



*DEFENSE INFORMATION SYSTEMS AGENCY*

*JOINT INTEROPERABILITY TEST COMMAND*
*FORT HUACHUCA, ARIZONA*

# DEPARTMENT OF DEFENSE ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER INTEROPERABILITY MASTER TEST PLAN VERSION 1.0

**JULY 2003**

# DEPARTMENT OF DEFENSE
# ONLINE CERTIFICATE STATUS
# PROTOCOL RESPONDER
# INTEROPERABILITY
# MASTER TEST PLAN
# VERSION 1.0

**JULY 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 Online Certificate Status Protocol (OCSP) allows Public Key Infrastructure-enabled (PKI-enabled) applications to verify the revocation status of an identified certificate by querying an OCSP Responder. OCSP Responders provide immediate and accurate revocation information on specific certificates rather than a lengthy list of certificate information in the form of Certificate Revocation Lists (CRLs).

An OCSP client submits a status request to an OCSP Responder and suspends acceptance of the certificate in question until the OCSP Responder provides a digitally signed response. The OCSP response indicates the status of the certificate by returning the value of "good," "revoked," or "unknown" (when the certificate status can not be determined).

The Joint Interoperability Test Command (JITC) will test OCSP Responders by using Department of Defense (DOD) Class 3 PKI test certificates and CRLs issued from the JITC PKI test Certificate Authority and Directory Server. Analysts will configure an OCSP-enabled client application to submit certificate validation requests to OCSP Responders. Analysts will introduce good, revoked, and unknown certificates to determine if OCSP Responders return accurate responses.

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

(This page intentionally left blank.)

## TABLE OF CONTENTS

## TABLE OF CONTENTS (continued)

## LIST OF TABLES

**Page**

## SYSTEM FUNCTIONAL DESCRIPTION

The Online Certificate Status Protocol (OCSP) is a response-request protocol used for obtaining online certificate revocation information from a trusted entity, referred to as an OCSP Responder. OCSP Responders provide immediate and accurate revocation information on specific certificates rather than a lengthy list of certificate information in the form of Certificate Revocation Lists (CRLs).

An OCSP client submits a certificate status request to an OCSP Responder and suspends acceptance of the certificate in question until the OCSP Responder provides a digitally signed response. The OCSP Responder signs all definitive responses to requests, providing an authoritative source for authentication and validation information. The OCSP response indicates the status of the certificate by returning the value of good, revoked, or unknown (when the certificate can not be identified). OCSP Responders return additional indicators that show the timeliness of the information returned in the response:

- thisUpdate - The time at which the status was known to be correct.
- nextUpdate - The time when newer status information will be available.
- producedAt - The time the OCSP Responder signed the request.

An OCSP Responder system consists of three components:

- Certificate Authority (CA) that issues and revokes certificates. The CA is the source of revocation data for the certificates they issue. The revocation data is usually in the form of a CRL. CAs periodically publish the CRLs to a Directory Server (DS).
- OCSP Responder that takes the bulk revocation data found in a CRL and translates it into individualized revocation information for a specified certificate. The OCSP Responder maintains the CRL it retrieves from the DS. When queried by an OCSP client about the status of a certificate, the OCSP Responder sends a digitally signed response.
- OCSP client application that submits certificate status requests to the OCSP Responder. The location of the OCSP Responder is manually configured at the client.

## TEST BACKGROUND

Department of Defense (DOD) CRLs are increasing in size and are bandwidth intensive. DOD organizations are therefore considering an OCSP architecture to improve certificate validation when compared with a purely CRL-based architecture.

Before use on a DOD network, all new public key components should be tested to ensure they interoperate with the current DOD Class 3 PKI. New OCSP Responders fall into this category.

## TEST PURPOSE

To determine if (OCSP RESPONDER) interoperates with the DOD Class 3 PKI.

## REQUIREMENTS

(OCSP RESPONDER) must meet the requirements listed in table 1 shown below. Detailed requirements are in appendix B. These requirements are derived from "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, Request for Comment (RFC) 2560," June 1999.

