product quality and functionality.
- Reduce technical risk.
- Make comprehensive PKI efforts more affordable.

F-3 PKI INTEROPERABILITY TESTING AND CERTIFICATION

The JITC PKI Test Laboratory provides interoperability certification for PKE applications. The JITC certification process was established by the DOD PKI Program Management Office (PMO) as an independent testing capability to ensure application interoperability with the DOD PKI. It is DOD policy that applications are tested to ensure interoperability and compatibility with the DOD PKI.

The JITC certification process includes test planning, execution, analysis, reporting, and certification. JITC tests applications by interfacing them with the JITC PKI test Certificate Authority (CA) and Directory Server (DS). JITC determines the extent the application interoperates with the DOD PKI in accordance with the "Department of Defense Class 3 Public Key Infrastructure PKE Application Requirements," 13 July 2000, and the "Department of Defense Class 3 Public Key Infrastructure Interface Specifications," version 1.0, 10 August 2000.

It is DOD policy that:

- PKE applications are tested to ensure interoperability and compatibility with the DOD PKI.
- Development authorities for PKE applications shall ensure interoperability with the DOD PKI in accordance with standards developed by the DOD PKI PMO.
- DOD Component Heads have the responsibility to ensure successful completion of interoperability testing for PKE applications.

F-4 APPLICATION ASSESSMENT WORKSHEET

The Application Assessment Worksheet is a form the JITC PKI certification team uses to obtain initial information about an application. This form is designed to be filled out by experts of the application with as much detail as possible. The questions in the Application Assessment Worksheet help the PKI Test Engineer determine which sections of the Master Test Plan apply to the application and need to be tested. Please provide as much information as possible on the Application Assessment Worksheet to assist the team in the assessment process of the application. A copy of the worksheet can be found in Appendix G or on the JITC PKI website:
http://jitc.fhu.disa.mil/pki

F-5 JITC TEST CERTIFICATE LAB

The JITC PKI Test Certificate Lab provides test certificate services in support of DOD and commercial partners to help successfully deploy a fully interoperable PKI. The Defense Information Systems Agency and the PKI PMO established the lab as the official test facility for the issuance of DOD PKI test certificates and help desk support.

The laboratory maintains a DOD PKI testbed that mirrors the operational PKI installed at the Defense Enterprise Computer Center. The PKI lab is a copy of the operational DOD PKI Environment and provides the same PKI operations as the operational PKI. This allows testing and training to occur in an environment separate from the operational infrastructure yet with the same functionality.

Customers of the PKI lab include:

- Commercial and government developers testing their products.
- Services and agencies training system administrators and end users.

- JITC PKI test engineer performing application interoperability certification testing.
- Commercial vendors demonstrating their products' interoperability with the DOD PKI.

F-6 PKI LAB ENVIRONMENT

Figure E-1, JITC PKI Lab Diagram, shows the current lab configuration. The lab currently operates Release 1 and Release 2 systems. The servers are operational 24 hours a day, seven days a week, with the exception of backups and routine maintenance Fridays from 1430 to 1730 Arizona time.

DOD and JITC plans to continue building upon the DOD PKI Lab and increase capabilities as a test facility. Future enhancements include the installation of Release 3 and SECRET Internet Protocol Router Network systems.

