# Conformance Testing of Relying Party Client Certificate Path Processing Logic

**Version 1.07**

**September 28, 2001**


**Suite 100 West♦7927 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960**

# TABLE OF CONTENTS

# 1 INTRODUCTION

## *1.1 Background*

The Department of Defense (DoD) is deploying Class 3 and Class 4 Public Key Infrastructure (PKI). The DoD and the DoD partners will rely on the commercial relying party PKI software and Applications Programming Interface (API) to perform the certification path validation. In order to ensure secure interoperation of the PKI enabled applications, the path validation must be done in accordance with the X.509 standard. This document provides the test assertions and the test cases for testing the path validation software.

## *1.2 Scope and Objective*

The objective of this document is to test the path validation logic.

The scope excludes testing whether certificates and Certificate Revocation Lists (CRLs) have been generated in accordance with any particular standard or profile such as X.509, PKIX, Federal Profile, or DoD Class 3 or Class 4 profile.

The scope also excludes testing of the client software to appropriately parse certificates and CRLs. The ability of the client software to appropriately parse certificates and CRLs will be tested to the extent that the certificates and CRLs need to be parsed during the path processing.

In summary, the assertions and test cases are NOT meant to exercise the client software's ability to handle correctly and incorrectly generated and coded certificates and CRLs.

## *1.3 Assumptions*

The following assumptions are used in generating the assertions and the test cases:

1. The certificates and CRLs are signed with the same Certification Authority (CA) using the same private key. Thus, the issuer Distinguished Name (DN) in the certificate and the issuer DN in the CRL must match. Furthermore, there is no need to develop a certification path for validating signatures on the CRL. In fact, the same public key used to validate the signature on a certificate MUST be used to validate the signature on the CRL.
2. The Issuing Distribution Point (IDP) and delta CRL indicator extensions are out of the scope of this document. A test including each extension has been included, which should fail whether or not the IDP or delta CRL indicator extensions are properly implemented.
3. The path processing logic used is from the X.509 2000 version.
4. The trust anchor certificate is not included in the certification path. Thus, the only inputs from the trust anchor to the certification path validation logic are the trust anchor DN and the trust anchor public key.
5. There are no self-issued certificates in the certification path. In other words, if a trust anchor rekeys, the subscribers have already replaced the old public key of

the trust anchor with the new public key of the trust anchor; the intermediate CA rekey by obtaining new certificates from the CAs that certify them.

6. The following extensions and their values will not be tested during path validation in this version of the test document: authority key identifier, subject key identifier, private key usage period, issuer alternative name, subject alternative name, and name constraints. Future versions of this document may contain tests that exercise these extensions.
7. Since the part of the 1997 defect resolution was to eliminate the processing differences between non-critical Certificate Policies extension and critical Certificate Policies extension, the tests assume that the certificate policies (and other extensions) will be processed the same way regardless of their criticality. In other words, 2000 path validation logic will be used.
8. The basic constraints extension must be present in all intermediate certificates (i.e., in CA certificates). This is a direct requirement of X.509 2000, reprinted here for emphasis.
9. The basic constraints extension may or may not be present in the end certificate. The path validation logic must not reject this certificate on the basis of the presence of this extension. The software may reject this certificate if the certificate contains a critical basic constraints extension and the software does not process this extension. But, in that case (see the previous assumption), the software is only capable of processing certification paths of length 1.
10. This version of the document only considers certificates signed with the RSA algorithm. DSA signatures and keys, cross-algorithm certificates, and the complications added by parameters and parameter inheritance are out of the scope of this document.
11. This version of the document assumes that applications will treat a CRL as a valid CRL if it contains a **nextUpdate** later than the current date. If the application decides CRL validity using another method (such as a delta from the **thisUpdate** date) the testers may need to configure the application and system so that the test data is acceptable to the local CRL policy. If the application rejects good paths (particularly if the operator is informed that the rejection is due to the lack of acceptable revocation information) the tester should attempt the following: (a) configure the application to allow CRLs with a **thisUpdate** of Jan. 1, 1999 (b) configure the system time to be Jan. 1, 1999.

## *1.4 Document Conventions*

### 1.4.1 Assertions

Sections 3 and 4 of this document correspond to requirements with X.509 related to Certificates and Certificate Revocation Lists, respectively. Within these sections, the corresponding interoperability and security requirements from X.509 are divided into a set of assertions. These assertions are statements that must be true in order for the software being tested to satisfy a given requirement of the X.509 path validation procedure. As appropriate, assertions will also contain a reference to the appropriate section and quote from X.509. Assertions are of the form:

**AS**:<requirement_type>.<assertion_sequence_number>

where “requirement_type” is an abbreviation for the type of requirement, and “assertion_sequence_number” is a sequential identifier for assertions within a requirement type. Possible values for the requirement type are **CP** (certificate processing), **IC** (intermediate certificate processing), **PP** (policy processing), **PL** (path length), **RL** (revocation list).

### 1.4.2 Testing Requirements

Following each assertion is a set of testing requirements. These requirements instruct the tester as to what he or she must do in order to test the software with respect to the given assertion. These requirements are denoted by the form:

**TE**:<requirement_type>.<assertion_sequence_number>.<sequence_number>

where “requirement_type” and “assertion_sequence_number” are identical to the corresponding assertion requirement type and assertion sequence number, and “sequence_number” is a sequential identifier for tester requirements within the assertion requirement.

### 1.4.3 Testing Levels

Following each test requirement is a testing level number, for example:

**TE:CP.01.01, Level 1**

indicates that test TE:CP.01.01 is a level 1 test. There are three levels assigned to tests in this document, as follows:

**Level 0**: No tests to run for this test requirement.
**Level 1**: Must run described test(s) to successfully test interoperability and security
**Level 2**: Described test(s) provide further assurance that the application will be interoperable and secure. Should be used to test applications if possible within scheduling and budgetary constraints.
**Level 3**: Described test(s) used to pinpoint a problem in the application. If an application fails certain level 1 or 2 tests, the level 3 tests should be provided to the application developer to assist with debugging and repair. These tests should not be run by the Government.

### 1.4.4 Test Data

Section 5 of this document contains descriptions of the test data that is required by the testing requirements. Each test requirement contains hyperlinks to the descriptions of the appropriate test data object(s).

Some of the tests depend on the value of specific inputs to the path processing procedure, as described by X.509. Due to space constraints, it is best to abbreviate the settings. The following describes the abbreviations and their meanings.

| **Abbreviation** | **Meaning** |
|---|---|
| ipolset | *initial-policy-set* |
| explicit | *initial-explicit-policy* indicator |
| inhibit | *initial-policy-mapping-inhibit* indicator |

### *1.5 Document Revision History*

| Version | Date | Modifier | Changes |
|---|---|---|---|
| 0.1 | 07/31/2000 | Santosh Chokhani, Peter Hesse, CygnaCom Solutions | Initial draft to get feedback on format |
| 0.2 | 08/04/2000 | Santosh Chokhani, Peter Hesse, Daun-Marie Curts, CygnaCom Solutions | First complete draft |
| 0.3 | 08/23/2000 | Peter Hesse, CygnaCom Solutions | Second draft, based on comments from David Cooper, NIST and Rich Nicholas, WGSI |
| 0.4 | 08/25/2000 | Peter Hesse, CygnaCom Solutions | Minor update, based on feedback from David Cooper, NIST |
| 0.9 | 09/19/2000 | Peter Hesse, CygnaCom Solutions | Updated based on feedback from David Cooper and Tim Polk, NIST. Removed overlapping tests, prioritized remaining tests |
| 0.91 | 09/22/2000 | Peter Hesse, CygnaCom Solutions | Updated based on feedback from Pierce Leonberger, WGSI. |
| 1.0 | 09/22/2000 | Peter Hesse, CygnaCom Solutions | Updated based on feedback from David Cooper, NIST. |
| 1.01 | 09/26/2000 | Peter Hesse, CygnaCom Solutions | Minor update, based on feedback from David Cooper, NIST and Pierce Leonberger, WGSI. |
| 1.02 | 09/28/2000 | Peter Hesse, CygnaCom Solutions | Minor update, based on feedback from David Cooper, NIST and Pierce Leonberger, WGSI. |
| 1.03 | 10/03/2000 | Peter Hesse, CygnaCom Solutions | Minor update, based on feedback from Pierce Leonberger, WGSI. |
| 1.04, 1.05, 1.06 | 10/05/2000, 10/06/2000, 11/06/2000 | Peter Hesse, CygnaCom Solutions | Updated based on feedback from David Cooper, NIST. |
| 1.07 | 09/28/2001 | David Cooper, NIST | Updated references to X.509. Sequentially numbered tests. |

# 2 DEFINITIONS

This section contains some of the definitions used in this document.

**CA Certificate:** A public key certificate whose subject is a CA.

**Certificate Chain:** See **Certification Path**

**Certificate Extension:** A field not within the original ASN.1 definition of **Certificate** which adds additional information to a certificate.

**Certificate Extension Criticality:** An extension can be marked critical by the signer. When an implementation processing a certificate does not recognize an extension, if the criticality flag is **FALSE**, it may ignore that extension. If the criticality flag is **TRUE**, unrecognized extensions shall cause the structure to be considered invalid.

**Certificate Path:** See **Certification Path**

**Certificate Serial Number:** A field in a certificate containing an integer assigned by the CA to each certificate. The value of **serialNumber** must be unique for each certificate issued by a given CA.

**Certification Path:** A chain of certificates starting from a certificate issued by the trust anchor of the relying party and ending with the certificate issued to the subject of interest to the relying party. A Certification Path consists of 0 or more **Intermediate Certificates** and 1 **End Certificate.** The first certificate in the Certification Path of length greater than 1 is also called **Intermediate Certificate**. The first certificate in the Certification Path of length 1 is called **End Certificate** since it the last certificate in the Certification Path.

**Certification Path Length:** The number of certificates in a **Certification Path**. Please note that in the basic constraints extension path length of n means n+1 certificates may follow.

**Current Time:** The current time is an input into the certificate path validation process, and should be calculated by the best available means; preferably (but not necessarily) a trusted time source.

**Delta CRL:** A CRL that provides updates to a referenced base CRL. The combination of a Delta CRL and the referenced base CRL constitute a full and complete CRL.

**Distinguished Name:** A unique name that identifies an entity. A distinguished name is made up of one or more relative distinguished names (RDNs).

**Distinguished Name Equality:** Distinguished names are equal if the ordered set of RDNs in one are equal to the ordered set of RDNs in the other. X.501 section 9.4 contains detailed information on “name matching”.

**End Certificate:** The last certificate in a **Certificate Chain.** The certificate could be a **CA Certificate** or an **End Entity Certificate**.

**End Entity Certificate:** A public key certificate whose subject is not a CA

**Intermediate Certificate:** Any certificate in a **Certificate Chain** except for the **End Certificate**. Please note that an Intermediate Certificate must be issued to a CA and hence it must be a **CA Certificate**.

**issuer:** A field in a certificate which identifies the entity that has signed and issued the certificate.

**notAfter:** A field in a certificate that contains a date and time after which the certificate can no longer be used.

**notBefore:** A field in a certificate that contains a date and time that the certificate can begin to be used.

**Signature:** A signature is an cryptographic calculation of information to provide source authentication and data integrity. The calculation is produced by first hashing the information, and then calculating a cryptographic function of the hash and the private key of the signer.

**Signature Verification:** A signature verification is an cryptographic calculation of information to validate source authentication and data integrity. The calculation is produced by first hashing the information, and then calculating a cryptographic function of the hash, signature and the public key of the signer.

**subject:** A field in a certificate which identifies the entity associated with the public-key found in the subject public key field.

**Subordinate:** An entity that has had its certificate signed by a superior.

**Superior:** A certificate signer.

# 3 CERTIFICATE TESTING

## *3.1 Certificate Processing Tests*

The certificate processing tests, denoted with **CP** in the assertion and test case numbers, deal with the processing of every certificate within the certificate path. This includes all intermediate certificates and the end certificate in the path. The trust anchor is not considered, because the inputs from the trust anchor should solely be a public key and distinguished name.

**AS:CP.01**

The application must verify digital signatures on each certificate in the certification path using the superior public key.

[X.509 10.5.1]Check that the signature verifies

**Test 1: TE:CP.01.01, Level 1**

The following path should be successfully validated, all signatures and data are correct:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, End Certificate CP.01.01

**Test 2: TE:CP.01.02, Level 1**

The following path should not validate successfully. The signature on the intermediate certificate is invalid.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.01.02, Intermediate CRL CP.01.02, End Certificate CP.01.02

**Test 3: TE:CP.01.03, Level 1**

The following path should not validate successfully. The signature on the end certificate is invalid.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.01.03, Intermediate CRL CP.01.03, End Certificate CP.01.03

**AS:CP.02**

The application must ensure that the **notBefore** time of each certificate in the certification path must be earlier than the current time.

[X.509 10.5.1] (Check that) that dates are valid

**Test 4: TE:CP.02.01, Level 1**

The following path should be successfully validated; all certificates have **notBefore** earlier than current time :

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, , Intermediate CRL 1 CP.02.01, Intermediate Certificate 2 CP.02.01, Intermediate CRL 2 CP.02.01, End Certificate CP.02.01

**Test 5: TE:CP.02.02, Level 1**

The following path should not validate successfully. The intermediate certificate has a **notBefore** later than current time:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.02.02, Intermediate CRL CP.02.02, End Certificate CP.02.02

**Test 6: TE:CP.02.03, Level 2**

The following path should not validate successfully. The end certificate has a **notBefore** later than current time:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.02.03, Intermediate CRL CP.02.03, End Certificate CP.02.03

**Test 7: TE:CP.02.04, Level 2**

The following path should be successfully validated; the end certificate has a **notBefore** set as a UTC time with a year of 50. (Client should treat as 1950)

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.02.04, Intermediate CRL CP.02.04, End Certificate CP.02.04

**Test 8: TE:CP.02.05, Level 2**

The following path should not validate successfully. The end certificate has a **notBefore** set as a generalized time with a year of 2050:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.02.05, Intermediate CRL CP.02.05, End Certificate CP.02.05

**AS:CP.03**

The application must ensure that the **notAfter** time of each certificate in the certification path must be later than the current time.