**Table 1. OCSP Responder Interoperability Requirements**

| Function | Requirements |
|---|---|
| OCSP Requests | OCSP Responder shall be capable of handling OCSP requests. |
| | OCSP Responder shall be capable of handling signed OCSP requests. |
| | OCSP Responder shall be capable of handling OCSP requests that contain multiple certificates under the service request list. |
| OCSP Responses | OCSP Responder shall return an OCSP-signed response. |
| | OCSP Responder may support OCSP request extensions. |
| Retrieving CRL | OCSP Responder shall be capable of retrieving CRLs from the DOD Class 3 PKI. |
| Verifying Communications Protocol | OCSP Responder shall be capable of communicating with the OCSP client using HTTP, and HTTPS. |
| | OCSP Responder shall be capable of communicating with the DOD Class 3 PKI using HTTP, HTTPS, LDAP, and LDAPS. |
| Legend | |
| CRL | Certificate Revocation List |
| DOD | Department of Defense |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol over Secure Socket Layer |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | Lightweight Directory Access Protocol over Secure Socket Layer |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |

## SCOPE

JITC will determine if (OCSP RESPONDER) interoperates with the DOD Class 3 PKI using the JITC test CA and DS. JITC will issue PKI software certificates from the JITC CA. Analysts will use good, revoked, and unknown certificates to determine if (OCSP RESPONDER) provides accurate responses. JITC will conduct the test at its PKI laboratory at Fort Huachuca, Arizona, and/or at the vendor's site, as applicable, from (DATE) through (DATE).

The (OCSP RESPONDER) will use a self-signed certificate because the DOD Class 3 PKI currently does not support OCSP Responder certificates. The OCSP client application must trust the OCSP Responder self-signed certificate. JITC will use hardware security modules to generate, store, and protect cryptographic keys.

## METHODOLOGY

To determine if (OCSP RESPONDER) interoperates with the DOD Class 3 PKI. Specifically, the test will exercise (OCSP RESPONDER)'s capability to validate DOD Class 3 PKI software certificates issued from the JITC CA.

Analysts will download test certificates, the root CA certificate, and (OCSP RESPONDER) certificate. Analysts will configure an OCSP-enabled client application to submit certificate validation requests to (OCSP RESPONDER). Analysts will introduce good, revoked, and unknown certificates to determine if (OCSP RESPONDER) responds accurately. Analysts will also determine the OCSP request format and the OCSP response format by transmitting and capturing the requests and responses using Open Secure Socket Layer. Analysts will determine if the OCSP responses are digitally signed and consist of the certificate identifier, the certificate status, and the validity interval of the response associated with each certificate identifier specified within the original request.

## PRESENTATION OF RESULTS AND ANALYSIS PROCEDURES

Analysts will examine the test results of each test event to determine if (OCSP RESPONDER) interoperates with the DOD Class 3 PKI. The test report will present the test results in text and in a table similar to table 2.

## Table 2. OCSP Responder Interoperability Test Results

| Function | Criteria | Results | Status |
|---|---|---|---|
| OCSP Requests | OCSP Requests | | |
| | OCSP-signed Requests | | |
| | Multiple Certificate Status Requests | | |
| OCSP Responses | OCSP-signed Responses | | |
| | OCSP Request Extensions | | |
| Retrieving CRLs | Retrieve 2 MB CRL from DOD CLASS 3 PKI | | |
| | Retrieve 4 MB CRL from DOD CLASS 3 PKI | | |
| | Retrieve 8 MB CRL from DOD CLASS 3 PKI | | |
| Verifying Communications Protocol | OCSP Responder to OCSP Client | | |
| | OCSP Responder to the DOD CLASS 3 PKI | | |

Legend

| | |
|---|---|
| CRLs | Certificate Revocation Lists |
| DOD | Department of Defense |
| MB | Megabyte |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |

(This page intentionally left blank.)

