DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE EXTERNAL CERTIFICATION AUTHORITY MASTER TEST PLAN VERSION 1.0

AUGUST 2003

DEPARTMENT OF DEFENSE
PUBLIC KEY INFRASTRUCTURE
EXTERNAL CERTIFICATION
AUTHORITY
MASTER TEST PLAN

AUGUST 2003

Submitted by: **Manuel Garcia**
Chief
Global Information Grid Strategic Networks Branch

Approved by: _____
LESLIE F. CLAUDIO
Chief
Networks, Transmission and Integration Division

Prepared Under the Direction of:

Gretchen Dixon
Joint Interoperability Test Command
Fort Huachuca, Arizona 85613-7051

(This page intentionally left blank.)

EXECUTIVE SUMMARY

The Department of Defense (DOD) established an accreditation process to create trust relationships with certification authorities (CAs) outside of the DOD domain that achieve an assurance level equivalent to or greater than the DOD Public Key Infrastructure (PKI) Medium Assurance policy. These External Certification Authorities (ECAs) will provide non-DOD personnel with certificate services that interoperate with the DOD PKI. Contractors, vendors and other interested parties may use certificates obtained from an accredited ECA to transact electronic business with DOD entities.

The Defense Information Systems Agency (DISA), PKI/Biometrics Branch (API23) tasked the Joint Interoperability Test Command (JITC) to perform standards compliance testing of ECA-issued certificates, certificate revocation lists (CRLs), and online certificate status protocol (OCSP) request and response formats (collectively ECA-issued objects), and interoperability testing of ECA-issued certificates and CRLs.

Standards compliance tests will consist of decoding base 64 encoded ECA-issued objects to produce a hard copy profile for visual inspection. JITC will compare these hard copy profiles with the profiles set forth in the "Certificate Policy for External Certification Authorities, V2.0," 4 June 2003. JITC will compare profiles of the following:

Root CA certificate	Subordinate CA certificates
Identity certificate	Encryption certificate
Component certificate	Code signing certificate
OCSP responder self-signed certificate	OCSP responder certificate
Root CA CRLs	Subordinate CA CRLs
OCSP request format	OCSP response format

Interoperability tests will consist of loading ECA-issued certificates and CRLs into a public key enabled (PKE) application that has been certified by JITC as interoperable with the DOD PKI and verifying that the PKE application can correctly process the certificates and CRLs. The DOD Class 3 PKI does not currently support OCSP responders; therefore, JITC will not perform interoperability tests with OCSP responder certificates and OCSP requests and responses.

JITC will perform the standards compliance tests and interoperability tests at its PKI laboratory at Fort Huachuca, Arizona. JITC will present the results of the standards compliance tests and the interoperability tests in a test report and will issue a certification letter to those ECA candidates that meet the requirements of these tests.

(This page intentionally left blank.)

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

TABLE OF CONTENTS (continued)

LIST OF TABLES

SYSTEM FUNCTIONAL DESCRIPTION

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

- Issue and manage x.509 Version (V) 3 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 (CRLs).
- Generate CRLs.

Certification authorities (CAs) outside of the DOD domain, External Certification Authorities (ECAs), will provide non-DOD personnel with certificate services that interoperate with the DOD PKI. Contractors, vendors, and other interested parties may use certificates obtained from an accredited ECA to transact electronic business with DOD entities.

TEST BACKGROUND

The DOD established an accreditation process to create trust relationships with ECAs that achieve an assurance level equivalent to or greater than the DOD PKI Medium Assurance policy. As part of the accreditation process for ECAs, the Defense Information Systems Agency (DISA), PKI/Biometrics Branch (API23) tasked the Joint Interoperability Test Command (JITC) to perform standards compliance testing of ECA-issued certificates, CRLs, and online certificate status protocol (OCSP) request and response formats (collectively ECA-issued objects) and interoperability testing of ECA-issued certificates and CRLs.

TEST PURPOSE

To determine the extent ECA-issued objects comply with the standard profiles set forth in the "Certificate Policy for External Certification Authorities, V2.0," 4 June 2003, (Certificate Policy) and the extent ECA-issued certificates and CRLs interoperate with a public key enabled (PKE) application that has been certified by JITC as interoperable with the DOD PKI.

REQUIREMENTS

The standard profiles set forth in the Certificate Policy are presented in tables in appendix B. The interoperability tests are in appendix C.

SCOPE

The DOD PKI operational environment is divided in two parts: DOD PKI production, and DOD PKI test. The purpose of the JITC DOD PKI laboratory is to create a test environment identical to that of the DOD PKI production side, and to provide DOD PKI test certificates for the testing, developing, and training communities.

JITC will perform the standards compliance tests and interoperability tests at its PKI laboratory at Fort Huachuca, Arizona. The ECA candidate will provide certificates, CRLs, OCSP request and response formats, and optional hardware tokens and/or smart cards. The number of certificates, CRLs, and OCSP request and response formats that must be submitted is set forth in appendix D. Because the DOD Class 3 PKI does not currently support OCSP responders, JITC will not perform interoperability tests with OCSP responder certificates and OCSP request and response formats.

OBJECTIVES AND METHODOLOGY

JITC will perform standards compliance testing of ECA-issued objects and interoperability testing of ECA-issued certificates and CRLs.