**Test 9: TE:CP.03.01, Level 1**

The following path should not validate successfully. The intermediate certificate has a **notAfter** earlier than current time:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.03.01, Intermediate CRL CP.03.01, End Certificate CP.03.01

**Test 10: TE:CP.03.02, Level 2**

The following path should not validate successfully. The end certificate has a **notAfter** earlier than current time:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.03.02, Intermediate CRL CP.03.02, End Certificate CP.03.02

**Test 11: TE:CP.03.03, Level 2**

The following path should not be successfully validated; the end certificate has a **notAfter** set as a UTC time with a year of 50. (Client should treat as 1950)

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.03.03, Intermediate CRL CP.03.03, End Certificate CP.03.03

**Test 12: TE:CP.03.04, Level 1**

The following path should be successfully validated; the end certificate has a **notAfter** set as a generalized time with a year of 2050.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.03.04, Intermediate CRL CP.03.04, End Certificate CP.03.04

**AS:CP.04**

The application must check that names chain correctly. Correct chaining is when the **issuer** of each certificate in the certificate path is equal to the **subject** of the superior certificate. (In the case of the first intermediate certificate in the path, the **issuer** of the certificate must be equal to the trusted anchor name).

[X.509 10.5.1] (Check) that the certificate subject and certificate issuer names chain correctly

**Test 13: TE:CP.04.01, Level 1**

The following path should not be successfully validated; the names that do not chain: (cn=A vs. cn=B):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.01, Intermediate CRL CP.04.01, End Certificate CP.04.01

**Test 14: TE:CP.04.02, Level 1**

The following path should not be successfully validated; the names differ by order (cn=A, ou=People, o=Org vs. cn=A, o=Org, ou=People):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.02, Intermediate CRL CP.04.02, End Certificate CP.04.02

**Test 15: TE:CP.04.03, Level 1**

The following path should be successfully validated; the names differ only by whitespace and capitalization which should be insignificant:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.03, Intermediate CRL CP.04.03, End Certificate CP.04.03

**Test 16: TE:CP.04.04, Level 3**

The following path should be successfully validated; the names differ only by whitespace (cn=My Name vs. cn=My Name):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.04, Intermediate CRL CP.04.04, End Certificate CP.04.04

**Test 17: TE:CP.04.05, Level 3**

The following path should be successfully validated; the names differ only by leading/trailing whitespace [quotes added for clarity] (cn=" My Name" vs. cn="My Name "):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.05, Intermediate CRL CP.04.05, End Certificate CP.04.05

**Test 18: TE:CP.04.06, Level 3**

The following path should be successfully validated; the names differ only by capitalization (cn=A vs. cn=a):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.04.06, Intermediate CRL CP.04.06, End Certificate CP.04.06

**TE:CP.04.07, Level 0**

(out of scope for current document)

Test values other than printableString in the distinguished name fields, such as teletexString, bMPString, utf8String.

**AS:CP.05**

The application must be able to retrieve valid revocation data[1] for each certificate in the certificate path; if the application is unable to retrieve valid revocation data, it must reject the certificate path.

[X.509 10.5.1] (Check) that the certificate has not been revoked.

**Test 19: TE:CP.05.01, Level 1**

The following path should not be successfully validated; it contains a path without revocation data:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.05.01, End Certificate CP.05.01

**TE:CP.05.02, Level 0**

(No test cases here) This assertion is further tested by the assertions in section 4 of this document. The assertions in section 4 of this document determine the validity of revocation data.

**AS:CP.06**

The application must reject the certificate path if any certificate in the certificate path has been revoked. (This assertion assumes valid revocation data can be used to check for revocation, and therefore depends upon assertion **AS:CP.05**).

**Test 20: TE:CP.06.01, Level 1**

The following path should not be successfully validated; the intermediate certificate has been revoked:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.06.01, Intermediate CRL CP.06.01, End Certificate CP.06.01

**Test 21: TE:CP.06.02, Level 1**

The following path should not be successfully validated; the end certificate has been revoked:

---

[1] Valid Revocation Data is defined as data which meet the requirements found within section 4 of this document.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate CP.06.02, Intermediate CRL CP.06.02, End Certificate CP.06.02

### *3.2 Intermediate Certificate Processing Tests*

The intermediate certificate processing tests, denoted with **IC** in the assertion and test case numbers, deal with the processing of every intermediate certificate within the certificate path.

**AS:IC.01**

The application must ensure that the basic constraints extension is present in every intermediate certificate in the certification path.

[X.509 10.5.1] For an intermediate certificate, if the basic constraints extension field is present in the certificate, check that the **cA** component is present and set to true.

[X.509 8.4.2.1, note 1] If (the basic constraints) extension is not present, or is flagged non-critical and is not recognized by a certificate-using system, then the certificate is to be considered an end-entity certificate and cannot be used to verify certificate signatures.

**Test 22: TE:IC.01.01, Level 1**

The following path should not be successfully validated; the intermediate certificate does not have a basicConstraints extension:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.01.01, Intermediate CRL IC.01.01, End Certificate IC.01.01

**AS:IC.02**

The application must ensure that every intermediate certificate in the certification path must have the basic constraints extension present, and the **cA** component set to true.

**Test 23: TE:IC.02.01, Level 2**

The following path should not be successfully validated; the intermediate certificate has the basicConstraints present and critical, with cA set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.02.01, Intermediate CRL IC.02.01, End Certificate IC.02.01

**Test 24: TE:IC.02.02, Level 3**

The following path should be successfully validated; the intermediate certificate has the basicConstraints present and critical, with cA set to true:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.02.02, Intermediate CRL IC.02.02, End Certificate IC.02.02

**Test 25: TE:IC.02.03, Level 1**

The following path should not be successfully validated; the intermediate certificate has the basicConstraints present and not critical, with cA set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.02.03, Intermediate CRL IC.02.03, End Certificate IC.02.03

**Test 26: TE:IC.02.04, Level 3**

The following path should be successfully validated; the intermediate certificate has the basicConstraints present and not critical, with cA set to true:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.02.04, Intermediate CRL IC.02.04, End Certificate IC.02.04

**AS:IC.03**

The application must reject 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.

[X.509 10.5.1]If the (basic constraints extension field is present in the certificate and the) **pathLenConstraint** component is present, check that the current certification path does not violate that constraint.

**TE:IC.03.01, Level 0**

This assertion is tested in section 3.4 of this document.

**AS:IC.04**

If the application encounters an intermediate certificate in the certificate path that has the key usage extension present with the **keyCertSign** bit set to true and the basic constraints extension present, the application must ensure that the certificate has the **cA** component of the basic constraints extension set to **TRUE**.

[X.509 8.2.2.3] If **KeyUsage** is set to **keyCertSign** and the basic constraints extension is present in the same certificate, the value of the **cA** component of that extension shall be set to **TRUE**.

[X.509 8.2.2.3] If [the **keyUsage**] extension is present, and the certificate-using system recognizes and processes the **keyUsage** extension type, then the certificate-using system shall ensure that the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one.

**Test 27: TE:IC.04.01, Level 1**

The following path should be successfully validated; the intermediate certificate has the **basicConstraints** extension present, with **cA** set to true, and the **keyUsage** extension present, with the **keyCertSign**, and **keyCRLSign** flags set to true:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.04.01, Intermediate CRL IC.04.01, End Certificate IC.04.01

**AS:IC.05**

The application must ensure that every intermediate certificate in the certificate path that has the key usage extension present has the **keyCertSign** bit set to **TRUE**.

Note: The tests for this assertion assume that the application can recognize and process the key usage extension. If the application cannot recognize the key usage extension, all tests containing a critical key usage extension should result in failure, and all tests containing a non-critical key usage extension should result in success.

[X.509 8.2.2.3] Bits in the **KeyUsage** type are as follows:… **keyCertSign**: for verifying a CA's signature on certificates; **cRLSign**: for verifying an authority's signature on CRLs…

[X.509 8.2.2.3] If the extension is flagged critical, then the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one.

[X.509 8.2.2.3] If the extension if flagged non-critical, then it indicates the intended purpose or purposes of the key, and may be used in finding the correct key/certificate of an entity that has multiple keys/certificates. If this extension is present, and the certificate-using system recognizes and processes the **keyUsage** extension type, then the certificate-using system shall ensure that the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one. A bit set to zero indicates that the key is not intended for that purpose. If all bits are zero, it indicates the key is intended for some purpose other than those listed.

**Test 28: TE:IC.05.01, Level 2**

The following path should not be successfully validated; the intermediate certificate with key usage present and marked critical, with keyCertSign set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.05.01, Intermediate CRL IC.05.01, End Certificate IC.05.01

**Test 29: TE:IC.05.02, Level 1**

The following path should not be successfully validated; the intermediate certificate with key usage present and marked not critical, with keyCertSign set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.05.02, Intermediate CRL IC.05.02, End Certificate IC.05.02

**Test 30: TE:IC.05.03, Level 3**

The following path should be successfully validated; the intermediate certificate with key usage present and marked not critical, with keyCertSign set to true:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.05.03, Intermediate CRL IC.05.03, End Certificate IC.05.03

**AS:IC.06**

The application must ensure 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**.

Note: The tests for this assertion assume that the application can recognize and process the key usage extension. If the application cannot recognize the key usage extension, all tests containing a critical key usage extension should result in failure, and all tests containing a non-critical key usage extension should result in success.

Note: This version of the document assumes all intermediate certificates will be issuers of complete, directly issued CRLs. Therefore, all intermediate certificates must be checked.

**Test 31: TE:IC.06.01, Level 2**

The following path should not be successfully validated; the intermediate certificate (that is a CRL issuer) with key usage present and marked critical, with **cRLSign** set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.06.01, Intermediate CRL IC.06.01, End Certificate IC.06.01

**Test 32: TE:IC.06.02, Level 1**

The following path should not be successfully validated; the intermediate certificate (that is a CRL issuer) with key usage present and marked not critical, with **cRLSign** set to false:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.06.02, Intermediate CRL IC.06.02, End Certificate IC.06.02

**Test 33: TE:IC.06.03, Level 3**

The following path should be successfully validated; the intermediate certificate (that is a CRL issuer) with key usage present and marked not critical, with **cRLSign** set to true:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate IC.06.03, Intermediate CRL IC.06.03, End Certificate IC.06.03

### *3.3 Policy Processing Tests*

The policy processing tests, denoted with **PP** in the assertion and test case numbers, deal with the processing of certificate policies throughout the certificate path. Many of these tests may be difficult to fully test for the following reasons:

- Applications may not be required to allow the user/tester flexibility in the configuration of the initial variables that are used as inputs to the path validation process. These applications may have coded certain acceptable values within them, and the tester may not be able to modify those values to exercise certain test cases.
- Applications may not output the results of the path validation process to the user, other than a simple accept/fail indicator. These applications will allow the tester to ensure that certificate paths which should not validate are not accepted, but will not allow the tester to view the outputs to ensure that they are being computed correctly by the application.
- Applications may not display policy qualifiers to the user before, during, or after certificate path validation. These applications will not be able to be tested for assertion **AS:PP.02**.

As is mentioned in the document conventions section, the results for many of these tests are related to the inputs to the path processing software. The test results are then depicted as a matrix, containing the different possible application configurations, and the resultant outputs from the validation process. Three inputs are possible, **ipolset** (*initial-policy-set*), **explicit** (*initial-explicit-policy*), and **inhibit** (*initial-inhibit-policy-mapping*). If an input is not listed in the table, any value of that input will create the same result.

In the test matrices below, paths in which the **user-constrained-policy-set** becomes <empty> and the **explicit policy indicator** is marked true, should be rejected by the application. In cases in which the **authority-constrained-policy-set** is not <empty> the X.509 path validation algorithm has actually succeeded. However, before accepting a path with an <empty> **user-constrained-policy-set** and a non-empty **authority-constrained-policy-set** the application must ensure the user has knowledge that the path is not acceptable for policies in the **user-constrained-policy-set**, and the user

must explicitly choose a policy from the **authority-constrained-policy-set** before accepting the path.

**AS:PP.01**

The software must be able to compute the authority constrained policy set correctly.

**Test 34: TE:PP.01.01, Level 1**

All certificates in the following path have the same policy asserted. Depending on the configuration of the application's inputs to the X.509 path processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = any-policy<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = test-policy-1<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = test-policy-1<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = set not including test-policy-1<br>explicit = true | reject | test-policy-1 | <empty> | true |
| ipolset = set not including test-policy-1<br>explicit = false | accept | test-policy-1 | <empty> | false |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.01.01, Intermediate CRL PP.01.01, End Certificate PP.01.01

**Test 35: TE:PP.01.02, Level 1**

All certificates in the following path have no policy asserted. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.01.02, Intermediate CRL PP.01.02, End Certificate PP.01.02

**Test 36: TE:PP.01.03, Level 2**

All certificates except the first certificate in the following path have the same policy asserted. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.03, Intermediate CRL 1 PP.01.03, Intermediate Certificate 2 PP.01.03, Intermediate CRL 2 PP.01.03, End Certificate PP.01.03

**Test 37: TE:PP.01.04, Level 2**

All certificates except the end certificate in the following path have the same policy asserted. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.04, Intermediate CRL 1 PP.01.04, Intermediate Certificate 2 PP.01.04, Intermediate CRL 2 PP.01.04, End Certificate PP.01.04

**Test 38: TE:PP.01.05, Level 1**

All certificates except the second certificate in the following path have the same policy asserted. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.05, Intermediate CRL 1 PP.01.05, Intermediate Certificate 2 PP.01.05, Intermediate CRL 2 PP.01.05, End Certificate PP.01.05

**Test 39: TE:PP.01.06, Level 1**

The following path is such that the intersection of certificate policies among all the certificates has exactly one policy. The end certificate in this test is a Certificate Authority. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = any-policy<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = set including test-policy-1<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = set including test-policy-1<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = set not including test-policy-1<br>explicit = true | reject | test-policy-1 | <empty> | true |
| ipolset = set not including test-policy-1<br>explicit = false | accept | test-policy-1 | <empty> | false |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.06, Intermediate CRL 1 PP.01.06, Intermediate Certificate 2 PP.01.06, Intermediate CRL 2 PP.01.06, Intermediate Certificate 3 PP.01.06, Intermediate CRL 3 PP.01.06, End Certificate PP.01.06

**Test 40: TE:PP.01.07, Level 2**

The following path is such that the intersection of certificate policies among all the certificates is empty, even though all certificates assert a policy. The end certificate in this test is a Certificate Authority. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.07, Intermediate CRL 1 PP.01.07, Intermediate Certificate 2 PP.01.07, Intermediate Certificate 3 PP.01.07, Intermediate CRL 3 PP.01.07, End Certificate PP.01.07

**Test 41: TE:PP.01.08, Level 1**

The following path is such that the intersection of certificate policies among all the certificates is empty, even though all certificates assert a policy. The end certificate in this test is a Certificate Authority. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.08, Intermediate CRL 1 PP.01.08, Intermediate Certificate 2 PP.01.08, Intermediate CRL 2 PP.01.08, Intermediate Certificate 3 PP.01.08, Intermediate CRL 3 PP.01.08, End Certificate PP.01.08

**Test 42: TE:PP.01.09, Level 2**

The following path is such that the intersection of certificate policies among all the certificates is empty, even though all certificates assert a policy. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.01.09, Intermediate CRL 1 PP.01.09, Intermediate Certificate 2 PP.01.09, Intermediate CRL 2 PP.01.09, Intermediate Certificate 3 PP.01.09, Intermediate CRL 3 PP.01.09, Intermediate Certificate 4 PP.01.09, Intermediate CRL 4 PP.01.09, End Certificate PP.01.09

**AS:PP.02**

The software must associate policy qualifiers with appropriate policies.