## APPENDIX A

## ACRONYMS

| | |
|---|---|
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| DOD | Department of Defense |
| DS | Directory Server |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol over Secure Socket Layer |
| JITC | Joint Interoperability Test Command |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | Lightweight Directory Access Protocol over Secure Socket Layer |
| MB | Megabyte |
| OCSP | Online Certificate Status Protocol |
| RFC | Request for Comment |
| PKI | Public Key Infrastructure |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |

(This page intentionally left blank.)

# APPENDIX B

# TEST CRITERIA, PROCEDURES, AND DATA REQUIRED

## GENERAL TEST INFORMATION

**Test Conduct.** Test analysts will determine if the (Online Certificate Status Protocol (OCSP) RESPONDER) interoperates with the Department of Defense (DOD) Class 3 Public Key Infrastructure (PKI) using the requirements derived from "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, Request for Comment 2560," June 1999. As test analysts execute each test procedure, they will capture screen-shots and each OCSP request and OCSP response in a text format for analysis during and after the test. Analysts will determine the Pass/Fail status for each test procedure's test event.

**Data Collection.** Test analysts will perform a visual inspection of each OCSP request and OCSP response and compare them with the OCSP response and request format in tables B-1 and B-2.

### Data Requirements for All Subtests

**a. Criterion Related**

(1) Communications protocol used between the test workstations and the JITC PKI test lab.

(2) Test certificates used.

(3) Detailed network diagram.

(4) System hardware and operating systems and software for test workstations.

**b. Supplemental.** Test dates, location, and type of testing.

## B-1 OCSP REQUESTS

**B-1.1 Objective.** To determine (OCSP RESPONDER)'s capability to accept OCSP requests.

### B-1.2 Criteria

**a. OCSP Requests.** (OCSP RESPONDER) shall be capable of accepting OCSP requests that contain the protocol version, service request, and target certificate identifiers. (OCSP RESPONDER) shall determine if the request is well formed, if the request contains information needed by the OCSP Responder, and if the OCSP Responder is configured to provide the requested service. If one of these conditions is not met, the (OCSP RESPONDER) shall produce an error message; otherwise, it shall return a definitive response. Table B-1 shows the OCSP request format. [Reference 2.1 in RFC 2560, page 2]

**Table B-1. OCSP Request Format**

| Field | Expected Value |
|---|---|
| Protocol Version | V1 (0) |
| Requestor Name | Optional |
| Service Request List | List of certificates |
| Extensions | Optional |
| Signature | Optional |

**b. OCSP-signed Requests.** (OCSP RESPONDER) shall be capable of handling OCSP requests that are signed and include a specified name in the *requestorName* field. [Reference 4.1.2 in RFC 2560, page 8]

**c. Multiple Certificate Status Requests.** (OCSP RESPONDER) shall be capable of accepting OCSP requests that contain multiple certificates under the service request list. [Reference 2.2 in RFC 2560, page 3]

### B-1.3 Test Procedures

**a. OCSP Requests.** Analysts will determine if (OCSP RESPONDER) can provide a definitive and accurate response to an unsigned request by:

(1) Sending an unsigned OCSP request to (OCSP RESPONDER).

(2) Determining if (OCSP RESPONDER) provides a definitive and accurate response.

(3) Sending an unsigned OCSP request that contains the wrong protocol version.

(4) Determining if (OCSP RESPONDER) provides the correct error message.

(5) Sending an unsigned OCSP request that contains invalid certificates in the service request list.

**b. OCSP-signed Requests.** Analysts will determine if (OCSP RESPONDER) can provide a definitive and accurate response to a signed request that includes a specified name in the *requestorName* field by:

(1) Sending a signed OCSP request to (OCSP RESPONDER).

(2) Determining if (OCSP RESPONDER) provides a definitive and accurate response.

**c. Multiple Certificate Status Requests.** Analysts will determine if (OCSP RESPONDER) can provide a definitive and accurate response to requests that include multiple certificates under the service request list by:

(1) Sending an OCSP request containing multiple certificates to (OCSP RESPONDER).

(2) Determining if (OCSP RESPONDER) can provide a definitive and accurate response for each of the certificates listed in the request.