Standards compliance tests will consist of decoding base 64 encoded ECA-issued objects to display at the workstation console or to produce a hard copy. JITC will perform a visual inspection and compare these profiles with the profiles set forth in the Certificate Policy. JITC will test the following profiles:

Root CA certificate	Subordinate CA certificates
Identity certificate	Encryption certificate
Component certificate	Code signing certificate
OCSP responder self-signed certificate	OCSP responder certificate
Root CA CRLs	Subordinate CA CRLs
OCSP request format	OCSP response format

Interoperability tests will consist of loading ECA-issued certificates into a PKE application that has been certified by JITC as interoperable with the DOD PKI and verifying that the PKE application can correctly process these certificates. PKE applications that may be used in the interoperability tests are posted at: http://jitc.fhu.disa.mil/pki/appstatus.html. JITC will also verify that the application can process the root CA CRL and the subordinate CA CRLs to determine certificate status.

The PKE application must meet the following interoperability criteria:

- Trust the ECA root certificate.
- Validate an ECA subordinate certificate.
- Validate an ECA identity certificate.
- Encrypt and decrypt using an ECA encryption certificate.
- Secure a web server using an ECA component certificate.
- Validate signatures on mobile code signed by an ECA code signing certificate.
- Check an ECA Root CA CRL.
- Use an ECA Subordinate CA CRL to check the status of a certificate.
- Reject a revoked ECA certificate.
- Reject an expired ECA certificate.

PRESENTATION OF RESULTS AND ANALYSIS PROCEDURES

Analysts will examine the pass/fail status of each test event to determine the extent the ECA-issued objects comply with the requirements for each test. The test report will present the results in tables B-1 through B-12, C-1, and in narrative text. The tables are both data collection tables and test results tables. They contain the required values for each field and columns to record the test results.

JITC will issue a certification letter to those ECA candidates that meet the requirements of the standards compliance and interoperability tests.

(This page intentionally left blank.)

APPENDIX A

ACRONYMS

AKID	Authority Key Identifier
CA	Certification Authority
CRL	Certificate Revocation List
DISA	Defense Information Systems Agency
DOD	Department of Defense
DS	Directory Server
ECA	External Certification Authority
HTTP	Hypertext Transfer Protocol
JITC	Joint Interoperability Test Command
OCSP	Online Certificate Status Protocol
PKE	Public Key Enabled
PKI	Public Key Infrastructure
SKID	Subject Key Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
V	Version

(This page intentionally left blank.)

APPENDIX B

EXTERNAL CERTIFICATION AUTHORITY (ECA) OBJECTS STANDARDS COMPLIANCE TESTS

B-1 TEST PROCEDURES

Tables B-1 through B-12 list the profiles set forth in the "Certificate Policy for External Certification Authorities, V2.0," 4 June 2003 (Certificate Policy).

a. Test Conduct. Testers will:

(1) Decode an ECA-issued object using the Joint Interoperability Test Command (JITC) Public Key Infrastructure (PKI) laboratory certificate/certificate revocation list (CRL) tool kit. The JITC PKI certificate/CRL tool kit is a collection of software utilities capable of decoding base 64 encoded certificates, CRLs, and Online Certificate Status Protocol (OCSP) requests and responses. Testers will display decoded ECA-issued objects to the workstation console or print a hard copy.

(2) Visually compare the profile of the ECA-issued object produced by the JITC PKI certificate/CRL tool kit with the profiles set forth in the Certificate Policy. The Certificate Policy profiles are in tables B-1 through B-12.

(3) Repeat steps 1 and 2 for each ECA-issued object.

b. Data Collection. Tables B-1 through B-12 are both data collection tables and test results tables. They contain the required values for each field and columns to record the test results. Testers will record the pass/fail status of each test event on the appropriate table.

B-2 PRESENTATION OF RESULTS. The test report will present the pass/fail status of each test event in tables B-1 through B-12, and a conclusion in narrative text.

Table B-1. ECA Root CA Self-Signed Certificate Requirements

Field	ECA Root CA Self-Signed Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US		
Validity Period	36 years from date of issue in Generalized Time format		
Subject Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption {1 2 840 113549 1 1 1}		
Issuer Unique Identifier	Not present		
Subject Unique Identifier	Not present		
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Authority Key Identifier[1]	Octet String (20 byte SHA-1 has of the binary DER encoding of the ECA Root CA's public key information)		
Subject Key Identifier	Octet String (20 byte SHA-1 has of the binary DER encoding of the ECA Root CA's public key information)		
Key Usage	c=yes; digitalSignature, keyCertSign, CRLSign		
Extended Key Usage	Not present		
Private Key Usage Period	Not present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}		
Policy Mapping	Not present		
Subject Alternate Name	Not present		
Issuer Alternate Name	Not present		
Subject Directory Attributes	Not present		
Basic Constraints	c=yes; cA=True; no path length constraint		
Name Constraints	Not present		
Policy Constraints	Not present		
CRL Distribution Points	Not present		

LEGEND

c	Country	o	Organization
CA	Certification Authority	ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
DER	Distinguished Encoding Rules	V	Version
ECA	External Certification Authority		

[1] The value of the Authority Key Identifier (AKID) field could be absent. If present, it must equal the value of the Subject Key Identifier (SKID) field.