Note: This assertion is out of the scope of the current effort, since policy qualifiers are not permitted in DOD Class 3 certificates.

**TE:PP.02.01**

**AS:PP.03**

The software must perform policy mapping correctly when policy mapping is not inhibited.

Note: This assertion is out of the scope of the current effort, since the policy mapping extension is not permitted in DOD Class 3 certificates. The test cases below are low-level ideas at possible tests, to be enhanced into actual tests in the future.

**TE:PP.03.01**

Initial value is not set and none of the certificates have the field – all mappings must be picked up.

**TE:PP.03.02**

Initial value is not set and the first certificate has value 10; certification path length is 5 – all mappings must be picked up

**TE:PP.03.03**

Initial value is not set and the first certificate has value 5; certification path length is 5 – all mappings must be picked up

**TE:PP.03.04**

Initial value is not set and the first certificate has value 4; certification path length is 5 – all mappings must be picked up

**AS:PP.04**

The software must not perform policy mapping when policy mapping is inhibited.

Note: This assertion is out of the scope of the current effort, since the policy mapping extension is not permitted in DOD Class 3 certificates. The test cases below are low-level ideas at possible tests, to be enhanced into actual tests in the future.

**TE:PP.04.01**

Initial value is set and none of the certificates have the field – no mapped policies must be picked up at all.

**TE:PP.04.02**

Initial value is set and the first certificate has value 10; certification path length is 5 – no mapped policies must be picked up at all.

**TE:PP.04.03**

Initial value is set and the first certificate has value 5; certification path length is 5 – no mapped policies must be picked up at all.

**TE:PP.04.04**

Initial value is set and the first certificate has value 4; certification path length is 5 – no mapped policies must be picked up at all.

**TE:PP.04.05**

Initial value is not set and the first certificate has value 4; certification path length is 5 – no mapped policies must be picked up at all.

**TE:PP.04.06**

Initial value is not set and the first certificate has value 0; certification path length is 5 – only the mapping from the first certificate must be picked up.

**TE:PP.04.07**

Initial value is not set and the first certificate has value 7; certification path length is 5; second certificate has value of 1; third certificate has value of 4 – only the mappings from the first, second and third certificates must be picked up.

**TE:PP.04.08**

Initial value is not set and the first certificate has value 7; certification path length is 5; second certificate has value of 0; third certificate has value of 1 – only the mappings from the first and second certificates must be picked up.

**TE:PP.04.09**

Initial value is not set and the first certificate has value 7; certification path length is 5; second certificate has value of 0; third certificate has value of 0 – only the mappings from the first and second certificates must be picked up.

**AS:PP.05**

The software must maintain the inhibit policy mapping state variable appropriately.

Note: This assertion is tested in conjunction with policy mapping assertions above.

Note: This assertion is out of the scope of the current effort, since the policy mapping extension is not permitted in DOD Class 3 certificates. The test cases below are low-level ideas at possible tests, to be enhanced into actual tests in the future.

**AS:PP.06**

The software must process explicit policy indicator state variable appropriately.

Note: Testing this assertion can only be accomplished if the software outputs the final value of the explicit policy indicator state variable to the user. If the application does not output this value, the possible testing is limited.

**Test 43: TE:PP.06.01, Level 3**

The first certificate in the following path (length 5) contains the policy constraints extension, with the **requireExplicitPolicy** present and set to 10.

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.06.01, Intermediate CRL 1 PP.06.01, Intermediate Certificate 2 PP.06.01, Intermediate CRL 2 PP.06.01, Intermediate Certificate 3 PP.06.01, Intermediate CRL 3 PP.06.01, Intermediate Certificate 4 PP.06.01, Intermediate CRL 4 PP.06.01, End Certificate PP.06.01

**Test 44: TE:PP.06.02, Level 1**

The first certificate in the following path (length 5) contains the policy constraints extension, with the **requireExplicitPolicy** present and set to 5.

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.06.02, Intermediate CRL 1 PP.06.02, Intermediate Certificate 2 PP.06.02, Intermediate CRL 2 PP.06.02, Intermediate Certificate 3 PP.06.02, Intermediate CRL 3 PP.06.02, Intermediate Certificate 4 PP.06.02, Intermediate CRL 4 PP.06.02, End Certificate PP.06.02

**Test 45: TE:PP.06.03, Level 1**

The first certificate in the following path (length 5) contains the policy constraints extension, with the **requireExplicitPolicy** present and set to 4.

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | reject | <empty> | <empty> | true |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.06.03, Intermediate CRL 1 PP.06.03, Intermediate Certificate 2 PP.06.03, Intermediate CRL 2 PP.06.03, Intermediate Certificate 3 PP.06.03, Intermediate CRL 3 PP.06.03, Intermediate Certificate 4 PP.06.03, Intermediate CRL 4 PP.06.03, End Certificate PP.06.03

**Test 46: TE:PP.06.04, Level 1**

The first certificate in the following path contains the policy constraints extension, with the **requireExplicitPolicy** present and set to 0. All certificates in the path contain a certificate policy.

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = any-policy<br>explicit = false | accept | test-policy-1 | test-policy-1 | true |
| ipolset = any-policy<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = set including test-policy-1<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = set including test-policy-1<br>explicit = false | accept | test-policy-1 | test-policy-1 | true |
| ipolset = set not including test-policy-1<br>explicit = true | reject | test-policy-1 | <empty> | true |
| ipolset = set not including test-policy-1<br>explicit = false | reject | test-policy-1 | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.06.04, Intermediate CRL 1 PP.06.04, Intermediate Certificate 2 PP.06.04, Intermediate CRL 2 PP.06.04, Intermediate Certificate 3 PP.06.04, Intermediate CRL 3 PP.06.04, Intermediate Certificate 4 PP.06.04, Intermediate CRL 4 PP.06.04, End Certificate PP.06.04

**Test 47: TE:PP.06.05, Level 1**

The first certificate in the following path (length 5) contains the policy constraints extension, with the **requireExplicitPolicy** present and set to 7. The second certificate has **requireExplicitPolicy** present and set to 2. The third certificate has **requireExplicitPolicy** present and set to 4.

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | reject | <empty> | <empty> | true |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PP.06.05, Intermediate CRL 1 PP.06.05, Intermediate Certificate 2 PP.06.05, Intermediate CRL 2 PP.06.05, Intermediate Certificate 3 PP.06.05, Intermediate CRL 3 PP.06.05, Intermediate Certificate 4 PP.06.05, Intermediate CRL 4 PP.06.05, End Certificate PP.06.05

**AS:PP.07**

The software must return the appropriate values of authority constrained policy set.

Note: This assertion is tested by testing other assertions 1 through 5.

**AS:PP.08**

The software must return the appropriate values of the user constrained policy set.

Note: The software may or may not output the values to the user. If the values are not output, this will be difficult to test.

**Test 48: TE:PP.08.01, Level 3**

All certificates in the following path assert the same policy. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = test-policy-1<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = test-policy-1<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-1 | test-policy-1 | false |
| ipolset = any-policy<br>explicit = true | accept | test-policy-1 | test-policy-1 | true |
| ipolset = set not including test-policy-1<br>explicit = false | accept | test-policy-1 | <empty> | false |
| ipolset = set not including test-policy-1<br>explicit = true | reject | test-policy-1 | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.01, Intermediate CRL PP.08.01, End Certificate PP.08.01

**Test 49: TE:PP.08.02, Level 3**

All certificates in the following path assert the same two policies. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = test-policy-1<br>explicit = false | accept | test-policy-1<br>test-policy-2 | test-policy-1 | false |
| ipolset = test-policy-1<br>explicit = true | accept | test-policy-1<br>test-policy-2 | test-policy-1 | true |
| ipolset = set not including test-policy-1 or test-policy-2<br>explicit = false | accept | test-policy-1<br>test-policy-2 | <empty> | false |
| ipolset = set not including test-policy-1 or test-policy-2<br>explicit = true | reject | test-policy-1<br>test-policy-2 | <empty> | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-1<br>test-policy-2 | test-policy-1<br>test-policy-2 | false |
| ipolset = any-policy<br>explicit = true | accept | test-policy-1<br>test-policy-2 | test-policy-1<br>test-policy-2 | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.02, Intermediate CRL PP.08.02, End Certificate PP.08.02

**Test 50: TE:PP.08.03, Level 3**

All certificates in the following path assert the special value any-policy. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = test-policy-1<br>explicit = false | accept | any-policy | test-policy-1 | false |
| ipolset = test-policy-1<br>explicit = true | accept | any-policy | test-policy-1 | true |
| ipolset = test-policy-1 and test-policy-2<br>explicit = false | accept | any-policy | test-policy-1<br>test-policy-2 | false |
| ipolset = test-policy-1 and test-policy-2<br>explicit = true | accept | any-policy | test-policy-1<br>test-policy-2 | true |
| ipolset = any-policy<br>explicit = false | accept | any-policy | any-policy | false |
| ipolset = any-policy<br>explicit = true | accept | any-policy | any-policy | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.03, Intermediate CRL PP.08.03, End Certificate PP.08.03

**Test 51: TE:PP.08.04, Level 3**

The certificates in the following path do not assert a contiguous set of policies. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| explicit = false | accept | <empty> | <empty> | false |
| explicit = true | reject | <empty> | <empty> | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.04, Intermediate CRL PP.08.04, End Certificate PP.08.04

**Test 52: TE:PP.08.05, Level 3**

The certificates in the following path assert the same policy, but the user-constrained set does not contain that policy. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = test-policy-1<br>explicit = false | accept | test-policy-3 | <empty> | false |
| ipolset = test-policy-1<br>explicit = true | reject | test-policy-3 | <empty> | true |
| ipolset = test-policy-1 and test-policy-2<br>explicit = false | accept | test-policy-3 | <empty> | false |
| ipolset = test-policy-1 and test-policy-2<br>explicit = true | reject | test-policy-3 | <empty> | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-3 | test-policy-3 | false |
| ipolset = any-policy<br>explicit = true | accept | test-policy-3 | test-policy-3 | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.05, Intermediate CRL PP.08.05, End Certificate PP.08.05

**Test 53: TE:PP.08.06, Level 3**

The certificates in the following path assert three policies. Depending on the configuration of the application's inputs to the X.509 path-processing machine, the results of this test will be as follows:

| Application Configuration | Accept/Reject | Authority-constrained policy set | User-constrained policy set | Explicit Policy Indicator |
|---|---|---|---|---|
| ipolset = test-policy-1<br>explicit = false | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1 | false |
| ipolset = test-policy-1<br>explicit = true | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1 | true |
| ipolset = test-policy-1 and test-policy-2<br>explicit = false | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1<br>test-policy-2 | false |
| ipolset = test-policy-1 and test-policy-2<br>explicit = true | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1<br>test-policy-2 | true |
| ipolset = set not including test-policy-1, test-policy-2, or test-policy-3<br>explicit = false | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | <empty> | false |
| ipolset = set not including test-policy-1, test-policy-2, or test-policy-3<br>explicit = true | reject | test-policy-1<br>test-policy-2<br>test-policy-3 | <empty> | true |
| ipolset = any-policy<br>explicit = false | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1<br>test-policy-2<br>test-policy-3 | false |
| ipolset = any-policy<br>explicit = true | accept | test-policy-1<br>test-policy-2<br>test-policy-3 | test-policy-1<br>test-policy-2<br>test-policy-3 | true |

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PP.08.06, Intermediate CRL PP.08.06, End Certificate PP.08.06

**AS:PP.09**

The software must return the appropriate value of explicit policy indicator.

Note: this assertion is tested by testing **AS:PP.06**

**AS:PP.10**

After validating a path, the software must return success or failure appropriately.

Note: this assertion is tested by testing other policy assertions.

### *3.4 Path Length Related Tests*

The path length related tests, denoted with **PL** in the assertion and test case numbers, deal with the processing of certificate path length.

**AS:PL.01**

The software must calculate the permitted path length correctly.