### B-1.4 Criteria-related Data Requirements

**a. OCSP Requests.** OCSP request.

**b. OCSP-signed Requests.** PKI certificate used to sign OCSP request.

**c. Multiple Certificate Status Requests.** OCSP request with multiple certificates.

## B-2 OCSP RESPONSES

**B-2.1 Objective.** To determine (OCSP RESPONDER)'s capability to provide an accurate response to OCSP requests.

**B-2.2 Criteria**

**a. OCSP-signed Responses.** (OCSP RESPONDER) responses shall consist of the certificate identifier, the certificate status, and the validity interval of the response associated with each certificate identifier specified within the original request. Table B-2 shows the OCSP response format.

**Table B-2. OCSP Response Format**

| Field | Expected Value |
|---|---|
| Response Status | Successful \| Malformed Request \| Internal Error \| Try Later |
| Response Type | Id-pkix-ocsp-basic {1 3 6 1 5 5 7 4 8 1 1} |
| Version | V1 (0) |
| Responder ID | Hash of responder public key |
| Produced At | Generalized Time |
| Responses<br>CertId<br>Cert Status<br>ThisUpdate<br>NextUpdate | Each response will contain certificate id, certificate status, thisUpdate, and nextUpdate from the Certificate Authority Certificate Revocation List |
| Signature Algorithm | SHA1 with Rivest, Shamir and Adleman (RSA) Encryption {1 2 840 113549 1 1 5} |
| Signature | Present |
| Extensions<br>Nonce<br>CRL Reference<br>Acceptable Response Type<br>Archive Cutoff | |
| Certificates | Applicable certificates issued to the OCSP Responder |

The (OCSP RESPONDER) must support the following:

(1) The Secure Hash Algorithm 1 (SHA1).
[Reference 4.3 in RFC 2560, page 11]

(2) The key used to sign the response must belong to a trusted (OCSP RESPONDER) whose public key is trusted by the OCSP client submitting the request. [Reference 2.2 in RFC 2560, page 3]

(3) Produce responses of the *id-pkix-ocsp-basic* response type. [Reference 4.2.1 in RFC 2560, page 9]

(4) Reflect the time at which the status was known to be correct in *thisUpdate* field of the response if (OCSP RESPONDER) produces pre-signed responses. [Reference 2.5 in RFC 2560, page 5]

(5) Provide the time at which the status being indicated is known to be correct in the *thisUpdate* field. [Reference 2.4 in RFC 2560, page 4]

(6) Provide the time at or before newer information will be available about the status of the certificate in the *nextUpdate* field. [Reference 2.4 in RFC 2560, page 4]

(7) Provide the time at which (OCSP RESPONDER) signed the response in the *producedAt* field. [Reference 2.4 in RFC 2560, page 4]

**b. OCSP Request Extensions.** If an (OCSP RESPONDER) is capable of handling the following OCSP extensions, it shall do so as required:

(1) Nonce. (OCSP RESPONDER) will include the nonce in the responseExtension if the nonce is included in the requestExtension in the OCSP request. The nonce will be identified by the object identifier id-pkix-ocsp-nonce, and the extnValue will be the value of the nonce. [Reference 4.4.1 in RFC 2560, page 12]

(2) CRL Reference. (OCSP RESPONDER) will include CRL references if the certificate status is revoked. The identifier for this extension will be id-pkix-csp-crl, with the value of CrlId. [Reference 4.4.2 in RFC 2560, page 12]

(3) Acceptable Response Type. (OCSP RESPONDER) shall be capable of responding to OCSP requests of the id-pkix-ocsp-basic response type. The acceptable response type will be identified by the object identifier id-pkix-ocsp-response and the AcceptableResponse will be the value of the acceptable response type. [Reference 4.4.3 in RFC 2560, page 12]

(4) Archive Cutoff. (OCSP RESPONDER) shall provide an archive cutoff date extension in the OCSP singleExtension field identified by the id-pkix-ocsp-archive-cutoff and of syntax GeneralizedTime if the (OCSP RESPONDER) chooses to retain revocation information beyond the certificate's expiration. [Reference 4.4.4 in RFC 2560, page 13]

### B-2.3 Test Procedures

**a. OCSP-signed Responses.** (OCSP RESPONDER) will:

(1) Transmit an OCSP signed response using SHA1.