Table B-2. ECA Subordinate CA Certificate Requirements

Field	ECA Subordinate CA Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US		
Validity Period	6 years from date of issue in UTC format		
Subject Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption {1 2 840 113549 1 1 1}		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption (1 2 840 113549 1 1 5)		
Authority Key Identifier[2]	octet string (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)		
Subject Key Identifier	octet string (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)		
Key Usage	c=yes; digitalSignature, keyCertSign, CRLSign		
Extended Key Usage	Not Present		
Private Key Usage Period	Not Present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1} {2 16 840 1 101 3 2 1 12 2}		
Policy Mapping	Not Present		
Subject Alternate Name	Not Present		
Issuer Alternate Name	Not Present		
Subject Directory Attributes	Not Present		
Basic Constraints	c=yes; cA=True; path length constraint = 0		
Name Constraints	c=no; permitted subtrees: ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Policy Constraints	Not Present		
Authority Information Access	c=no; optional; pointer to OCSP Responder		
CRL Distribution Points[3]	c=no; always present		

LEGEND

c	Country	OCSP	Online Certificate Status Protocol
CA	Certification Authority	ou	Organizational Unit
cn	Common Name	PKI	Public Key Infrastructure
CRL	Certificate Revocation List	RSA	Rivest, Shamir, and Adleman
DER	Distinguished Encoding Rules	SHA	Secure Hash Algorithm
DOD	Department of Defense	UTC	Coordinated Universal Time
ECA	External Certification Authority	V	Version
o	Organization		

[2] The value of the AKID field should be the same as the value of the SKID field in the external certification authority (ECA) Root Certification Authority (CA) Self-Signed certificate.

[3] The certificate revocation list (CRL) distribution point extension shall only populate the distributionPoint field. The field shall only contain the uniform resource identifier (URI) name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). It will point to the ECA Root issued CRL.

Table B-3. ECA Identity Certificate Requirements

Field	ECA Identity Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S Government, c=US		
Validity Period	3 years from date of issue in UTC format		
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber CompanyName>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption		
Authority Key Identifier[4]	c=no; octet string		
Subject Key Identifier[5]	c=no, octet string		
Key Usage	c=yes;digitalSignature, nonRepudiation		
Extended Key Usage	Not Present		
Private Key Usage Period	Not Present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1} or [{2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}]		
Policy Mapping	Not Present		
Subject Alternate Name	c=no; always present, contains RFC822 email address		
Issuer Alternate Name	Not Present		
Subject Directory Attributes	Not Present		
Basic Constraints	Not Present		
Name Constraints	Not Present		
Policy Constraints	Not Present		
Authority Information Access	c=no; optional; pointer to OCSP Responder		
CRL Distribution Points[6]	c=no; always present		

LEGEND

c	Country	ou	Organizational Unit
CA	Certification Authority	RFC	Request for Comments
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
ECA	External Certification Authority	UTC	Coordinated Universal Time
o	Organization	V	Version
OCSP	Online Certificate Status Protocol		

[4] The value of this field is the 20-byte secure hash algorithm (SHA)-1 hash of the binary distinguished encoding rules (DER) encoding of the signing CA's public key information. The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate.

[5] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[6] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table B-4. ECA Encryption Certificate Requirements

Field	ECA Encryption Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Validity Period	3 years from date of issue in UTC format		
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption		
Authority Key Identifier[7]	c=no; octet string		
Subject Key Identifier[8]	c=no; octet string		
Key Usage	c=yes; keyEncipherment		
Extended Key Usage	Not Present		
Private Key Usage Period	Not Present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1} or [{2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}]		
Policy Mapping	Not Present		
Subject Alternate Name	c=no; always present, contains RFC822 email address		
Issuer Alternate Name	Not Present		
Subject Directory Attributes	Not Present		
Basic Constraints	Not Present		
Name Constraints	Not Present		
Policy Constraints	Not Present		
Authority Information Access	c=no; optional; pointer to OCSP Responder		
CRL Distribution Points[9]	c=no; always present		

LEGEND

c	Country	ou	Organizational Unit
CA	Certification Authority	RFC	Request for Comments
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
ECA	External Certification Authority	UTC	Coordinated Universal Time
o	Organization	V	Version
OCSP	Online Certificate Status Protocol		

[7] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the signing CA's public key information. The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate.

[8] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[9] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table B-5. ECA Component Certificate Requirements

Field	ECA Component Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=<ECA CA Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Validity Period	3 years from date of issue in UTC format		
Subject Distinguished Name	cn=<Host URL | IP Address | Host Name>, ou=<Host Company Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption		
Authority Key Identifier[10]	c=no; octet string		
Subject Key Identifier[11]	c=no; octet string		
Key Usage	c=yes; keyEncipherment, digitalSignature		
Extended Key Usage	Not Present		
Private Key Usage Period	Not Present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1}		
Policy Mapping	Not Present		
Subject Alternate Name	c=no; always present, Host URL | IP Address | Host Name		
Issuer Alternate Name	Not Present		
Subject Directory Attributes	Not Present		
Basic Constraints	Not Present		
Name Constraints	Not Present		
Policy Constraints	Not Present		
Authority Information Access	c=no; optional; pointer to OCSP Responder		
CRL Distribution Points[12]	c=no; always present		

LEGEND

c	Country	OCSP	Online Certificate Status Protocol
CA	Certification Authority	Ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
ECA	External Certification Authority	URL	Uniform Resource Locator
IP	Internet Protocol	UTC	Coordinated Universal Time
o	Organization	V	Version

[10] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the signing CA's public key information. The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate.