**Test 54: TE:PL.01.01, Level 1**

The following path must be rejected. The first certificate in the path has a path length constraint of 0 (allowing 0 additional intermediate certificates in the path). There is one additional intermediate certificate. The end certificate is not a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.01, Intermediate CRL 1 PL.01.01, Intermediate Certificate 2 PL.01.01, Intermediate CRL 2 PL.01.01, End Certificate PL.01.01

**Test 55: TE:PL.01.02, Level 2**

The following path must be rejected. The first certificate in the path has a path length constraint of 0 (allowing 0 additional intermediate certificates in the path). There is one additional intermediate certificate. The end certificate is a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.02, Intermediate CRL 1 PL.01.02, Intermediate Certificate 2 PL.01.02, Intermediate CRL 2 PL.01.02, End Certificate PL.01.02

**Test 56: TE:PL.01.03, Level 2**

The following path must be accepted. The first certificate in the path has a path length constraint of 0 (allowing 0 additional intermediate certificates in the path). There are no additional intermediate certificates. The end certificate is not a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PL.01.03, Intermediate CRL PL.01.03, End Certificate PL.01.03

**Test 57: TE:PL.01.04, Level 1**

The following path must be accepted. The first certificate in the path has a path length constraint of 0 (allowing 0 additional intermediate certificates in the path). There are no additional intermediate certificates. The end certificate is a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate PL.01.04, Intermediate CRL PL.01.04, End Certificate PL.01.04

**Test 58: TE:PL.01.05, Level 2**

The following path must be rejected. The path length is 4. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 0. The third certificate has a path length constraint of 0. The end certificate is not a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.05, Intermediate CRL 1 PL.01.05, Intermediate Certificate 2 PL.01.05, Intermediate CRL 2 PL.01.05, Intermediate Certificate 3 PL.01.05, Intermediate CRL 3 PL.01.05, End Certificate PL.01.05

**Test 59: TE:PL.01.06, Level 2**

The following path must be rejected. The path length is 4. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 0. The third certificate has a path length constraint of 0. The end certificate is a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.06, Intermediate CRL 1 PL.01.06, Intermediate Certificate 2 PL.01.06, Intermediate CRL 2 PL.01.06, Intermediate Certificate 3 PL.01.06, Intermediate CRL 3 PL.01.06, End Certificate PL.01.06

**Test 60: TE:PL.01.07, Level 1**

The following path must be rejected. The path length is 5. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 1. The third certificate has a path length constraint of 1. The end certificate is not a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.07, Intermediate CRL 1 PL.01.07, Intermediate Certificate 2 PL.01.07, Intermediate CRL 2 PL.01.07, Intermediate Certificate 3 PL.01.07, Intermediate CRL 3 PL.01.07, Intermediate Certificate 4 PL.01.07, Intermediate CRL 4 PL.01.07, End Certificate PL.01.07

**Test 61: TE:PL.01.08, Level 2**

The following path must be rejected. The path length is 5. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 1. The third certificate has a path length constraint of 1. The end certificate is a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.08, Intermediate CRL 1 PL.01.08, Intermediate Certificate 2 PL.01.08, Intermediate CRL 2 PL.01.08, Intermediate Certificate 3 PL.01.08, Intermediate CRL 3 PL.01.08, Intermediate Certificate 4 PL.01.08, Intermediate CRL 4 PL.01.08, End Certificate PL.01.08

**Test 62: TE:PL.01.09, Level 2**

The following path must be accepted. The path length is 5. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 4. The third certificate has a path length constraint of 1. The end certificate is not a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.09, Intermediate CRL 1 PL.01.09, Intermediate Certificate 2 PL.01.09, Intermediate CRL 2 PL.01.09, Intermediate Certificate 3 PL.01.09, Intermediate CRL 3 PL.01.09, Intermediate Certificate 4 PL.01.09, Intermediate CRL 4 PL.01.09, End Certificate PL.01.09

**Test 63: TE:PL.01.10, Level 2**

The following path must be accepted. The path length is 5. The first certificate in the path has a path length constraint of 6 (allowing 6 additional intermediate certificates in the path). The second certificate has a path length constraint of 4. The third certificate has a path length constraint of 1. The end certificate is a CA.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 PL.01.10, Intermediate CRL 1 PL.01.10, Intermediate Certificate 2 PL.01.10, Intermediate CRL 2 PL.01.10, Intermediate Certificate 3 PL.01.10, Intermediate CRL 3 PL.01.10, Intermediate Certificate 4 PL.01.10, Intermediate CRL 4 PL.01.10, End Certificate PL.01.10

# 4 REVOCATION STATUS RELATED TESTS

There are different methods of providing revocation status data within an X.509 compliant certificate issuing system. Currently, only complete CRLs issued directly by the certificate-issuing authority are being tested. Future versions of this document may include other revocation status methods.

## *4.1 Directly Issued Full CRL Related Tests*

The certificate revocation list (CRL) related tests, denoted with **RL** in the assertion and test case numbers, deal with the processing of CRLs during certificate path validation.

**AS:RL.01**

Certificate Revocation Lists (CRLs) may be used as the revocation status mechanism

[X.509 7.3] (The X.509 specification) defines a Certificate Revocation List (CRL) mechanism but does not preclude the use of alternative mechanisms

**TE:RL.01.01, Level 0**

No testing for this. If the application uses CRLs this assertion is satisfied.

**AS:RL.02**

The application must verify the signature on each certificate revocation list in the certification path using the same public key used to sign certificates.

[X.509 7.3] The certificates may be revoked by the same certificate-issuing authority directly

**Test 64: TE:RL.02.01, Level 1**

The following path should not be successfully validated; the path has a CRL containing an invalid signature:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.02.01, Intermediate CRL RL.02.01, End Certificate RL.02.01

**AS:RL.03**

When checking to see if a certificate is present on a certificate revocation list, the application must verify that the issuer name in the certificate matches the issuer name in the certificate revocation list.

**Test 65: TE:RL.03.01, Level 1**

The following path should not be successfully validated; the path contains a certificate revocation list from the wrong issuer, and the CRL signer's certificate:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 RL.03.01, Intermediate Certificate 2 RL.03.01, Intermediate CRL RL.03.01, End Certificate RL.03.01

**Test 66: TE:RL.03.02, Level 2**

The following path should not be successfully validated; the path contains a certificate revocation list with the wrong issuer name, and that list has the end certificate's serial

number on it. If specified, the application should state the path failed because of a lack of revocation information, not because the end certificate was revoked.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.03.02, Intermediate CRL RL.03.02, End Certificate RL.03.02

**Test 67: TE:RL.03.03, Level 2**

The following path should be successfully validated; the path contains two certificate revocation lists, one with the wrong issuer name and one with the correct issuer name.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.03.03, Intermediate CRL 1 RL.03.03, Intermediate CRL 2 RL.03.03, End Certificate RL.03.03

**AS:RL.04**

The application should reject the path if any certificate in the certificate path has been revoked. A certificate is revoked if its serial number appears in the **revokedCertificates** component of the CRL associated with the certificate signer.

[X.509 7.3] **revokedCertificates** identifies certificates that have been revoked. The revoked certificates are identified by their serial numbers.

**TE:RL.04.01, Level 0**

This assertion is tested by the tests TE:CP.06.01 and TE:CP.06.02

**AS:RL.05**

The application should reject the path if any certificate in the certificate path has been revoked regardless of whether there are unrecognized critical **crlEntryExtensions** present in the CRL.

[X.509 7.3] When an implementation processing a certificate revocation list does not recognize a critical extension in the **crlEntryExtensions** field, it shall assume that, at a minimum, the identified certificate has been revoked and is no longer valid and perform additional actions concerning that revoked certificate as dictated by local policy.

**Test 68: TE:RL.05.01, Level 1**

The following path should not be successfully validated; the path contains an intermediate certificate that has been revoked, along with a made up critical **crlEntryExtension**:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 RL.05.01, Intermediate CRL 1 RL.05.01, Intermediate Certificate 2 RL.05.01, Intermediate CRL 2 RL.05.01, End Certificate RL.05.01

ASN for private extension:

**id-test-extension OBJECT IDENTIFIER ::= { 2 16 840 1 101 2 1 12 2 }**

```
privateExtension EXTENSION ::= {
        SYNTAX          privateNumber
        IDENTIFIED BY   id-test-extension }
```

**privateNumber ::= INTEGER**

**Test 69: TE:RL.05.02, Level 2**

The following path should not be successfully validated; the path contains an end certificate that has been revoked, along with a made up critical **crlEntryExtension**:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.05.02, Intermediate CRL RL.05.02, End Certificate RL.05.02

**AS:RL.06**

The application should reject the path if any certificate in the certification path has been revoked regardless of whether there are unrecognized critical **crlExtensions** present in the CRL.

[X.509 7.3] When an implementation does not recognize a critical extension in the **crlExtensions** field, it shall assume that identified certificates have been revoked and are no longer valid

**Test 70: TE:RL.06.01, Level 1**

The following path should not be successfully validated; the path contains an intermediate certificate that has been revoked, along with a made up critical **crlExtension**:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate 1 RL.06.01, Intermediate CRL 1 RL.06.01, Intermediate Certificate 2 RL.06.01, Intermediate CRL 2 RL.06.01, End Certificate RL.06.01

**Test 71: TE:RL.06.02, Level 2**

The following path should not be successfully validated; the path contains an end certificate that has been revoked, along with a made up critical **crlExtension**:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.06.02, Intermediate CRL RL.06.02, End Certificate RL.06.02

**AS:RL.07**

The application should consider a certificate revocation list invalid if the **nextUpdate** time in the certificate is earlier than the current time.

Note: local policy may permit a CRL be used even if the current time is later than the **nextUpdate** time in the CRL. These tests contain CRLs that are very old, and most policies should restrict their use.

[X.509 7.3] **nextUpdate**, if present, indicates the date/time by which the next revocation list in this series will be issued. The next revocation list could be issued before the indicated date, but it will not be issued any later than the indicated time.

**Test 72: TE:RL.07.01, Level 1**

The following path should not be successfully validated; the path contains a CRL with **nextUpdate** earlier than the current date:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.07.01, Intermediate CRL RL.07.01, End Certificate RL.07.01

**Test 73: TE:RL.07.02, Level 2**

The following path should not be successfully validated; the path contains a CRL with **nextUpdate** in UTC time with 50 as the year value (should treat as 1950):

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.07.02, Intermediate CRL RL.07.02, End Certificate RL.07.02

**Test 74: TE:RL.07.03, Level 2**

The following path should be successfully validated; the path contains a CRL with **nextUpdate** as a Generalized time of 2050.

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.07.03, Intermediate CRL RL.07.03, End Certificate RL.07.03

**AS:RL.08**

The application should ensure that the certificate revocation list does not contain the **deltaCRLIndicator** extension.

[X.509 8.6.2.4] The delta CRL indicator field identifies a CRL as being a delta CRL (dCRL) that provides updates to a referenced base CRL. The referenced base CRL is a CRL that was explicitly issued as a CRL that is complete for a given scope. The CRL containing the delta CRL indicator extension contains updates to the certificate revocation status for that same scope. This scope does not necessarily include all revocation reasons or all certificates issued by a CA, especially in the case where the CRL is a CRL distribution point.

**Test 75: TE:RL.08.01, Level 1**

The following path should not be successfully validated; the path contains a CRL containing **deltaCRLIndicator** marked critical, with no Base CRL to serve as a reference:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.08.01, Intermediate CRL RL.08.01, End Certificate RL.08.01

**AS:RL.09**

The application should ensure that the certificate revocation list does not contain the **issuingDistributionPoint** extension.

[X.509 8.6.2.2] This CRL extension field identifies the CRL distribution point for this particular CRL, and indicates if the CRL is limited to revocations for end-entity certificates only, for authority certificates only, or for a limited set of reasons only.

**Test 76: TE:RL.09.01, Level 1**

The following path should not be successfully validated; the path contains a CRL for end-entity certificates containing IDP marked critical, stating that only CA certificates are contained:

Trust Anchor CP.01.01, Trust Anchor CRL CP.01.01, Intermediate Certificate RL.09.01, Intermediate CRL RL.09.01, End Certificate RL.09.01

# 5 TEST DATA DESCRIPTIONS

## *5.1 Data Description Format*

Each test requirement will be tested by the use of a series of certificates, CRLs, and associated private keys as necessary, hereafter referred to as “data objects”. This section of the document describes the construction of each data object required for testing.

The data description format for each data object starts with a base data object and describes the differences between the base object and the target object.

Example:

**End Certificate CP.99.99**

include Base End Certificate
issuer name: cn=CA1-CP.99.99 (other RDNs preserved)
subject name: cn=User1-CP.99.99 (other RDNs preserved)
validity notBefore: 440101120000Z (01/01/2044, 12:00:00 GMT)
signed by Intermediate Certificate CP.99.99

The table format used to describe the base data objects was developed by Robert Moskowitz of ICSA.net, and modified by Booz-Allen and Hamilton. It has been further refined for this effort. If a field or extension is not listed in the table, it is not used in any certificate.

## *5.2 Base Data Objects*

Where possible, the actual value that should be used in encoding has been inserted into the tables below. Binary fields, such as keys, hashes, and signatures have been omitted. Please refer to the comments field to determine how to construct any values that are not within the table.

Additionally, some rows have been added to the table but do not exist in the base data object. These rows are typically marked “absent” in the comments field. The rows have been inserted as placeholders, because there are certificates within the test data that use those fields or extensions.