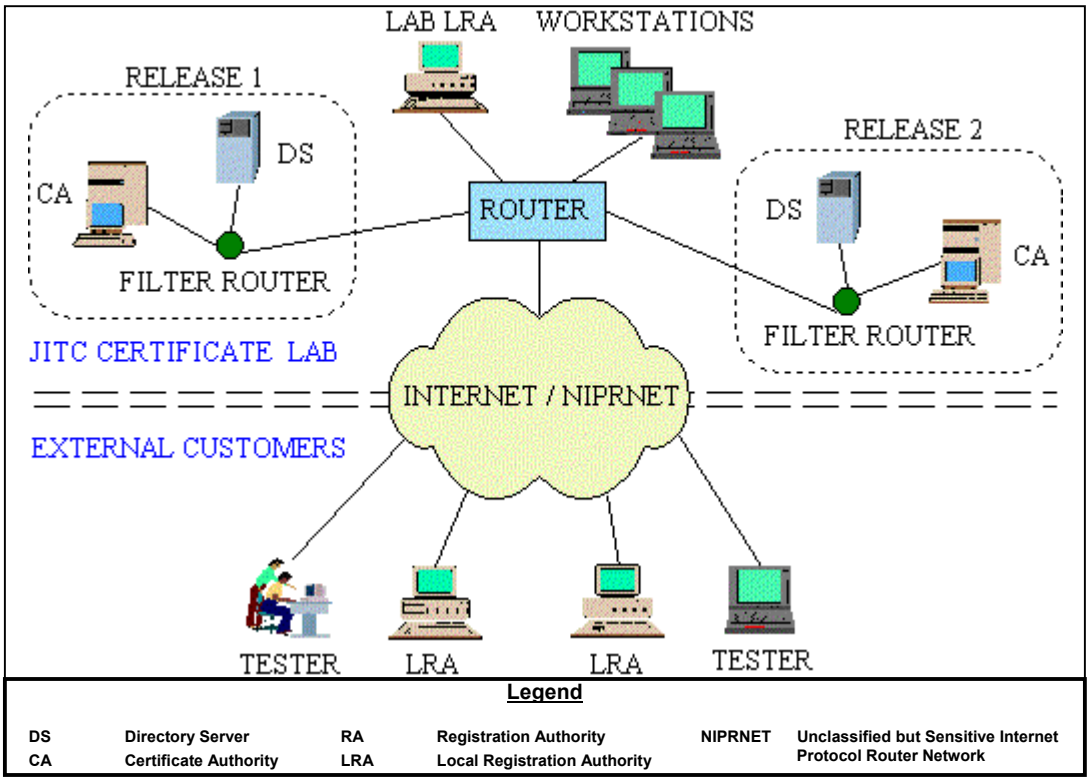


Figure F-1. JITC PKI Lab Diagram

F-7 CERTIFICATE AND DIRECTORY SERVICES

The following services and products are provided by the lab for the purpose of DOD PKI-related development, testing, training, and demonstrations:

- DOD PKI Test Certificates:
  Registration Authority (RA)

Local Registration Authority (LRA)
Server Identification (web sites)
User Identification
E-mail Identification
E-mail Encryption

- Directory services
  Certificate Revocation Lists (CRLs) and services
- Help Desk Support

F-8 OBTAINING A TEST CERTIFICATE

DOD PKI functions may require using Netscape 4.0 or greater.

If your organization is interested in obtaining test certificates, please read the information below and then contact the JITC PKI lab.

If your service or agency already has assigned a JITC test LRA or RA, please contact them first to receive certificates. If this information is unknown, the JITC PKI lab can assist you. DOD groups that require a large number of certificates should obtain their own test LRA. This allows the production of user and e-mail certificates at the discretion of the designated LRA/RA without dependence on JITC personnel. The Help Desk can answer questions about becoming an LRA.

- **User certificates** are generated by LRAs. Our lab can act as an LRA for modest DOD requests if a test LRA is not available for your organization. In the case of commercial vendors, JITC will always act as the LRA. The test LRA will instruct you on downloading the certificate once the request has been processed.

- **E-mail certificates** can be generated by any user once a user certificate has been issued. E-mail certificates have two types: identification and encryption. Access the appropriate server below and follow the instructions.

- **Server certificates,** or certificates for **web sites,** must be requested from the server they are intended for because they are tied to the machine generating the request. You will be required to generate a certificate on your server and upload it to the Certificate Authority. Once the request has been submitted, contact your test RA for authorization. JITC can act as the RA if you do not have one. The test RA will provide instructions for retrieving the approved certificate.

- **LRA certificates** must be requested from a test RA or the JITC PKI lab.

- **RA certificates** must be issued by the JITC PKI lab.

F-9 HELP DESK

The JITC PKI Help Desk is available to assist you Monday through Friday from 0830 to 1730 Arizona time. Refer to Appendix H for Help Desk Point of Contact information.

(This page intentionally left blank.)