[11] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[12] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table B-6. ECA Code Signing Certificate Requirements

Field	ECA Code Signing Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Validity Period	10 years from date of issue		
Subject Distinguished Name	cn=CS.<Code Signer Company Name>.<optional number>, ou=<Code Signer Company Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024-bit RSA key modulus, RSAEncryption		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1 WithRSAEncryption		
Authority Key Identifier[13]	c=no; octet string		
Subject Key Identifier[14]	c=no; octet string		
Key Usage	c=yes; digitalSignature, nonRepudiation		
Extended Key Usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3) }		
Private Key Usage Period	Not Present		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}		
Policy Mapping	Not Present		
Subject Alternate Name	always present; c=no; <cn=Code Signing private key holder name>, <ou=Code Signing ECA Subscriber Company Name>, <ou=ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Issuer Alternate Name	Not Present		
Subject Directory Attributes	Not Present		
Basic Constraints	Not Present		
Name Constraints	Not Present		
Policy Constraints	Not Present		
Authority Information Access	c=no; optional; pointer to OCSP Responder		
CRL Distribution Points[15]	c= no; always present		

LEGEND

c	Country	o	Organization
CA	Certification Authority	OCSP	Online Certificate Status Protocol
cn	Common Name	ou	Organizational Unit
CRL	Certificate Revocation List	PKI	Public Key Infrastructure
CS	Code Signer	RSA	Rivest, Shamir, and Adleman
DOD	Department of Defense	SHA	Secure Hash Algorithm
ECA	External Certification Authority	UTC	Coordinated Universal Time
ID	Identification	V	Version
ISO	International Organization for Standards		

[13] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the signing CA's public key information. The value of the AKID field must match the value of the SKID field in the issuer CA certificate

[14] The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[15] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table B-7. ECA OCSP Responder Self-Signed Certificate Requirements

Field	OCSP Responder Self-Signed Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Issuer Distinguished Name	cn=<OCSP Responder Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Validity Period	36 years from date of issue in Generalized Time format		
Subject Distinguished Name	cn=<OCSP Responder Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024 bit RSA key modulus, RSAEncryption {1 2 840 113549 1 1 1}		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Extensions	Not Present		

LEGEND

c	Country	ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
ECA	External Certification Authority	SHA	Secure Hash Algorithm
o	Organization	V	Version
OCSP	Online Certificate Status Protocol		

Table B-8. ECA OCSP Responder Certificate Requirements

Field	OCSP Responder Certificate Value	Results	Pass or Fail
Version	V3 (2)		
Serial Number	Must be unique		
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Issuer Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Validity Period	One month from date of issue in UTC format		
Subject Distinguished Name	cn=<OCSP Responder Name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
Subject Public Key Information	1024 bit RSA key modulus, RSAEncryption {1 2 840 113549 1 1 1}		
Issuer Unique Identifier	Not Present		
Subject Unique Identifier	Not Present		
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}		
Extensions			
Authority Key Identifier[16]	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA CA's public key information)		
Subject Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the OCSP Responder public key information)		
Key Usage	c=yes; nonRepudiation, digitalSignature		
Extended Key Usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}		
Certificate Policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}		
Subject Alternate Name	HTTP URL for the OCSP Responder		
No Check	id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}		

LEGEND

c	Country	OCSP	Online Certificate Status Protocol
CA	Certification Authority	ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
DER	Distinguished Encoding Rules	SHA	Secure Hash Algorithm
ECA	External Certification Authority	URL	Uniform Resource Locator
HTTP	Hypertext Transfer Protocol	UTC	Coordinated Universal Time
ID	Identification	V	Version
o	Organization		

[16] The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate.

Table B-9. ECA OCSP Request Format Requirements

Field	OCSP Request Format Expected Value	Results	Pass or Fail
Version	V1 (0)		
Requester Name	Not Required		
Requester List	List of certificates – generally this should be the list of two certificates: ECA certificate and end entity certificate		
Signature	Not Required		
Extensions	Not Required		

LEGEND

ECA	External Certification Authority	V	Version

Table B-10. ECA OCSP Response Format Requirements

Field	OCSP Response Format Expected Value	Results	Pass or Fail
Response Status	Successful | Malformed Request | Internal Error | Try Later		
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}		
Version	V1 (0)		
Responder ID	Hash of Responder public key		
Produce At	UTC		
List of Reponses	Each response will contain certificate id; certificate status[17], thisUpdate, nextUpdate[18],		
Extension			
Nonce	Will be present if nonce extension is present in the request		
Signature Algorithm	sha-1 WithRSAEncryption {1 2 840 113549 1 1 5}		
Signature	Present		
Certificates	Applicable certificates issued to the OCSP Responder		

LEGEND

ID	Identification	SHA	Secure Hash Algorithm
OCSP	Online Certificate Status Protocol	UTC	Coordinated Universal Time
RSA	Rivest, Shamir, and Adleman	V	Version

[17] If the certificate is revoked, the ECA OCSP Responder shall provide revocation time and revocation reason from the CRL entry and the CRL entry extension.

[18] The ECA OCSP Responder shall use thisUpdate and nextUpdate from the ECA Root CA CRL.

Table B-11. ECA Root CA CRL Requirements

Field	ECA Root CA CRL Value	Results	Pass or Fail
Version	V2 (1)		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US		
thisUpdate	UTC		
nextUpdate	UTC; thisUpdate + 28 days		
Revoked Certificates List	0 or more 2-tuple of certificate serial number and revocation date (in UTC)		
CRL Extensions			
CRL Number	Integer		
Authority Key identifier[19]	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)		
CRL Entry Extensions			
Invalidity Date	optional		
Reason Code	Always Present; Will not include certificateHold		

LEGEND

c	Country	o	Organization
CA	Certification Authority	ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
DER	Distinguished Encoding Rules	UTC	Coordinated Universal Time
ECA	External Certification Authority	V	Version

[19] The value of the AKID field in the ECA CA Root CRL must match the value of the SKID field in the ECA CA Root Self-Signed certificate.