### 5.2.1 Base Trust Anchor

The base trust anchor information is as follows:

**Distinguished Name**: cn=Trust Anchor, ou=Testing, ou=DoD, o=U.S. Government, c=US

**Public Key**: Any acceptable RSA public key, to be chosen by the developers of the test data.

### 5.2.2 Base End Certificate

| 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=Trust Anchor, 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 | Jan. 1, 1998, 12:01:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |
| notAfter | | | |
| Time | | | |
| utcTime | | | |
| UTCTime | | 480101120100Z | Jan. 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 |
| **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 |

### 5.2.3 Base Intermediate Certificate

| 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=Trust Anchor, 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 | Jan. 1, 1998, 12:01:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |

| | | | |
|---|---|---|---|
| notAfter | | | |
| Time | | | |
| utcTime | | | |
| UTCTime | | 480101120100Z | Jan. 1, 2048, 12:01:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |
| **subject** | | | |
| Name | | cn=CA1-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 |
| **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 | | |
| cA | | TRUE | |
| pathLenConstraint | | INTEGER | not present unless otherwise specified |
| **keyUsage** | TRUE | | |
| digitalSignature | | 0 | |
| nonRepudiation | | 0 | |
| keyEncipherment | | 0 | |
| dataEncipherment | | 0 | |
| keyAgreement | | 0 | |
| keyCertSign | | 1 | |
| cRLSign | | 1 | |
| 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 |

### 5.2.4 Base CRL

| Field | Critical Flag | Value | Comments |
|---|---|---|---|
| CertificateList | | | |
| tbsCertList | | | Fields to be signed. |
| **version** | | 1 | Integer Value of "2" for Version 3 certificate. |
| **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=CA1-CP.01.01, 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 | |
| **thisUpdate** | | | |
| Time | | | |
| utcTime | | | |
| UTCTime | | 990101120100Z | Jan. 1, 1999, 12:01:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |
| **nextUpdate** | | | |
| Time | | | |
| utcTime | | | |
| UTCTime | | 480101120100Z | Jan. 1, 2048, 12:01:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |
| **revokedCertificates** | | | absent unless otherwise specified |
| userCertificate | | | |
| CertificateSerialNumber | | | |
| revocationDate | | | |
| Time | | | |
| utcTime | | | |
| UTCTime | | 990101120000Z | Jan. 1, 1999, 12:00:00 GMT |
| generalTime | | | |
| GeneralizedTime | | | Use for dates after 2049 |
| crlEntryExtensions | | | |
| Extensions | | | |
| **reasonCode** | FALSE | | |
| CRLReason | | keyCompromise | |
| **crlExtensions** | | | |
| **authorityKeyIdentifier** | FALSE | | |
| keyIdentifier | | OCTET STRING | Derived using the SHA-1 hash of the issuer public key. |
| **cRLNumber** | FALSE | 1 | |
| algorithmIdentifier | | | |
| AlgorithmIdentifier | | | |
| algorithm | | 1.2.840.113549.1.1.5 | SHA-1WithRSAEncryption |
| parameters | | | |
| encrypted | | | signature calculated |

### *5.3 Test Object Identifiers*

The following is a list of test object identifiers that are used by the test data. These OIDs have all been registered by NIST for testing use only.

| Name | Object Identifier (OID) |
|---|---|
| test-policy-1 | 2.16.840.1.101.3.1.48.1 |
| test-policy-2 | 2.16.840.1.101.3.1.48.2 |
| test-policy-3 | 2.16.840.1.101.3.1.48.3 |
| test-policy-4 | 2.16.840.1.101.3.1.48.4 |
| test-policy-5 | 2.16.840.1.101.3.1.48.5 |

### *5.4 Data Descriptions*

5.4.1 Certificate Processing Test Data

**Trust Anchor CP.01.01**

include Base Trust Anchor

**Trust Anchor CRL CP.01.01**

include Base CRL
issuer name: DN of Trust Anchor CP.01.01
revokedCertificate: present
CertificateSerialNumber: 39
signed by Trust Anchor CP.01.01

**End Certificate CP.01.01**

include Base End Certificate
serial number: 1
signed by Trust Anchor CP.01.01

**Intermediate Certificate CP.01.02**

include Base Intermediate Certificate
serial number: 2
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.01.02 (other RDNs preserved)
signed by Trust Anchor CP.01.01; one or more bits in the signature is modified

**Intermediate CRL CP.01.02**

include Base CRL
issuer name: DN of Intermediate Certificate CP.01.02
signed by Intermediate Certificate CP.01.02

**End Certificate CP.01.02**

include Base End Certificate

issuer name: DN of Intermediate Certificate CP.01.02
subject name: cn=User1-CP.01.02 (other RDNs preserved)
serial number: 3
signed by Intermediate Certificate CP.01.02

**Intermediate Certificate CP.01.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.01.03 (other RDNs preserved)
serial number: 4
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.01.03**

include Base CRL
issuer name: DN of Intermediate Certificate CP.01.03
signed by Intermediate Certificate CP.01.03

**End Certificate CP.01.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.01.03
subject name: cn=User1-CP.01.03 (other RDNs preserved)
serial number: 5
signed by Intermediate Certificate CP.01.03; one or more bits in the signature is modified

**Intermediate Certificate 1 CP.02.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.02.01 (other RDNs preserved)
serial number: 6
notBefore: UTC:990101120100Z (January 1,1999, 12:01:00; earlier than current time)
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 CP.02.01**

include Base CRL
issuer name: DN of Intermediate Certificate 1 CP.02.01
signed by Intermediate Certificate 1 CP.02.01

**Intermediate Certificate 2 CP.02.01**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 CP.02.01
subject name: cn=CA2-CP.02.01 (other RDNs preserved)
serial number: 7
notBefore: UTC:990101120100Z (January 1,1999, 12:01:00; earlier than current time)
signed by Intermediate Certificate 1 CP.02.01

**Intermediate CRL 2 CP.02.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 CP.02.01
signed by Intermediate Certificate 2 CP.02.01

**End Certificate CP.02.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 CP.02.01
subject name: cn=User1-CP.02.01 (other RDNs preserved)
serial number: 8
notBefore: UTC:990101120100Z (January 1,1999, 12:01:00; earlier than current time)
signed by Intermediate Certificate 2 CP.02.01

**Intermediate Certificate CP.02.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.02.02 (other RDNs preserved)
serial number: 9
notBefore: UTC:470101120100Z (January 1,2047, 12:01:00; later than current time)
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.02.02**

include Base CRL
issuer name: DN of Intermediate Certificate CP.02.02
signed by Intermediate Certificate CP.02.02

**End Certificate CP.02.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.02.02
subject name: cn=User1-CP.02.02 (other RDNs preserved)
serial number: 10
signed by Intermediate Certificate CP.02.02

**Intermediate Certificate CP.02.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.02.03 (other RDNs preserved)
serial number: 11
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.02.03**

include Base CRL
issuer name: DN of Intermediate Certificate CP.02.03

signed by Intermediate Certificate CP.02.03

**End Certificate CP.02.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.02.03
subject name: cn=User1-CP.02.03 (other RDNs preserved)
serial number: 12
notBefore: UTC:470101120100Z (January 1,2047, 12:01:00; later than current time)
signed by Intermediate Certificate CP.02.03

**Intermediate Certificate CP.02.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.02.04 (other RDNs preserved)
serial number: 13
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.02.04**

include Base CRL
issuer name: DN of Intermediate Certificate CP.02.04
signed by Intermediate Certificate CP.02.04

**End Certificate CP.02.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.02.04
subject name: cn=User1-CP.02.04 (other RDNs preserved)
serial number: 14
notBefore: UTC:500101120100Z (January 1,1950, 12:01:00; should treat it as 1950; earlier than current time)
signed by Intermediate Certificate CP.02.04

**Intermediate Certificate CP.02.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.02.05 (other RDNs preserved)
serial number: 15
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.02.05**

include Base CRL
issuer name: DN of Intermediate Certificate CP.02.05
signed by Intermediate Certificate CP.02.05

**End Certificate CP.02.05**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.02.05
subject name: cn=User1-CP.02.05 (other RDNs preserved)

serial number: 16
notBefore: GT:20500101120100Z (January 1,2050, 12:01:00; later than current time)
signed by Intermediate Certificate CP.02.05

**Intermediate Certificate CP.03.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.03.01 (other RDNs preserved)
serial number: 17
notAfter: UTC:000101120100Z (January 1,2000, 12:01:00; earlier than current time)
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.03.01**

include Base CRL
issuer name: DN of Intermediate Certificate CP.03.01
signed by Intermediate Certificate CP.03.01

**End Certificate CP.03.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.03.01
subject name: cn=User1-CP.03.01 (other RDNs preserved)
serial number: 18
signed by Intermediate Certificate CP.03.01

**Intermediate Certificate CP.03.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.03.02 (other RDNs preserved)
serial number: 19
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.03.02**

include Base CRL
issuer name: DN of Intermediate Certificate CP.03.02
signed by Intermediate Certificate CP.03.02

**End Certificate CP.03.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.03.02
subject name: cn=User1-CP.03.02 (other RDNs preserved)
serial number: 20
notAfter: UTC:000101120100Z (January 1,2000, 12:01:00; earlier than current time)
signed by Intermediate Certificate CP.03.02

**Intermediate Certificate CP.03.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.03.03 (other RDNs preserved)
serial number: 21
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.03.03**

include Base CRL
issuer name: DN of Intermediate Certificate CP.03.03
signed by Intermediate Certificate CP.03.03

**End Certificate CP.03.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.03.03
subject name: cn=User1-CP.03.03 (other RDNs preserved)
serial number: 22
notAfter: UTC:500701120100Z (July 1,1950, 12:01:00; should be treated as 1950; earlier than current time)
signed by Intermediate Certificate CP.03.03

**Intermediate Certificate CP.03.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.03.04 (other RDNs preserved)
serial number: 23
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.03.04**

include Base CRL
issuer name: DN of Intermediate Certificate CP.03.04
signed by Intermediate Certificate CP.03.04

**End Certificate CP.03.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.03.04
subject name: cn=User1-CP.03.04 (other RDNs preserved)
serial number: 24
notAfter: GT:20500101120100Z (January 1,2050, 12:01:00; should be treated as 2050;  later than current time)
signed by Intermediate Certificate CP.03.04

**Intermediate Certificate CP.04.01**

include Base Intermediate Certificate

issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.04.01 (other RDNs preserved)
serial number: 25
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.01**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.01
signed by Intermediate Certificate CP.04.01

**End Certificate CP.04.01**

include Base End Certificate
issuer name: cn=CA1-CP.99.99 (other RDNs preserved; issuer does not equal Intermediate Cert subject name)
subject name: cn=User1-CP.04.01 (other RDNs preserved)
serial number: 26
signed by Intermediate Certificate CP.04.01

**Intermediate Certificate CP.04.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.04.02, ou=Testing, ou=DoD, o=U.S. Government, c=US
serial number: 27
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.02**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.02
signed by Intermediate Certificate CP.04.02

**End Certificate CP.04.02**

include Base End Certificate
issuer name: cn=CA1-CP.04.02, ou=DoD, ou=Testing, o=U.S. Government, c=US (name order is different)
subject name: cn=User1-CP.04.02 (other RDNs preserved)
serial number: 28
signed by Intermediate Certificate CP.04.02

**Intermediate Certificate CP.04.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name (quotes for clarity): cn=”  CA1 -   CP.04.03” (other RDNs preserved)
serial number: 29
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.03**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.03
signed by Intermediate Certificate CP.04.03

**End Certificate CP.04.03**

include Base End Certificate
issuer name (quotes for clarity): cn="ca1 - CP.04.03 " (other RDNs preserved)
subject name: cn=User1-CP.04.03 (other RDNs preserved)
serial number: 30
signed by Intermediate Certificate CP.04.03

**Intermediate Certificate CP.04.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1 - CP.04.04 (other RDNs preserved)
serial number: 31
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.04**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.04
signed by Intermediate Certificate CP.04.04

**End Certificate CP.04.04**

include Base End Certificate
issuer name: cn=CA1 - CP.04.04, ou=Testing, ou=DoD, o=U.S. Government, c=US (whitespace is different)
subject name: cn=User1-CP.04.04 (other RDNs preserved)
serial number: 32
signed by Intermediate Certificate CP.04.04

**Intermediate Certificate CP.04.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name (quotes for clarity): cn=" CA1-CP.04.05" (other RDNs preserved)
serial number: 33
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.05**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.05
signed by Intermediate Certificate CP.04.05

**End Certificate CP.04.05**

include Base End Certificate
issuer name (quotes for clarity): cn="CA1-CP.04.05 " (other RDNs preserved)
subject name: cn=User1-CP.04.05 (other RDNs preserved)

serial number: 34
signed by Intermediate Certificate CP.04.05

**Intermediate Certificate CP.04.06**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.04.06 (other RDNs preserved)
serial number: 35
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.04.06**

include Base CRL
issuer name: DN of Intermediate Certificate CP.04.06
signed by Intermediate Certificate CP.04.06

**End Certificate CP.04.06**

include Base End Certificate
issuer name: cn=ca1-CP.04.06, OU=TESTING, OU=DoD, O=u.s. GOVERNMENT, c=US (capitalization is different)
subject name: cn=User1-CP.04.06 (other RDNs preserved)
serial number: 36
signed by Intermediate Certificate CP.04.06

**Intermediate Certificate CP.05.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.05.01 (other RDNs preserved)
serial number: 37
signed by Trust Anchor CP.01.01

**End Certificate CP.05.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.05.01
subject name: cn=User1-CP.05.01 (other RDNs preserved)
serial number: 38
signed by Intermediate Certificate CP.05.01

**Intermediate Certificate CP.06.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.06.01 (other RDNs preserved)
serial number: 39
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate CP.06.01
signed by Intermediate Certificate CP.06.01

**End Certificate CP.06.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.06.01
subject name: cn=User1-CP.06.01 (other RDNs preserved)
serial number: 40
signed by Intermediate Certificate CP.06.01

**Intermediate Certificate CP.06.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-CP.06.02 (other RDNs preserved)
serial number: 41
signed by Trust Anchor CP.01.01

**Intermediate CRL CP.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate CP.06.02
revokedCertificate: present
  CertificateSerialNumber: 42 (the serial # of the end certificate)
signed by Intermediate Certificate CP.06.02

**End Certificate CP.06.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate CP.06.02
subject name: cn=User1-CP.06.02 (other RDNs preserved)
serial number: 42
signed by Intermediate Certificate CP.06.02

5.4.2 Intermediate Certificate Processing Test Data

**Intermediate Certificate IC.01.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.01.01 (other RDNs preserved)
serial number: 43
basicConstraints: absent
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.01.01**

include Base CRL
issuer name: DN of Intermediate Certificate IC.01.01
signed by Intermediate Certificate IC.01.01

**End Certificate IC.01.01**

include Base End Certificate

issuer name: DN of Intermediate Certificate IC.01.01
subject name: cn=User1-IC.01.01 (other RDNs preserved)
serial number: 44
signed by Intermediate Certificate IC.01.01

**Intermediate Certificate IC.02.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.02.01 (other RDNs preserved)
serial number: 45
basicConstraints: present and critical
  cA: FALSE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.02.01**

include Base CRL
issuer name: DN of Intermediate Certificate IC.02.01
signed by Intermediate Certificate IC.02.01

**End Certificate IC.02.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.02.01
subject name: cn=User1-IC.02.01 (other RDNs preserved)
serial number: 46
signed by Intermediate Certificate IC.02.01

**Intermediate Certificate IC.02.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.02.02 (other RDNs preserved)
serial number: 47
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.02.02**

include Base CRL
issuer name: DN of Intermediate Certificate IC.02.02
signed by Intermediate Certificate IC.02.02

**End Certificate IC.02.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.02.02
subject name: cn=User1-IC.02.02 (other RDNs preserved)
serial number: 48
signed by Intermediate Certificate IC.02.02