(2) Transmit digitally signed definitive and accurate response messages and determine if the key used to sign the response belonged to a trusted OCSP Responder whose public key was trusted by the OCSP client submitting the request.

(3) Transmit OCSP responses of the *id-pkix-ocsp-basic* response type.

(4) Transmit OCSP responses that provide the time at which the status was known to be correct in *thisUpdate* field of the response if (OCSP RESPONDER) produces pre-signed responses.

(5) Transmit OCSP responses that provide an archive cutoff date extension in the OCSP *singleExtension* field identified by *the id-pkix-ocsp-archive-cutoff* and of syntax *GeneralizedTime* if (OCSP RESPONDER) chose to retain revocation information beyond the certificate's expiration.

(6) Transmit OCSP responses that provide the time at which the status being indicated was known to be correct in the *thisUpdate* field.

(7) Transmit OCSP responses that provide the time at or before newer information was available about the status of the certificate in the *nextUpdate* field.

**b. OCSP Response Extensions**. If an (OCSP RESPONDER) is capable of handling the following OCSP extensions, it shall do so as required:

(1) Nonce

(a) Transmit an OCSP request that includes the nonce extension.

(b) Transmit an OCSP response that includes the nonce extension.

(2) CRL Reference

(a) Transmit an OCSP request that specifies a revoked certificate.

(b) Transmit an OCSP response that includes the CRL reference for the revoked certificate contained in the OCSP request.

(3) Acceptable Response Type

(a) Transmit an OCSP request specifying the acceptable response type of the id-pkix-ocsp-basic response type.

(b) Transmit an OCSP response of the id-pkix-ocsp-basic response type.

(4) Archive Cutoff. Transmit an OCSP response that includes the archive cutoff date extension in the OCSP singleExtension field.

### B-2.4 Criteria-related Data Requirements

#### a. OCSP-signed Responses

(1) OCSP signed response that used the SHA1 hashing algorithm.

(2) Digitally signed definitive OCSP response.

(3) OCSP response of the id-pkix-ocsp-basic response type.

(4) OCSP pre-signed response.

(5) OCSP response that includes an archive cutoff date extension.

(6) OCSP response that has the *thisUpdate* field present.

(7) OCSP response that has the *nextUpdate* field present.

#### b. OCSP Response Extensions

(1) Nonce. OCSP response with the nonce extension present.

(2) CRL Reference. OCSP response with the CRL reference present.

(3) Acceptable Response Type. OCSP response in the id-pkix-ocsp-basic response type.

(4) Archive Cutoff. OCSP response with the archive cutoff date extension present.

## B-3 RETRIEVING CERTIFICATE REVOCATION LISTS

**B-3.1 Objective.** To determine (OCSP RESPONDER)'s capability to download CRLs from the DOD Class 3 PKI Directory Server (DS) and Certificate Authority (CA).

**B-3.2 Criteria.** The (OCSP RESPONDER) shall be capable of retrieving large CRLs from the DOD CLASS 3 PKI. (OCSP RESPONDER) shall be capable of providing OCSP responses for these CRLs. Test analysts will determine if the (OCSP RESPONDER):

**a.** Retrieves a 2-megabyte (MB) CRL from the DOD CLASS 3 PKI.

**b.** Retrieves a 4-MB CRL from the DOD CLASS 3 PKI.

**c.** Retrieves an 8-MB CRL from the DOD CLASS 3 PKI.

**B-3.3 Test Procedures.** The OCSP Responder will retrieve a:

**a.** 2-MB CRL from the DOD CLASS 3 PKI.

**b.** 4-MB CRL from the DOD CLASS 3 PKI.

**c.** 8-MB CRL from the DOD CLASS 3 PKI.

**B-3.4 Criteria-related Data Requirements**

**a.** 2-MB CRL from the DOD CLASS 3 PKI.

**b.** 4-MB CRL from the DOD CLASS 3 PKI.

**c.** 8-MB CRL from the DOD CLASS 3 PKI.

## B-4 VERIFYING COMMUNICATIONS PROTOCOL

**B-4.1 Objective.** To determine if (OCSP RESPONDER) uses multiple communication protocols to communicate with the DOD CLASS 3 PKI.