Table B-12. ECA Subordinate CA CRL Requirements

Field	ECA Subordinate CA CRL Value	Results	Pass or Fail
Version	V2 (1)		
Issuer Signature Algorithm	sha-1WithRSAEncryption		
Issuer Distinguished Name	cn=<ECA CA name>, ou=<ECA Company Name>, ou=ECA, o=U.S. Government, c=US		
thisUpdate	UTC		
nextUpdate	UTC; thisUpdate + 7 days		
Revoked Certificates List	0 or more 2-tuple of certificate serial number and revocation date (in UTC)		
CRL Extensions			
CRL Number	Integer		
Authority Key Identifier[20]	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)		
CRL Entry Extensions			
Invalidity Date	optional		
Reason Code	Always Present; Will not include certificateHold		

LEGEND

c	Country	o	Organization
CA	Certification Authority	ou	Organizational Unit
cn	Common Name	RSA	Rivest, Shamir, and Adleman
CRL	Certificate Revocation List	SHA	Secure Hash Algorithm
DER	Distinguished Encoding Rules	UTC	Coordinated Universal Time
ECA	External Certification Authority	V	Version

[20] The value of the AKID field in the ECA Subordinate CA CRL must match the value of the SKID field in the ECA Subordinate CA certificate.

APPENDIX C

EXTERNAL CERTIFICATION AUTHORITY (ECA) OBJECTS INTEROPERABILITY TESTS

C-1 TEST PROCEDURES

a. Test Conduct. Testers will load ECA-issued certificates and certificate revocation lists (CRLs) into a public key enabled (PKE) application that has been certified by the Joint Interoperability Test Command (JITC) as interoperable with the Department of Defense (DOD) Public Key Infrastructure (PKI) to verify that the application will:

(1) Trust the ECA root certificate.

(2) Validate an ECA subordinate certificate.

(3) Validate an ECA identity certificate.

(4) Encrypt and decrypt using an ECA encryption certificate.

(5) Secure a web server using an ECA component certificate.

(6) Validate signatures on mobile code signed by an ECA code signing certificate.

(7) Check the ECA root certificate authority (CA) CRL.

(8) Use an ECA Subordinate CA CRL to check the status of a certificate.

(9) Reject a revoked ECA certificate.

(10) Reject an expired ECA certificate.

Test procedures specific to each test event are in sections C-3.1 through C-3.12.

b. Data Collection. Table C-1 is both a requirements table and a test results table. Testers will record the pass/fail status of each event in table C-1.

C-2 PRESENTATION OF RESULTS. The test report will present the pass/fail status of each test event in table C-1 and a conclusion in narrative text.

Table C-1. ECA Certificates and CRLs Interoperability Tests

ECA-issued Certificates and CRLs	Pass or Fail
ECA Root CA Self-Signed Certificate	
Load the ECA root CA self-signed certificate into application	
Application shall trust the ECA root CA self-signed certificate	
ECA Subordinate CA Certificate	
Load an ECA subordinate CA certificate into application	
Application shall validate an ECA subordinate CA certificate	
ECA Identity Certificate	
Load an ECA identity certificate into application	
Application shall validate an ECA identity certificate	
Load a revoked ECA identity certificate into application	
Application shall reject the revoked ECA identity certificate	
Load an expired ECA identity certificate into application	
Application shall reject the expired ECA identity certificate	
ECA Encryption Certificate	
Load an ECA encryption certificate into application	
Application shall encrypt a test document using the ECA encryption certificate	
Application shall decrypt a test document using the ECA encryption certificate	
Load a revoked ECA encryption certificate into application	
Application shall reject the revoked ECA encryption certificate	
Load an expired ECA encryption certificate into application	
Application shall reject the expired ECA encryption certificate	
ECA Component Certificate	
Load an ECA component certificate into a server	
Secure a web server using an ECA component certificate	
View a test web page	
Secured web server shall grant access to a user using a valid ECA identity certificate	
Secured web server shall deny access to a user using a revoked ECA identity certificate	
Secured web server shall deny access to a user using an expired ECA identity certificate	
ECA Code Signing Certificate	
Load an ECA code signing certificate into application	
Application shall validate signature on mobile code signed by the ECA code signing certificate	
ECA Root CA CRL	
Load the ECA Root CA CRL into application	
Application shall check the ECA Root CA CRL	

Table C-1. ECA Certificates and CRLs Interoperability Tests (continued)

ECA-issued Certificates and CRLs	Pass or Fail
ECA Subordinate CA CRLs	
Load an ECA subordinate CA CRL into application	
Application shall use the ECA subordinate CA CRL to check the status of a certificate	

LEGEND

CA	Certification Authority	ECA	External Certification Authority
CRL	Certificate Revocation List		

C-3 DETAILED TEST PROCEDURES AND CRITERIA-RELATED DATA REQUIREMENTS

C-3.1 ECA Root CA Self-Signed Certificate

a. Objective. To determine if an ECA root CA self-signed certificate will load into a PKE application's trust point list.

b. Criterion. Application shall trust the ECA root CA self-signed certificate.

c. Test Procedures. Testers will invoke the functionality of the PKE application to trust the ECA root CA self-signed certificate. Testers will:

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

(2) Verify that the application trusts the ECA root CA self-signed certificate.

d. Criterion-related Data Requirements. ECA root CA self-signed certificate.