APPENDIX G

APPLICATION ASSESSMENT WORKSHEET

JITC PKI APPLICATION ASSESSMENT WORKSHEET GENERAL INFORMATION	
Vendor Name:	Date:
Application:	Version:
Point of Contact:	
Phone #:	E-mail:
Organization/Agency:	
Give a brief description of application:	

SOFTWARE FUNCTION AND DEFINITION (Select one)		
Application		Client or server programs that are public key enabled (PKE) to provide security services, such as authentication, confidentiality, non-repudiation and access control.
Middleware		Middleware, or "glue", is a layer of software between the network and the applications. This software provides services such as identification, authentication, authorization, directories, and security.
Tool Kit		Toolkits enable developers to quickly and easily incorporate high-level security features into their applications. Toolkits add additional code to functional programs to achieve features such as authentication, confidentiality, non-repudiation and access control.

DETAILS (Please answer as thoroughly as possible)
1. What hardware/operating system(s) does the application use?
2. What other application(s) is your application dependent on? (e.g. Netscape, Internet Explorer)
3. Can the application request and obtain new certificates?
4. Can the application import and/or export certificates in PKCS #12 format?

DETAILS (continued)
5. Does the application generate key pairs and/or certificates?
a) What algorithm is used to generate key pairs?
b) Can the application provide the private encryption key it generates to the DOD Key Recovery Manager (KRM)?
6. Does the application perform path validation and processing?
7. Does the application have the capability to retrieve certificates belonging to other entities? (e.g. Public Key from Directory Server)
8. How does the application manage and store trust points?
a) Who is authorized to manage trust points? (e.g. User or Network Administrator)
9. Does the application use LDAP, HTTP, and/or HTTPS to communicate?

DETAILS (continued)
10. How does the application check the status of certificates? (e.g. Use of Directory Server, Manual loading of CRL's, Online Status Check)
11. Describe how and for what purpose a DOD issued PKI certificate is used in the application?

Use this space for questions/comments or any additional information you can provide.

Instructions

This form will be used to gather information to assess an application and help determine how PKI was implemented. Please provide detailed information pertaining to the questions on this form. Feel free to expand the height of the rows to fit additional information. After completion, e-mail this form to: pki@fhu.disa.mil

More Information

For links to our Master Test Plan, frequently asked questions, lab information, testing requirements, point of contacts and other information visit us at:

http://jitc.fhu.disa.mil/pki

Required Information

Prior to the commencement of testing, JITC requires the following be provided:

- Final version of application software to be tested.
- Application Documentation
  - User Manuals
  - Configuration Guides
- Other Resources as applicable

(This page intentionally left blank.)

APPENDIX H

POINTS OF CONTACT

JITC PKI Web Site:

http://jitc.fhu.disa.mil/pki

Government POC:

Ms. Cammie Webster
JITC PKI Test Officer
(520) 538-5485, DSN 879-5485
E-mail: websterc@fhu.disa.mil

Interoperability Testing POC:

Mr. Wesley Graybill
PKI Testing Services Manager
(520) 538-1702, DSN 879-1702
E-mail: graybilw@fhu.disa.mil

Test Certificate Services POC:

Mr. Eric Eager
PKI Testing Support Technical Lead
(520) 533-8805, DSN 821-8805
E-mail: eagerj@fhu.disa.mil

JITC PKI Help Desk:

Mr. Tony Jensen
PKI System Administrator
(520) 533-8793, DSN 821-8793
E-mail: jensena@fhu.disa.mil

(This page intentionally left blank.)

APPENDIX I

REFERENCES

I-1 DEFENSE INFORMATION SYSTEMS AGENCY (DISA) AND NATIONAL SECURITY AGENCY (NSA) DOCUMENTS

a. DISA and NSA, "Department of Defense (DOD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0, 13 July 2000.

b. DISA and NSA, "Department of Defense Class 3 Public Key Infrastructure Interface Specification," Version 1.2, 10 August 2000.

I-2 CYGNACOM SOLUTIONS DOCUMENT

Cygnacom Solutions, "Conformance Testing of Relying Party Client Certificate Path Processing Logic," Version 1.06, 6 November 2000.

(This page intentionally left blank.)