### B-4.2 Criteria

**a. OCSP Responder to OCSP Client.** (OCSP RESPONDER) shall be capable of communicating with the OCSP client using Hypertext Transmission Protocol (HTTP) and HTTP over Secure Socket Layer (HTTPS).

**b. OCSP Responder to the DOD CLASS 3 PKI.** (OCSP RESPONDER) shall be capable of communicating with the DOD Class 3 PKI using HTTP, HTTPS, Lightweight Directory Access Protocol (LDAP) and LDAP over Secure Socket Layer (LDAPS).

### B-4.3 Test Procedures

**a. OCSP Responder to OCSP Client.** The (OCSP RESPONDER) will:

(1) transmit OCSP responses using HTTP.

(2) transmit OCSP responses using HTTPS.

**b. OCSP Responder to the DOD CLASS 3 PKI.** The (OCSP RESPONDER) will:

(1) retrieve a CRL from the DOD Class 3 PKI using HTTP.

(2) retrieve a CRL from the DOD Class 3 PKI using HTTPS.

(3) retrieve a CRL from the DOD Class 3 PKI using LDAP.

(4) retrieve a CRL from the DOD CLASS 3 PKI using LDAPS.

### B-4.4 Criteria-related Data Requirements

**a. OCSP Responder to OCSP Client**

(1) OCSP responses using HTTP.

(2) OCSP responses using HTTPS.

**b. OCSP Responder to DOD CLASS 3 PKI**

(1) CRL retrieved from the DOD CLASS 3 PKI using HTTP.

(2) CRL retrieved from the DOD CLASS 3 PKI using HTTPS.
(3) CRL retrieved from the DOD CLASS 3 PKI using LDAP.

(4) CRL retrieved from the DOD CLASS 3 PKI using LDAPS.

(This page intentionally left blank.)

# APPENDIX C

# TEST RESOURCES

## C-1 TEST RESOURCES

**C-1.1 Test Sites and Facilities.** The Joint Interoperability Test Command (JITC) will test (Online Certificate Status Protocol (OCSP) RESPONDER) at the JITC Public Key Infrastructure (PKI) laboratory at Fort Huachuca, Arizona, and/or at the vendor's site, as applicable, from (DATE) through (DATE).

**C-1.2 Test Equipment/Network.** Analysts will configure an OCSP-enabled client workstation and an OCSP Responder to conduct interoperability tests. Figure C-1 shows a typical test configuration.