**Intermediate Certificate IC.02.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.02.03 (other RDNs preserved)

serial number: 49
basicConstraints: present and not critical
cA: FALSE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.02.03**

include Base CRL
issuer name: DN of Intermediate Certificate IC.02.03
signed by Intermediate Certificate IC.02.03

**End Certificate IC.02.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.02.03
subject name: cn=User1-IC.02.03 (other RDNs preserved)
serial number: 50
signed by Intermediate Certificate IC.02.03

**Intermediate Certificate IC.02.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.02.04 (other RDNs preserved)
serial number: 51
basicConstraints: present and not critical
cA: TRUE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.02.04**

include Base CRL
issuer name: DN of Intermediate Certificate IC.02.04
signed by Intermediate Certificate IC.02.04

**End Certificate IC.02.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.02.04
subject name: cn=User1-IC.02.04 (other RDNs preserved)
serial number: 52
signed by Intermediate Certificate IC.02.04

**Intermediate Certificate IC.04.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.04.01 (other RDNs preserved)
serial number: 53
basicConstraints: present and not critical
cA: TRUE
keyUsage: present and not critical
keyCertSign: TRUE
cRLSign: TRUE

signed by Trust Anchor CP.01.01

**Intermediate CRL IC.04.01**

include Base CRL
issuer name: DN of Intermediate Certificate IC.04.01
signed by Intermediate Certificate IC.04.01

**End Certificate IC.04.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.04.01
subject name: cn=User1-IC.04.01 (other RDNs preserved)
serial number: 54
signed by Intermediate Certificate IC.04.01

**Intermediate Certificate IC.05.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.05.01 (other RDNs preserved)
serial number: 55
keyUsage: present and critical
  keyCertSign: FALSE
  cRLSign: TRUE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.05.01**

include Base CRL
issuer name: DN of Intermediate Certificate IC.05.01
signed by Intermediate Certificate IC.05.01

**End Certificate IC.05.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.05.01
subject name: cn=User1-IC.05.01 (other RDNs preserved)
serial number: 56
signed by Intermediate Certificate IC.05.01

**Intermediate Certificate IC.05.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.05.02 (other RDNs preserved)
serial number: 57
keyUsage: present and not critical
  keyCertSign: FALSE
  cRLSign: TRUE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.05.02**

include Base CRL
issuer name: DN of Intermediate Certificate IC.05.02
signed by Intermediate Certificate IC.05.02

**End Certificate IC.05.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.05.02
subject name: cn=User1-IC.05.02 (other RDNs preserved)
serial number: 58
signed by Intermediate Certificate IC.05.02

**Intermediate Certificate IC.05.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.05.03 (other RDNs preserved)
serial number: 59
keyUsage: present and not critical
  keyCertSign: TRUE
  cRLSign: TRUE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.05.03**

include Base CRL
issuer name: DN of Intermediate Certificate IC.05.03
signed by Intermediate Certificate IC.05.03

**End Certificate IC.05.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.05.03
subject name: cn=User1-IC.05.03 (other RDNs preserved)
serial number: 60
signed by Intermediate Certificate IC.05.03

**Intermediate Certificate IC.06.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.06.01 (other RDNs preserved)
serial number: 61
keyUsage: present and critical
  keyCertSign: TRUE
  cRLSign: FALSE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate IC.06.01

signed by Intermediate Certificate IC.06.01

**End Certificate IC.06.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.06.01
subject name: cn=User1-IC.06.01 (other RDNs preserved)
serial number: 62
signed by Intermediate Certificate IC.06.01

**Intermediate Certificate IC.06.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.06.02 (other RDNs preserved)
serial number: 63
keyUsage: present and not critical
  cRLSign: FALSE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate IC.06.02
signed by Intermediate Certificate IC.06.02

**End Certificate IC.06.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.06.02
subject name: cn=User1-IC.06.02 (other RDNs preserved)
serial number: 64
signed by Intermediate Certificate IC.06.02

**Intermediate Certificate IC.06.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-IC.06.03 (other RDNs preserved)
serial number: 65
keyUsage: present and not critical
  keyCertSign: TRUE
  cRLSign: TRUE
signed by Trust Anchor CP.01.01

**Intermediate CRL IC.06.03**

include Base CRL
issuer name: DN of Intermediate Certificate IC.06.03
signed by Intermediate Certificate IC.06.03

**End Certificate IC.06.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate IC.06.03
subject name: cn=User1-IC.06.03 (other RDNs preserved)

serial number: 66
signed by Intermediate Certificate IC.06.03

### 5.4.3 Policy Processing Test Data

**Intermediate Certificate PP.01.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.01 (other RDNs preserved)
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
serial number: 67
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.01.01**

include Base CRL
issuer name: DN of Intermediate Certificate PP.01.01
signed by Intermediate Certificate PP.01.01

**End Certificate PP.01.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.01.01
subject name: cn=User1-PP.01.01 (other RDNs preserved)
serial number: 68
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate PP.01.01

**Intermediate Certificate PP.01.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.02 (other RDNs preserved)
serial number: 69
certificate policy extension not present
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.01.02**

include Base CRL
issuer name: DN of Intermediate Certificate PP.01.02
signed by Intermediate Certificate PP.01.02

**End Certificate PP.01.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.01.02
subject name: cn=User1-PP.01.02 (other RDNs preserved)
serial number: 70

certificate policy extension not present
signed by Intermediate Certificate PP.01.02

**Intermediate Certificate 1 PP.01.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.03 (other RDNs preserved)
serial number: 71
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.03**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.03
signed by Intermediate Certificate 1 PP.01.03

**Intermediate Certificate 2 PP.01.03**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.03
subject name: cn=CA2-PP.01.03 (other RDNs preserved)
serial number: 72
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 1 PP.01.03

**Intermediate CRL 2 PP.01.03**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.03
signed by Intermediate Certificate 2 PP.01.03

**End Certificate PP.01.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.03
subject name: cn=User1-PP.01.03 (other RDNs preserved)
serial number: 73
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 2 PP.01.03

**Intermediate Certificate 1 PP.01.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.04 (other RDNs preserved)
serial number: 74
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.04**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.04
signed by Intermediate Certificate 1 PP.01.04

**Intermediate Certificate 2 PP.01.04**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.04
subject name: cn=CA2-PP.01.04 (other RDNs preserved)
serial number: 75
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 1 PP.01.04

**Intermediate CRL 2 PP.01.04**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.04
signed by Intermediate Certificate 2 PP.01.04

**End Certificate PP.01.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.04
subject name: cn=User1-PP.01.04 (other RDNs preserved)
serial number: 76
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Intermediate Certificate 2 PP.01.04

**Intermediate Certificate 1 PP.01.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.05 (other RDNs preserved)
serial number: 77
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.05**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.05
signed by Intermediate Certificate 1 PP.01.05

**Intermediate Certificate 2 PP.01.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.05
subject name: cn=CA2-PP.01.05 (other RDNs preserved)
serial number: 78
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Intermediate Certificate 1 PP.01.05

**Intermediate CRL 2 PP.01.05**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.05
signed by Intermediate Certificate 2 PP.01.05

**End Certificate PP.01.05**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.05
subject name: cn=User1-PP.01.05 (other RDNs preserved)
serial number: 79
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 2 PP.01.05

**Intermediate Certificate 1 PP.01.06**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.06 (other RDNs preserved)
serial number: 80
certificate policy extension present, not critical, four certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3
- test-policy-4

signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.06
signed by Intermediate Certificate 1 PP.01.06

**Intermediate Certificate 2 PP.01.06**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.06
subject name: cn=CA2-PP.01.06 (other RDNs preserved)
serial number: 81
certificate policy extension present, not critical, three certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3

signed by Intermediate Certificate 1 PP.01.06

**Intermediate CRL 2 PP.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.06
signed by Intermediate Certificate 2 PP.01.06

**Intermediate Certificate 3 PP.01.06**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.06
subject name: cn=CA3-PP.01.06 (other RDNs preserved)
serial number: 82
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Intermediate Certificate 2 PP.01.06

**Intermediate CRL 3 PP.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.01.06
signed by Intermediate Certificate 3 PP.01.06

**End Certificate PP.01.06**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.01.06
subject name: cn=CA4-PP.01.06 (other RDNs preserved)
serial number: 83
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  (all others false)
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 3 PP.01.06

**Intermediate Certificate 1 PP.01.07**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.07 (other RDNs preserved)
serial number: 84
certificate policy extension present, not critical, three certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3

signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.07
signed by Intermediate Certificate 1 PP.01.07

**Intermediate Certificate 2 PP.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.07
subject name: cn=CA2-PP.01.07 (other RDNs preserved)
serial number: 85
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Intermediate Certificate 1 PP.01.07

**Intermediate CRL 2 PP.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.07
signed by Intermediate Certificate 2 PP.01.07

**Intermediate Certificate 3 PP.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.07
subject name: cn=CA3-PP.01.07 (other RDNs preserved)
serial number: 86
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 2 PP.01.07

**Intermediate CRL 3 PP.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.01.07
signed by Intermediate Certificate 3 PP.01.07

**End Certificate PP.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.01.07
subject name: cn=CA4-PP.01.07 (other RDNs preserved)
serial number: 87
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  (all others false)
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Intermediate Certificate 3 PP.01.07

**Intermediate Certificate 1 PP.01.08**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.08 (other RDNs preserved)
serial number: 88
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.08
signed by Intermediate Certificate 1 PP.01.08

**Intermediate Certificate 2 PP.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.08
subject name: cn=CA2-PP.01.08 (other RDNs preserved)
serial number: 89
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 1 PP.01.08

**Intermediate CRL 2 PP.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.08
signed by Intermediate Certificate 2 PP.01.08

**Intermediate Certificate 3 PP.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.08
subject name: cn=CA3-PP.01.08 (other RDNs preserved)
serial number: 90
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Intermediate Certificate 2 PP.01.08

**Intermediate CRL 3 PP.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.01.08
signed by Intermediate Certificate 3 PP.01.08

**End Certificate PP.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.01.08
subject name: cn=CA4-PP.01.08 (other RDNs preserved)
serial number: 91
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  (all others false)
signed by Intermediate Certificate 3 PP.01.08

**Intermediate Certificate 1 PP.01.09**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.01.09 (other RDNs preserved)
serial number: 92
certificate policy extension present, not critical, three certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3

signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.01.09
signed by Intermediate Certificate 1 PP.01.09

**Intermediate Certificate 2 PP.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.01.09
subject name: cn=CA2-PP.01.09 (other RDNs preserved)
serial number: 93
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Intermediate Certificate 1 PP.01.09

**Intermediate CRL 2 PP.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.01.09
signed by Intermediate Certificate 2 PP.01.09

**Intermediate Certificate 3 PP.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.01.09
subject name: cn=CA3-PP.01.09 (other RDNs preserved)
serial number: 94
certificate policy extension present, not critical, certPolicy oid set to test-policy-2
signed by Intermediate Certificate 2 PP.01.09

**Intermediate CRL 3 PP.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.01.09
signed by Intermediate Certificate 3 PP.01.09

**Intermediate Certificate 4 PP.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.01.09
subject name: cn=CA4-PP.01.09 (other RDNs preserved)
serial number: 95
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 3 PP.01.09

**Intermediate CRL 4 PP.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.01.09
signed by Intermediate Certificate 4 PP.01.09

**End Certificate PP.01.09**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.01.09
subject name: cn=User1-PP.01.09 (other RDNs preserved)
serial number: 96
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 4 PP.01.09

**Intermediate Certificate 1 PP.06.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.06.01 (other RDNs preserved)
serial number: 97
policy constraints extension present, not critical
requireExplicitPolicy present, skipCerts = 10
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.06.01
signed by Intermediate Certificate 1 PP.06.01

**Intermediate Certificate 2 PP.06.01**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.06.01
subject name: cn=CA2-PP.06.01 (other RDNs preserved)
serial number: 98
signed by Intermediate Certificate 1 PP.06.01

**Intermediate CRL 2 PP.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.06.01
signed by Intermediate Certificate 2 PP.06.01

**Intermediate Certificate 3 PP.06.01**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.06.01
subject name: cn=CA3-PP.06.01 (other RDNs preserved)
serial number: 99
signed by Intermediate Certificate 2 PP.06.01

**Intermediate CRL 3 PP.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.06.01
signed by Intermediate Certificate 3 PP.06.01

**Intermediate Certificate 4 PP.06.01**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.06.01
subject name: cn=CA4-PP.06.01 (other RDNs preserved)
serial number: 100
signed by Intermediate Certificate 3 PP.06.01

**Intermediate CRL 4 PP.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.06.01
signed by Intermediate Certificate 4 PP.06.01

**End Certificate PP.06.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.06.01
subject name: cn=User1-PP.06.01 (other RDNs preserved)
serial number: 101
certificate policy extension not present
signed by Intermediate Certificate 4 PP.06.01

**Intermediate Certificate 1 PP.06.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.06.02 (other RDNs preserved)
serial number: 102
policy constraints extension present, not critical
requireExplicitPolicy present, skipCerts = 5
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.06.02
signed by Intermediate Certificate 1 PP.06.02

**Intermediate Certificate 2 PP.06.02**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.06.02
subject name: cn=CA2-PP.06.02 (other RDNs preserved)
serial number: 103
signed by Intermediate Certificate 1 PP.06.02

**Intermediate CRL 2 PP.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.06.02
signed by Intermediate Certificate 2 PP.06.02

**Intermediate Certificate 3 PP.06.02**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.06.02
subject name: cn=CA3-PP.06.02 (other RDNs preserved)
serial number: 104
signed by Intermediate Certificate 2 PP.06.02

**Intermediate CRL 3 PP.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.06.02
signed by Intermediate Certificate 3 PP.06.02

**Intermediate Certificate 4 PP.06.02**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.06.02
subject name: cn=CA4-PP.06.02 (other RDNs preserved)
serial number: 105
signed by Intermediate Certificate 3 PP.06.02

**Intermediate CRL 4 PP.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.06.02
signed by Intermediate Certificate 4 PP.06.02

**End Certificate PP.06.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.06.02
subject name: cn=User1-PP.06.02 (other RDNs preserved)
serial number: 106
certificate policy extension not present
signed by Intermediate Certificate 4 PP.06.02