C-3.2 ECA Subordinate CA Certificate

a. Objective. To determine if an ECA subordinate CA certificate will load into a PKE application.

b. Criterion. Application shall validate an ECA subordinate CA certificate.

c. Test Procedures. Testers will:

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

(2) Load an ECA subordinate CA certificate.

(3) Verify that the application validates an ECA subordinate CA certificate.

d. Criterion-related Data Requirements. ECA subordinate CA certificate.

C-3.3 ECA Identity Certificate

a. Objective. To determine if a PKE application can authenticate users using an ECA identity certificate.

b. Criterion. Application shall use an ECA identity certificate to authenticate users.

c. Test Procedures. Testers will:

(1) Load an ECA identity certificate into application.

(2) Verify that the application validates an ECA identity certificate.

d. Criterion-related Data Requirements. ECA identity certificate.

C-3.4 Revoked ECA Identity Certificate

a. Objective. To determine if a PKE application rejects a revoked ECA identity certificate.

b. Criterion. Application shall reject a revoked ECA identity certificate.

c. Test Procedures. Testers will:

(1) Load a revoked ECA identity certificate into application.

(2) Verify that the application rejects a revoked ECA identity certificate.

d. Criterion-related Data Requirements. Revoked ECA identity certificate.

C-3.5 Expired ECA Identity Certificate

a. Objective. To determine if a PKE application rejects an expired ECA identity certificate.

b. Criterion. Application shall reject an expired ECA identity certificate.

c. Test Procedures. Testers will:

(1) Load an expired ECA identity certificate into application.

(2) Verify that the application rejects an expired ECA identity certificate.

d. Criterion-related Data Requirements. Expired ECA identity certificate.

C-3.6 ECA Encryption Certificate

a. Objective. To determine if a PKE application can encrypt and decrypt data using the ECA encryption certificate.

b. Criterion. Application shall encrypt and decrypt data using the ECA encryption certificate.

c. Test Procedures. Testers will:

(1) Load the ECA encryption certificate into the application.

(2) Verify that the application can encrypt a test document using the ECA encryption certificate.

(3) Verify that the application can decrypt a test document using the ECA encryption certificate.

d. Criterion-related Data Requirements. ECA encryption certificate.

C-3.7 Revoked ECA Encryption Certificate

a. Objective. To determine if a PKE application rejects a revoked ECA encryption certificate.

b. Criterion. Application shall reject a revoked ECA encryption certificate.

c. Test Procedures. Testers will:

(1) Load a revoked ECA encryption certificate into application.

(2) Verify that the application rejects a revoked ECA encryption certificate.

d. Criterion-related Data Requirements. Revoked ECA encryption certificate.

C-3.8 Expired ECA Encryption Certificate

a. Objective. To determine if a PKE application rejects an expired ECA encryption certificate.

b. Criterion. Application shall reject an expired ECA encryption certificate.

c. Test Procedures. Testers will:

(1) Load an expired ECA encryption certificate into application.

(2) Verify that the application rejects an expired ECA encryption certificate.

d. Criterion-related Data Requirements. Expired ECA encryption certificate.

C-3.9 ECA Component Certificate

a. Objective. To determine if a web server can be secured with an ECA component certificate and if the server can authenticate a user using an ECA identity certificate.

b. Criterion. A web server shall be secured using an ECA component certificate and only users with valid ECA identity certificates shall be allowed access to such a server.

c. Test Procedures. Testers will:

(1) Load an ECA component certificate into a web server.

(2) Verify that a web server can be secured using an ECA component certificate.

(3) Ensure the tester can view a test web page.

(4) Access the secured web server using a valid ECA identity certificate.

(5) Ensure the web server cannot be accessed using a revoked ECA identity certificate.

(6) Ensure the web server cannot be accessed using an expired ECA identity certificate.

d. Criteria-related Data Requirements. ECA component certificate, ECA identity certificate, revoked ECA identity certificate, expired ECA identity certificate.

C-3.10 ECA Code Signing Certificate

a. Objective. To determine if an ECA code signing certificate validates signatures on mobile code.

b. Criterion. Application shall validate signature on mobile code using an ECA code signing certificate.

c. Test Procedures. Testers will:

(1) Load an ECA code signing certificate into application.

(2) Validate a signature on mobile code signed by an ECA code signing certificate.

d. Criterion-related Data Requirements. ECA code signing certificate.

C-3.11 ECA Root CA CRL

a. Objective. To determine if a PKE application can use the ECA Root CA CRL to retrieve accurate revocation information.

b. Criterion. Application shall use the ECA Root CA CRL to check the status of an ECA subordinate CA certificate.

c. Test Procedures. Testers will:

(1) Load the ECA root CA CRL into the application.

(2) Verify that the application can use the ECA Root CA CRL to check the status of an ECA subordinate CA certificate.

d. Criteria-related Data Requirements. ECA Root CA CRL, ECA subordinate CA certificate.

C-3.12 ECA Subordinate CA CRL

a. Objective. To determine if a PKE application can use an ECA subordinate CA CRL to retrieve accurate revocation information.

b. Criterion. Application shall use an ECA subordinate CA CRL to check the status of an ECA identity certificate.

c. Test Procedures. Testers will:

(1) Load an ECA subordinate CA CRL into application.

(2) Verify that the application can use the ECA subordinate CA CRL to check the status of an ECA identity certificate.

d. Criteria-related Data Requirements. ECA Subordinate CA CRL, ECA identity certificate.