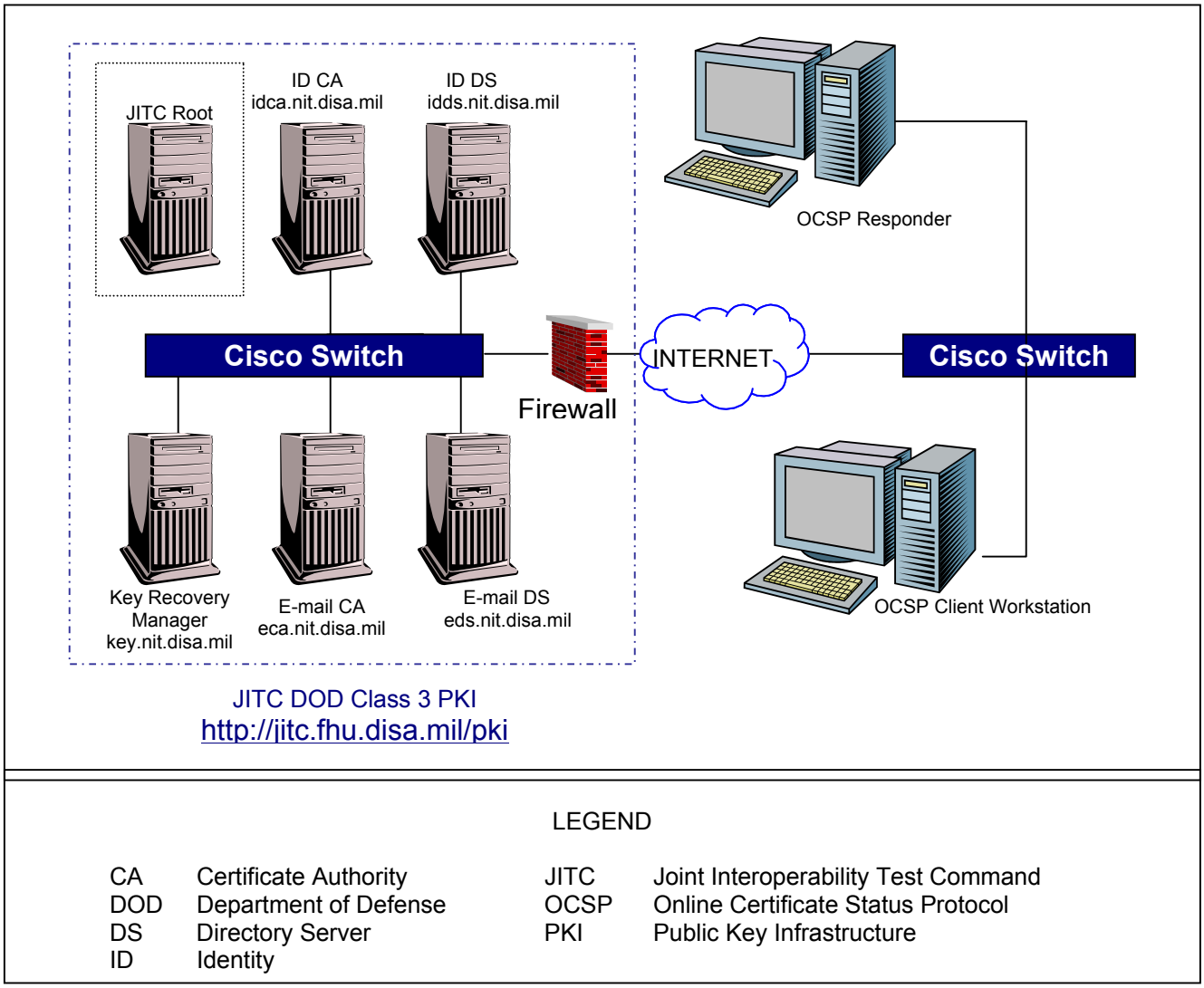


**Figure C-1. (OCSP RESPONDER) Test Configuration**

**C-2 PERSONNEL REQUIREMENTS.** The number of test analysts required depends on the test requirements and/or the test equipment. Table C-1 shows the number of personnel required for a typical test.

**Table C-1. Personnel Requirements for a Typical Test**

| Function | Number | Source |
|---|---|---|
| Test Analyst/Data Collector | 1 | JITC |
| Operator | 1 | JITC |

**C-3 SOFTWARE DESCRIPTIONS.** The test report will describe the OCSP Responder being tested, version numbers, and any patches or upgrades.

# APPENDIX D

# REFERENCES

## D-1 REQUEST FOR COMMENT 2560

"X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, Request for Comment 2560," June 1999.

(This page intentionally left blank).

# APPENDIX E

## POINTS OF CONTACT

JITC PKI Web Site:

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

Government POC:

**Ms. Gretchen Dixon**
JITC PKI Test Officer
(520) 538-5439, DSN 879-5439
E-mail: dixong@fhu.disa.mil

Interoperability Testing POC:

**Mr. Brannon Biehl**
PKE Technical Lead
(520) 538-1709, DSN 879-1709
E-mail: biehlb@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.)