**Intermediate Certificate 1 PP.06.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.06.03 (other RDNs preserved)
serial number: 107
policy constraints extension present, not critical
requireExplicitPolicy present, skipCerts = 4
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.06.03**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.06.03
signed by Intermediate Certificate 1 PP.06.03

**Intermediate Certificate 2 PP.06.03**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.06.03
subject name: cn=CA2-PP.06.03 (other RDNs preserved)
serial number: 108
signed by Intermediate Certificate 1 PP.06.03

**Intermediate CRL 2 PP.06.03**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.06.03
signed by Intermediate Certificate 2 PP.06.03

**Intermediate Certificate 3 PP.06.03**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.06.03
subject name: cn=CA3-PP.06.03 (other RDNs preserved)
serial number: 109
signed by Intermediate Certificate 2 PP.06.03

**Intermediate CRL 3 PP.06.03**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.06.03
signed by Intermediate Certificate 3 PP.06.03

**Intermediate Certificate 4 PP.06.03**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.06.03
subject name: cn=CA4-PP.06.03 (other RDNs preserved)
serial number: 110
signed by Intermediate Certificate 3 PP.06.03

**Intermediate CRL 4 PP.06.03**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.06.03
signed by Intermediate Certificate 4 PP.06.03

**End Certificate PP.06.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.06.03
subject name: cn=User1-PP.06.03 (other RDNs preserved)
serial number: 111
certificate policy extension not present
signed by Intermediate Certificate 4 PP.06.03

**Intermediate Certificate 1 PP.06.04**

include Base Intermediate Certificate

issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.06.04 (other RDNs preserved)
serial number: 112
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
policy constraints extension present, not critical
requireExplicitPolicy present, skipCerts = 0
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.06.04**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.06.04
signed by Intermediate Certificate 1 PP.06.04

**Intermediate Certificate 2 PP.06.04**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.06.04
subject name: cn=CA2-PP.06.04 (other RDNs preserved)
serial number: 113
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 1 PP.06.04

**Intermediate CRL 2 PP.06.04**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.06.04
signed by Intermediate Certificate 2 PP.06.04

**Intermediate Certificate 3 PP.06.04**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.06.04
subject name: cn=CA3-PP.06.04 (other RDNs preserved)
serial number: 114
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 2 PP.06.04

**Intermediate CRL 3 PP.06.04**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.06.04
signed by Intermediate Certificate 3 PP.06.04

**Intermediate Certificate 4 PP.06.04**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.06.04
subject name: cn=CA4-PP.06.04 (other RDNs preserved)
serial number: 115
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 3 PP.06.04

**Intermediate CRL 4 PP.06.04**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.06.04
signed by Intermediate Certificate 4 PP.06.04

**End Certificate PP.06.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.06.04
subject name: cn=User1-PP.06.04 (other RDNs preserved)
serial number: 116
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Intermediate Certificate 4 PP.06.04

**Intermediate Certificate 1 PP.06.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.06.05 (other RDNs preserved)
serial number: 117
policy constraints extension present, not critical
    requireExplicitPolicy present, skipCerts = 7
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PP.06.05**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PP.06.05
signed by Intermediate Certificate 1 PP.06.05

**Intermediate Certificate 2 PP.06.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PP.06.05
subject name: cn=CA2-PP.06.05 (other RDNs preserved)
serial number: 118
policy constraints extension present, not critical
    requireExplicitPolicy present, skipCerts = 2
signed by Intermediate Certificate 1 PP.06.05

**Intermediate CRL 2 PP.06.05**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PP.06.05
signed by Intermediate Certificate 2 PP.06.05

**Intermediate Certificate 3 PP.06.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PP.06.05
subject name: cn=CA3-PP.06.05 (other RDNs preserved)
serial number: 119
policy constraints extension present, not critical

requireExplicitPolicy present, skipCerts = 4
signed by Intermediate Certificate 2 PP.06.05

**Intermediate CRL 3 PP.06.05**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PP.06.05
signed by Intermediate Certificate 3 PP.06.05

**Intermediate Certificate 4 PP.06.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PP.06.05
subject name: cn=CA4-PP.06.05 (other RDNs preserved)
serial number: 120
signed by Intermediate Certificate 3 PP.06.05

**Intermediate CRL 4 PP.06.05**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PP.06.05
signed by Intermediate Certificate 4 PP.06.05

**End Certificate PP.06.05**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PP.06.05
subject name: cn=User1-PP.06.05 (other RDNs preserved)
serial number: 121
certificate policy extension not present
signed by Intermediate Certificate 4 PP.06.05

**Intermediate Certificate PP.08.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.01 (other RDNs preserved)
serial number: 122
certificate policy extension present, not critical, certPolicy oid set to test-policy-1
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.01**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.01
signed by Intermediate Certificate PP.08.01

**End Certificate PP.08.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.01
subject name: cn=User1-PP.08.01 (other RDNs preserved)
serial number: 123
certificate policy extension present, not critical, certPolicy oid set to test-policy-1

signed by Intermediate Certificate PP.08.01

**Intermediate Certificate PP.08.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.02 (other RDNs preserved)
serial number: 124
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.02**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.02
signed by Intermediate Certificate PP.08.02

**End Certificate PP.08.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.02
subject name: cn=User1-PP.08.02 (other RDNs preserved)
serial number: 125
certificate policy extension present, not critical, two certPolicy oids set to

- test-policy-1
- test-policy-2

signed by Intermediate Certificate PP.08.02

**Intermediate Certificate PP.08.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.03 (other RDNs preserved)
serial number: 126
certificate policy extension present, not critical, certPolicy oid set to anyPolicy (2:5:29:32:0)
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.03**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.03
signed by Intermediate Certificate PP.08.03

**End Certificate PP.08.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.03
subject name: cn=User1-PP.08.03 (other RDNs preserved)
serial number: 127

certificate policy extension present, not critical, certPolicy oid set to anyPolicy (2:5:29:32:0)
signed by Intermediate Certificate PP.08.03

**Intermediate Certificate PP.08.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.04 (other RDNs preserved)
serial number: 128
certificate policy extension present, not critical, certPolicy oid set to test-policy-3
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.04**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.04
signed by Intermediate Certificate PP.08.04

**End Certificate PP.08.04**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.04
subject name: cn=User1-PP.08.04 (other RDNs preserved)
serial number: 129
certificate policy extension present, not critical, certPolicy oid set to test-policy-4
signed by Intermediate Certificate PP.08.04

**Intermediate Certificate PP.08.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.05 (other RDNs preserved)
serial number: 130
certificate policy extension present, not critical, certPolicy oid set to test-policy-3
signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.05**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.05
signed by Intermediate Certificate PP.08.05

**End Certificate PP.08.05**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.05
subject name: cn=User1-PP.08.05 (other RDNs preserved)
serial number: 131
certificate policy extension present, not critical, certPolicy oid set to test-policy-3
signed by Intermediate Certificate PP.08.05

**Intermediate Certificate PP.08.06**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PP.08.06 (other RDNs preserved)
serial number: 132
certificate policy extension present, not critical, three certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3

signed by Trust Anchor CP.01.01

**Intermediate CRL PP.08.06**

include Base CRL
issuer name: DN of Intermediate Certificate PP.08.06
signed by Intermediate Certificate PP.08.06

**End Certificate PP.08.06**

include Base End Certificate
issuer name: DN of Intermediate Certificate PP.08.06
subject name: cn=User1-PP.08.06 (other RDNs preserved)
serial number: 133
certificate policy extension present, not critical, three certPolicy oids set to

- test-policy-1
- test-policy-2
- test-policy-3

signed by Intermediate Certificate PP.08.06

### 5.4.4 Path Length Related Test Data

**Intermediate Certificate 1 PL.01.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.01 (other RDNs preserved)
serial number: 134
basic constraints extension, pathLenConstraint present and set to 0
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.01**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.01
signed by Intermediate Certificate 1 PL.01.01

**Intermediate Certificate 2 PL.01.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA2-PL.01.01 (other RDNs preserved)
serial number: 135

signed by Intermediate Certificate 1 PL.01.01

**Intermediate CRL 2 PL.01.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.01
signed by Intermediate Certificate 2 PL.01.01

**End Certificate PL.01.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.01
subject name: cn=User1-PL.01.01 (other RDNs preserved)
serial number: 136
signed by Intermediate Certificate 2 PL.01.01

**Intermediate Certificate 1 PL.01.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.02 (other RDNs preserved)
serial number: 137
basic constraints extension, pathLenConstraint present and set to 0
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.02**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.02
signed by Intermediate Certificate 1 PL.01.02

**Intermediate Certificate 2 PL.01.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.02
subject name: cn=CA2-PL.01.02 (other RDNs preserved)
serial number: 138
signed by Intermediate Certificate 1 PL.01.02

**Intermediate CRL 2 PL.01.02**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.02
signed by Intermediate Certificate 2 PL.01.02

**End Certificate PL.01.02**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.02
subject name: cn=CA3-PL.01.02 (other RDNs preserved)
serial number: 139
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE

keyEncipherment: TRUE
keyCertSign: TRUE
cRLSign: TRUE
(all others false)
signed by Intermediate Certificate 2 PL.01.02

**Intermediate Certificate PL.01.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.03 (other RDNs preserved)
serial number: 140
basic constraints extension, pathLenConstraint present and set to 0
signed by Trust Anchor CP.01.01

**Intermediate CRL PL.01.03**

include Base CRL
issuer name: DN of Intermediate Certificate PL.01.03
signed by Intermediate Certificate PL.01.03

**End Certificate PL.01.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate PL.01.03
subject name: cn=User1-PL.01.03 (other RDNs preserved)
serial number: 141
signed by Intermediate Certificate PL.01.03

**Intermediate Certificate PL.01.04**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.04 (other RDNs preserved)
serial number: 142
basic constraints extension, pathLenConstraint present and set to 0
signed by Trust Anchor CP.01.01

**Intermediate CRL PL.01.04**

include Base CRL
issuer name: DN of Intermediate Certificate PL.01.04
signed by Intermediate Certificate PL.01.04

**End Certificate PL.01.04**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate PL.01.04
subject name: cn=CA2-PL.01.04 (other RDNs preserved)
serial number: 143
keyUsage: present and critical
digitalSignature: TRUE
nonRepudiation: TRUE
keyEncipherment: TRUE

keyCertSign: TRUE
cRLSign: TRUE
(all others false)
signed by Intermediate Certificate PL.01.04

**Intermediate Certificate 1 PL.01.05**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.05 (other RDNs preserved)
serial number: 144
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.05**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.05
signed by Intermediate Certificate 1 PL.01.05

**Intermediate Certificate 2 PL.01.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.05
subject name: cn=CA2-PL.01.05 (other RDNs preserved)
serial number: 145
basic constraints extension, pathLenConstraint present and set to 0
signed by Intermediate Certificate 1 PL.01.05

**Intermediate CRL 2 PL.01.05**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.05
signed by Intermediate Certificate 2 PL.01.05

**Intermediate Certificate 3 PL.01.05**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.05
subject name: cn=CA3-PL.01.05 (other RDNs preserved)
serial number: 146
basic constraints extension, pathLenConstraint present and set to 0
signed by Intermediate Certificate 2 PL.01.05

**Intermediate CRL 3 PL.01.05**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PL.01.05
signed by Intermediate Certificate 3 PL.01.05

**End Certificate PL.01.05**

include Base End Certificate

issuer name: DN of Intermediate Certificate 3 PL.01.05
subject name: cn=User1-PL.01.05 (other RDNs preserved)
serial number: 147
signed by Intermediate Certificate 3 PL.01.05

**Intermediate Certificate 1 PL.01.06**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.06 (other RDNs preserved)
serial number: 148
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.06
signed by Intermediate Certificate 1 PL.01.06

**Intermediate Certificate 2 PL.01.06**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.06
subject name: cn=CA2-PL.01.06 (other RDNs preserved)
serial number: 149
basic constraints extension, pathLenConstraint present and set to 0
signed by Intermediate Certificate 1 PL.01.06

**Intermediate CRL 2 PL.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.06
signed by Intermediate Certificate 2 PL.01.06

**Intermediate Certificate 3 PL.01.06**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.06
subject name: cn=CA3-PL.01.06 (other RDNs preserved)
serial number: 150
basic constraints extension, pathLenConstraint present and set to 0
signed by Intermediate Certificate 2 PL.01.06

**Intermediate CRL 3 PL.01.06**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PL.01.06
signed by Intermediate Certificate 3 PL.01.06

**End Certificate PL.01.06**

include Base Intermediate Certificate

issuer name: DN of Intermediate Certificate 3 PL.01.06
subject name: cn=CA4-PL.01.06 (other RDNs preserved)
serial number: 151
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  keyCertSign: TRUE
  cRLSign: TRUE
  (all others false)
signed by Intermediate Certificate 3 PL.01.06

**Intermediate Certificate 1 PL.01.07**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.07 (other RDNs preserved)
serial number: 152
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.07
signed by Intermediate Certificate 1 PL.01.07

**Intermediate Certificate 2 PL.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.07
subject name: cn=CA2-PL.01.07 (other RDNs preserved)
serial number: 153
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 1 PL.01.07

**Intermediate CRL 2 PL.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.07
signed by Intermediate Certificate 2 PL.01.07

**Intermediate Certificate 3 PL.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.07
subject name: cn=CA3-PL.01.07 (other RDNs preserved)
serial number: 154
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 2 PL.01.07

**Intermediate CRL 3 PL.01.07**

include Base CRL

issuer name: DN of Intermediate Certificate 3 PL.01.07
signed by Intermediate Certificate 3 PL.01.07

**Intermediate Certificate 4 PL.01.07**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PL.01.07
subject name: cn=CA4-PL.01.07 (other RDNs preserved)
serial number: 155
signed by Intermediate Certificate 3 PL.01.07

**Intermediate CRL 4 PL.01.07**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PL.01.07
signed by Intermediate Certificate 4 PL.01.07

**End Certificate PL.01.07**

include Base End Certificate
issuer name: DN of Intermediate Certificate 4 PL.01.07
subject name: cn=User1-PL.01.07 (other RDNs preserved)
serial number: 156
signed by Intermediate Certificate 4 PL.01.07