APPENDIX D

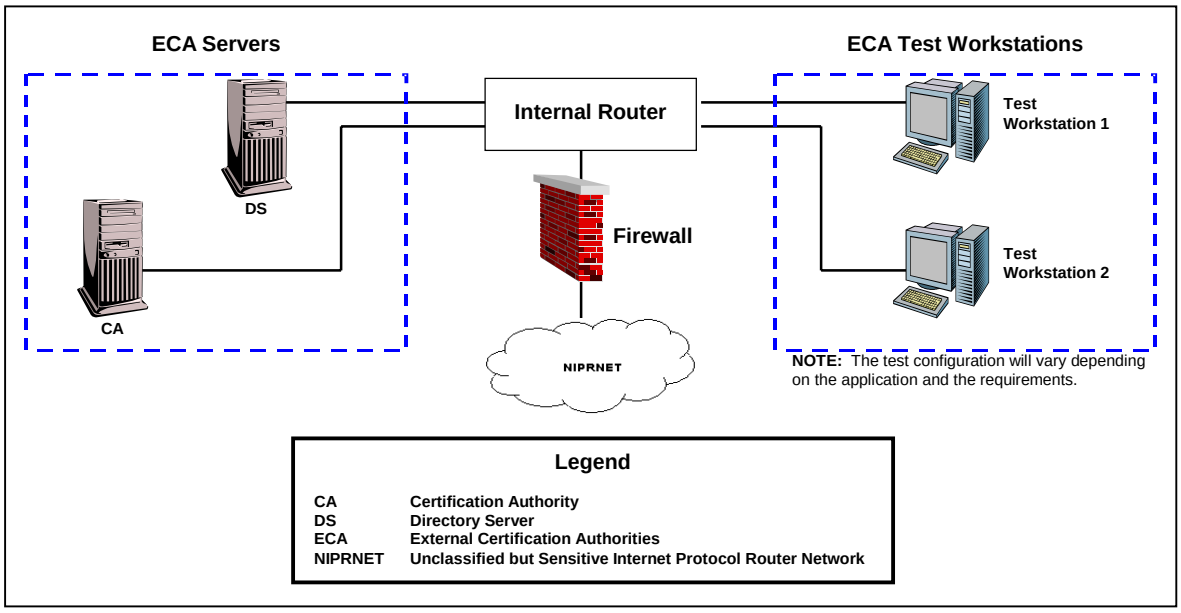
TEST RESOURCES REQUIRED AND PREREQUISITES

D-1 TEST RESOURCES

D-1.1 Test Sites and Facilities. The Joint Interoperability Test Command (JITC) will test External Certification Authority (ECA)-issued objects at the JITC Public Key Infrastructure (PKI) laboratory at Fort Huachuca, Arizona.

D-1.2 Test Equipment/Network. Testers will use at least one workstation to test ECA-issued objects. Figure D-1 depicts a typical test configuration.

Figure D-1. Typical Test Configuration



D-1.3 Personnel Requirements. The number of testers required depends on the test requirements and/or the test equipment/networks. Table D-1 shows the personnel requirements for a typical test.

Table D-1. Personnel Requirements for a Typical Test

Function	Number	Source
Test Analyst/Data Collector	2	Joint Interoperability Test Command

D-1.4 Software Descriptions. To conduct the standards compliance profile tests, testers will use ECA-issued certificates, certificate revocation lists (CRLs), and online certificate status protocol (OCSP) request and response formats. Testers will use the

JITC PKI certificate/CRL tool kit to decode these objects and print them at the console or print a hard copy to perform a visual inspection. To conduct the interoperability tests, testers will use ECA-issued certificates and CRLs, which shall be loaded into a PKE application that has been certified by JITC as interoperable with the Department of Defense PKI.

D-2 TEST PREREQUISITES

D-2.1 Standards Compliance Test Prerequisites. ECA candidates must submit base 64 encoded certificates, CRLs, and OCSP requests and responses by mail to JITC on the ECAs' choice of media. Packages should be addressed to:

Ms. Gretchen Dixon, JTEB
Building 57305
Joint Interoperability Test Command
2001 Brainard Road
Fort Huachuca, AZ 85613-7051

D-2.2 Interoperability Test Prerequisites. JITC testers must be able to generate a request for ECA certificates from the ECA candidate. ECA candidates must provide Uniform Resource Locators to download the certificates.

Table D-2 shows the ECA-issued object types, the minimum number of each object the ECA candidate must submit, the types of tests, and applicable sections of this Master Test Plan.

Table D-2. Standards Compliance and Interoperability Test Prerequisites

ECA Object Type	Quantity Required	Standards Compliance	Interoperability
		Reference Section	Reference Section
ECA Root CA Self-Signed Certificate	1	B-1	C-3.1
ECA Subordinate CA Certificate	1	B-2	C-3.2
ECA Identity Certificate	3	B-3	C-3.3
Revoked ECA Identity Certificate	1	B-3	C-3.4
Expired ECA Identity Certificate	1	B-3	C-3.5
ECA Encryption Certificate	3	B-4	C-3.6
Revoked ECA Encryption Certificate	1	B-4	C-3.7
Expired ECA Encryption Certificate	1	B-4	C-3.8
ECA Component Certificate	1	B-5	C-3.9
ECA Code Signing Certificate	3	B-6	C-3.10
ECA OCSP Responder Self-Signed Certificate	1	B-7	N/A

Table D-2. Standards Compliance and Interoperability Test Prerequisites (continued)

ECA Object Type	Quantity Required	Standards Compliance	Interoperability
		Reference Section	Reference Section
ECA OCSP Responder Certificate	1	B-8	N/A
ECA OCSP Request Format	3	B-9	N/A
ECA OCSP Response Format	3	B-10	N/A
ECA Root CA CRL	1	B-11	C-3.11
ECA Subordinate CA CRL	1	B-12	C-3.12

LEGEND

CA	Certification Authority	N/A	Not Available
CRL	Certificate Revocation List	OCSP	Online Certificate Status Protocol
ECA	External Certification Authority		

NOTE: Certificates must be numbered sequentially.

D-2.3 Optional Testing Prerequisites. The JITC PKI laboratory can test smart cards and/or tokens. If the ECA candidate wishes JITC to test these items, the candidate must provide the following:

- ECA-issued hardware tokens with ECA-issued keys and certificates present.
- Card readers.

Card reader's middleware.

- Hardware tokens.
- Passwords to download ECA-issued objects.
- Personal identification numbers for tokens and smart cards.

APPENDIX E

REFERENCES

E-1 "Certificate Policy for External Certification Authorities, V2.0," 4 June 2003.

Department of Defense Public Key Infrastructure
http://jitc.fhu.disa.mil/pki/appstatus.html. 14 May 2003.

(This page intentionally left blank.)

SUMMARY OF CHANGES TO THE DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE EXTERNAL CERTIFICATION AUTHORITY MASTER TEST PLAN VERSION 1.0

1. In Appendix B added footnotes to specify additional requirements for the values for the Authority Key Identifier (AKID) and the Subject Key Identifier (SKID) fields for the external certification authority (ECA) objects listed in a, b, c, and d.

a. Added the following footnote for the ECA Root certification authority (CA) Self-Signed Certificate Requirements: The value of the AKID field could be absent. If present, it must equal the value of the SKID field.

b. Added the following footnote for the ECA Subordinate CA Certificate Requirements: The value of the AKID field should be the same as the value of the SKID field in the ECA Root CA Self-Signed certificate.

c. Changed footnote from: The value of this field is the 20-byte secure hash algorithm (SHA)-1 hash of the binary distinguished encoding rule (DER) encoding of the signing CA's public key information to: The value of this field is the 20-byte SHA-1 hash of the binary DER encoding of the signing CA's public key information. The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate. This change was made for the following ECA objects:

- ECA Identity Certificate Requirements.
- ECA Encryption Certificate Requirements.
- ECA Component Certificate Requirements.
- ECA Code Signing Certificate Requirements.

d. Added the following footnote: The value of the AKID field must match the value of the SKID field in the ECA Subordinate CA certificate to the below ECA objects:

- ECA online certificate status protocol (OCSP) Responder Certificate Requirements.
- ECA Root CA certificate revocation list (CRL) Requirements.
- ECA Subordinate CA CRL Requirements.

2. Changed the order of ECA objects and placed revoked and expired ECA certificates at the end of the list to generalize their use (Pages 3 and C-1). These objects are referenced more specifically under the following sections:

- C-3.4 Revoked ECA Identity Certificate.
- C-3.5 Expired ECA Identity Certificate.
- C-3.7 Revoked ECA Encryption Certificate.
- C-3.8 Expired ECA Encryption Certificate.

3. Changed the value of the Name Constraints field in the profiles listed in tables B-1 through B-12 from: c=yes; permitted subtrees: ou=ECA-n, ou=contractor, ou=PKI, ou=DOD, o=U.S. Government, c=US to: c=no; permitted subtrees: ou=<ECA Company Name>, ou=ECA.

4. Added the following comments for the CRL Distribution Point field footnote in table B-2: It will point to the ECA Root issued CRL (Page B-3).

5. Changed values in the Subject Alternate Name field in the profile listed in table B-6 from: always present; c=no; cn=Name o=U.S. Government, c=US to: always present; c=no; cn=Name, cn=CompanyName (optional), ou=ECA-n, ou=Contractor, ou=PKI, ou=DoD, o=U.S. Government, c=US (Page B-7).

6. Added the word ECA to the following lines (Page C-2):

- Application shall validate an ECA Subordinate CA certificate.
- Load an ECA identity certificate into application.
- Application shall validate an ECA entity certificate.
- Application shall encrypt a test document using the ECA encryption certificate.
- Application shall decrypt a test document using the ECA encryption certificate.

7. Added the following lines under ECA Identity Certificate in Table C-1:

- Load an expired ECA identity certificate into application.
- Application shall reject the expired ECA identity certificate.

8. Added the following lines under ECA Encryption Certificate in Table C-1:

- Load a revoked ECA encryption certificate into application.
- Application shall reject the revoked ECA encryption certificate.
- Load an expired ECA encryption certificate into application.
- Application shall reject the expired ECA encryption certificate.

9. Changed name of ECA Web Server Certificate to ECA Component Certificate throughout the entire document.

10. Changed ECA Key Management (Encryption) Certificate to ECA Encryption Certificate, throughout the entire document.

11. Added AKID and SKID to the list of acronyms (Appendix A).

12. Changed name and date of ECA certificate policy from “Certificate Policy for External Certificate Authorities Version 0.7,” September 13, 2002, to "Certificate Policy

for External Certification Authorities, V2.0," 4 June 2003 to reflect new version throughout the entire document.

13. Added Revoked ECA Encryption Certificate, and Expired ECA Encryption Certificate in the Standards Compliance and Interoperability Test Prerequisites Table D-2 (Page D-2).

14. Changed quantity of certificates required for ECA Subordinate CA Certificate, and ECA Subordinate CA CRL from three to one in table D-2 (Page D-2).