**Intermediate Certificate 1 PL.01.08**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.08 (other RDNs preserved)
serial number: 157
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.08
signed by Intermediate Certificate 1 PL.01.08

**Intermediate Certificate 2 PL.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.08
subject name: cn=CA2-PL.01.08 (other RDNs preserved)
serial number: 158
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 1 PL.01.08

**Intermediate CRL 2 PL.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.08

signed by Intermediate Certificate 2 PL.01.08

**Intermediate Certificate 3 PL.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.08
subject name: cn=CA3-PL.01.08 (other RDNs preserved)
serial number: 159
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 2 PL.01.08

**Intermediate CRL 3 PL.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PL.01.08
signed by Intermediate Certificate 3 PL.01.08

**Intermediate Certificate 4 PL.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PL.01.08
subject name: cn=CA4-PL.01.08 (other RDNs preserved)
serial number: 160
signed by Intermediate Certificate 3 PL.01.08

**Intermediate CRL 4 PL.01.08**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PL.01.08
signed by Intermediate Certificate 4 PL.01.08

**End Certificate PL.01.08**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 4 PL.01.08
subject name: cn=CA5-PL.01.08 (other RDNs preserved)
serial number: 161
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  keyCertSign: TRUE
  cRLSign: TRUE
  (all others false)
signed by Intermediate Certificate 4 PL.01.08

**Intermediate Certificate 1 PL.01.09**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.09 (other RDNs preserved)
serial number: 162
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.09
signed by Intermediate Certificate 1 PL.01.09

**Intermediate Certificate 2 PL.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.09
subject name: cn=CA2-PL.01.09 (other RDNs preserved)
serial number: 163
basic constraints extension, pathLenConstraint present and set to 4
signed by Intermediate Certificate 1 PL.01.09

**Intermediate CRL 2 PL.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.09
signed by Intermediate Certificate 2 PL.01.09

**Intermediate Certificate 3 PL.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.09
subject name: cn=CA3-PL.01.09 (other RDNs preserved)
serial number: 164
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 2 PL.01.09

**Intermediate CRL 3 PL.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PL.01.09
signed by Intermediate Certificate 3 PL.01.09

**Intermediate Certificate 4 PL.01.09**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 3 PL.01.09
subject name: cn=CA4-PL.01.09 (other RDNs preserved)
serial number: 165
signed by Intermediate Certificate 3 PL.01.09

**Intermediate CRL 4 PL.01.09**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PL.01.09
signed by Intermediate Certificate 4 PL.01.09

**End Certificate PL.01.09**

include Base End Certificate

issuer name: DN of Intermediate Certificate 4 PL.01.09
subject name: cn=User1-PL.01.09 (other RDNs preserved)
serial number: 166
signed by Intermediate Certificate 4 PL.01.09

**Intermediate Certificate 1 PL.01.10**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-PL.01.10 (other RDNs preserved)
serial number: 167
basic constraints extension, pathLenConstraint present and set to 6
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 PL.01.10**

include Base CRL
issuer name: DN of Intermediate Certificate 1 PL.01.10
signed by Intermediate Certificate 1 PL.01.10

**Intermediate Certificate 2 PL.01.10**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 PL.01.10
subject name: cn=CA2-PL.01.10 (other RDNs preserved)
serial number: 168
basic constraints extension, pathLenConstraint present and set to 4
signed by Intermediate Certificate 1 PL.01.10

**Intermediate CRL 2 PL.01.10**

include Base CRL
issuer name: DN of Intermediate Certificate 2 PL.01.10
signed by Intermediate Certificate 2 PL.01.10

**Intermediate Certificate 3 PL.01.10**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 2 PL.01.10
subject name: cn=CA3-PL.01.10 (other RDNs preserved)
serial number: 169
basic constraints extension, pathLenConstraint present and set to 1
signed by Intermediate Certificate 2 PL.01.10

**Intermediate CRL 3 PL.01.10**

include Base CRL
issuer name: DN of Intermediate Certificate 3 PL.01.10
signed by Intermediate Certificate 3 PL.01.10

**Intermediate Certificate 4 PL.01.10**

include Base Intermediate Certificate

issuer name: DN of Intermediate Certificate 3 PL.01.10
subject name: cn=CA4-PL.01.10 (other RDNs preserved)
serial number: 170
signed by Intermediate Certificate 3 PL.01.10

**Intermediate CRL 4 PL.01.10**

include Base CRL
issuer name: DN of Intermediate Certificate 4 PL.01.10
signed by Intermediate Certificate 4 PL.01.10

**End Certificate PL.01.10**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 4 PL.01.10
subject name: cn=CA5-PL.01.10 (other RDNs preserved)
serial number: 171
keyUsage: present and critical
  digitalSignature: TRUE
  nonRepudiation: TRUE
  keyEncipherment: TRUE
  keyCertSign: TRUE
  cRLSign: TRUE
  (all others false)
signed by Intermediate Certificate 4 PL.01.10

5.4.5 Directly Issued Full CRL Related Test Data

**Intermediate Certificate RL.02.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.02.01 (other RDNs preserved)
serial number: 172
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.02.01**

include Base CRL
issuer name: DN of Intermediate Certificate RL.02.01
signed by Intermediate Certificate RL.02.01 (one or more bits in the signature is modified)

**End Certificate RL.02.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.02.01
subject name: cn=User1-RL.02.01 (other RDNs preserved)
serial number: 173
signed by Intermediate Certificate RL.02.01

**Intermediate Certificate 1 RL.03.01**

include Base Intermediate Certificate

issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.03.01 (other RDNs preserved)
serial number: 174
signed by Trust Anchor CP.01.01

**Intermediate Certificate 2 RL.03.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA2-RL.03.01 (other RDNs preserved)
serial number: 175
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.03.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 RL.03.01
signed by Intermediate Certificate 2 RL.03.01

**End Certificate RL.03.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 1 RL.03.01
subject name: cn=User1-RL.03.01 (other RDNs preserved)
serial number: 176
signed by Intermediate Certificate 1 RL.03.01

**Intermediate Certificate RL.03.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.03.02 (other RDNs preserved)
serial number: 177
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.03.02**

include Base CRL
issuer name: DN of Intermediate Certificate RL.02.01 (the wrong issuer)
revokedCertificate: present
  CertificateSerialNumber: 178 (the serial # of the end certificate)
signed by Intermediate Certificate RL.03.02

**End Certificate RL.03.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.03.02
subject name: cn=User1-RL.03.02 (other RDNs preserved)
serial number: 178
signed by Intermediate Certificate RL.03.02

**Intermediate Certificate RL.03.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.03.03 (other RDNs preserved)
serial number: 179
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 RL.03.03**

include Base CRL
issuer name: DN of Intermediate Certificate RL.02.01 (the wrong issuer)
revokedCertificate: present
  CertificateSerialNumber: 180 (the serial # of the end certificate)
signed by Intermediate Certificate RL.03.03

**Intermediate CRL 2 RL.03.03**

include Base CRL
issuer name: DN of Intermediate Certificate RL.03.03
signed by Intermediate Certificate RL.03.03

**End Certificate RL.03.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.03.03
subject name: cn=User1-RL.03.03 (other RDNs preserved)
serial number: 180
signed by Intermediate Certificate RL.03.03

**Intermediate Certificate 1 RL.05.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.05.01 (other RDNs preserved)
serial number: 181
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 RL.05.01**

include Base CRL
issuer name: DN of Intermediate Certificate 1 RL.05.01
revokedCertificate: present
  CertificateSerialNumber: 182 (the serial # of the intermediate certificate)
  crlEntryExtension:
    id-test-extension: present and critical
    privateNumber: 0
signed by Intermediate Certificate 1 RL.05.01

**Intermediate Certificate 2 RL.05.01**

include Base Intermediate Certificate

issuer name: DN of Intermediate Certificate 1 RL.05.01
subject name: cn=CA2-RL.05.01 (other RDNs preserved)
serial number: 182
signed by Intermediate Certificate 1 RL.05.01

**Intermediate CRL 2 RL.05.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 RL.05.01
signed by Intermediate Certificate 2 RL.05.01

**End Certificate RL.05.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 RL.05.01
subject name: cn=User1-RL.05.01 (other RDNs preserved)
serial number: 183
signed by Intermediate Certificate 2 RL.05.01

**Intermediate Certificate RL.05.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.05.02 (other RDNs preserved)
serial number: 184
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.05.02**

include Base CRL
issuer name: DN of Intermediate Certificate RL.05.02
revokedCertificate: present
  CertificateSerialNumber: 185 (the serial # of the end certificate)
  crlEntryExtension:
    id-test-extension: present and critical
    privateNumber: 0
signed by Intermediate Certificate RL.05.02

**End Certificate RL.05.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.05.02
subject name: cn=User1-RL.05.02 (other RDNs preserved)
serial number: 185
signed by Intermediate Certificate RL.05.02

**Intermediate Certificate 1 RL.06.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.06.01 (other RDNs preserved)
serial number: 186
signed by Trust Anchor CP.01.01

**Intermediate CRL 1 RL.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 1 RL.06.01
revokedCertificate: present
  CertificateSerialNumber: 187 (the serial # of the intermediate certificate)
  crlExtension:
    id-test-extension: present and critical
    privateNumber: 0
signed by Intermediate Certificate 1 RL.06.01

**Intermediate Certificate 2 RL.06.01**

include Base Intermediate Certificate
issuer name: DN of Intermediate Certificate 1 RL.06.01
subject name: cn=CA2-RL.06.01 (other RDNs preserved)
serial number: 187
signed by Intermediate Certificate 1 RL.06.01

**Intermediate CRL 2 RL.06.01**

include Base CRL
issuer name: DN of Intermediate Certificate 2 RL.06.01
signed by Intermediate Certificate 2 RL.06.01

**End Certificate RL.06.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate 2 RL.06.01
subject name: cn=User1-RL.06.01 (other RDNs preserved)
serial number: 188
signed by Intermediate Certificate 2 RL.06.01

**Intermediate Certificate RL.06.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.06.02 (other RDNs preserved)
serial number: 189
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.06.02**

include Base CRL
issuer name: DN of Intermediate Certificate RL.06.02
revokedCertificate: present
  CertificateSerialNumber: 190 (the serial # of the end certificate)
crlExtension:
  id-test-extension: present and critical
  privateNumber: 0
signed by Intermediate Certificate RL.06.02

**End Certificate RL.06.02**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.06.02
subject name: cn=User1-RL.06.02 (other RDNs preserved)
serial number: 190
signed by Intermediate Certificate RL.06.02

**Intermediate Certificate RL.07.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.07.01 (other RDNs preserved)
serial number: 191
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.07.01**

include Base CRL
issuer name: DN of Intermediate Certificate RL.07.01
thisUpdate: UTC:980101060100Z (January 1, 1998, 06:01:00)
nextUpdate: UTC:980101120100Z (January 1,1998, 12:01:00; earlier than current time)
signed by Intermediate Certificate RL.07.01

**End Certificate RL.07.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.07.01
subject name: cn=User1-RL.07.01 (other RDNs preserved)
serial number: 192
signed by Intermediate Certificate RL.07.01

**Intermediate Certificate RL.07.02**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.07.02 (other RDNs preserved)
serial number: 193
notBefore: UTC:500101060030Z (January 1,1950, 06:00:30)
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.07.02**

include Base CRL
issuer name: DN of Intermediate Certificate RL.07.02
thisUpdate: UTC:500101060100Z (January 1, 1950, 06:01:00)
nextUpdate: UTC:500101120100Z (January 1,1950, 12:01:00; should treat it as 1950; earlier than current time)
signed by Intermediate Certificate RL.07.02

**End Certificate RL.07.02**

include Base End Certificate

issuer name: DN of Intermediate Certificate RL.07.02
subject name: cn=User1-RL.07.02 (other RDNs preserved)
serial number: 194
signed by Intermediate Certificate RL.07.02

**Intermediate Certificate RL.07.03**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.07.03 (other RDNs preserved)
serial number: 195
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.07.03**

include Base CRL
issuer name: DN of Intermediate Certificate RL.07.03
thisUpdate: UTC:990101060100Z (January 1, 1999, 06:01:00)
nextUpdate: GT:20500101120100Z (January 1,2050, 12:01:00; later than current time)
signed by Intermediate Certificate RL.07.03

**End Certificate RL.07.03**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.07.03
subject name: cn=User1-RL.07.03 (other RDNs preserved)
serial number: 196
signed by Intermediate Certificate RL.07.03

**Intermediate Certificate RL.08.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.08.01 (other RDNs preserved)
serial number: 197
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.08.01**

include Base CRL
issuer name: DN of Intermediate Certificate RL.08.01
crlExtension:
deltaCRLIndicator: present and critical
BaseCRLNumber:1
signed by Intermediate Certificate RL.08.01

**End Certificate RL.08.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.08.01
subject name: cn=User1-RL.08.01 (other RDNs preserved)
serial number: 198
signed by Intermediate Certificate RL.08.01

**Intermediate Certificate RL.09.01**

include Base Intermediate Certificate
issuer name: DN of Trust Anchor CP.01.01
subject name: cn=CA1-RL.09.01 (other RDNs preserved)
serial number: 199
signed by Trust Anchor CP.01.01

**Intermediate CRL RL.09.01**

include Base CRL
issuer name: DN of Intermediate Certificate RL.09.01
crlExtension:
issuingDistributionPoint: present and critical
onlyContainsCaCerts: TRUE
signed by Intermediate Certificate RL.09.01

**End Certificate RL.09.01**

include Base End Certificate
issuer name: DN of Intermediate Certificate RL.09.01
subject name: cn=User1-RL.09.01 (other RDNs preserved)
serial number: 200
signed by Intermediate Certificate RL.09.01

# 6 LIST OF ACRONYMS

| | |
|---|---|
| **API** | Applications Programming Interface |
| **ARL** | Authority Revocation List |
| **CA** | Certification Authority |
| **CP** | Certificate Policy |
| **CRL** | Certificate Revocation List |
| **DN** | Distinguished Name |
| **DoD** | Department of Defense |
| **IDP** | Issuing Distribution Point Extension (in a **CRL**) |
| **PKI** | Public Key Infrastructure |
| **RDN** | Relative distinguished name |