Public Key Interoperability Test Suite (PKITS) Certification Path Validation

Version 1.0.1
April 14, 2011

Table of Contents

1 Introduction

1.1 Overview

A certification path is an ordered list of certificates starting with a certificate issued by the relying party's trust root, and ending with the target certificate that needs to be validated. Certification path validation procedures are based on the algorithm supplied in ITU-T Recommendation X.509 and further defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 3280. Certification path processing verifies the binding between the subject distinguished name and/or subject alternative name and the subject public key defined in the target certificate. The binding is limited by constraints, which are specified in the certificates that comprise the path, and inputs that are specified by the relying party. To ensure secure interoperation of PKI-enabled applications, the path validation must be done in accordance with the X.509 and RFC 3280 specifications. This document provides the test assertions and the test cases for testing path validation software against these specifications.

1.2 Background

In the fall of 2000, NIST worked in conjunction with CygnaCom Solutions and Getronics Government Solutions, LLC to develop a test suite for a subset of the features defined in the IETF PKIX Certificate and CRL Profile, RFC 2459. The resulting test suite, documented in *Conformance Testing of Relying Party Client Certificate Path Processing Logic* v. 1.07, has been widely used since its creation.

This document was developed in an effort to extend the previous test suite to cover most of the features described in the successor to RFC 2459, RFC 3280. The tests in the document include all of the tests from *Conformance Testing of Relying Party Client Certificate Path Processing Logic* in addition to tests covering certificate and CRL extensions that were not tested by that test suite. Section 5 of this document includes a table mapping tests from the original test suite to their corresponding tests in this test suite.

1.3 Getting the Test Data

Information about obtaining the data needed to run the tests in this test suite may be found at http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html. From this site it will be possible to download a copy of this document as well as all of the certificates, CRLs, S/MIME messages, and PKCS #12 files needed to run the tests in this test suite. The Web site will also specify the location of an LDAP server from which the certificates and CRLs used in this test suite may be retrieved.

2 References

2.1 Documents

PKCS#12	PKCS 12 v1.0: Personal Information Exchange Syntax. RSA Laboratories, June 1999.
RFC 822	Standard for the Format of ARPA Internet Text Messages, August 1982.
RFC 2253	IETF Request for Comments 2253, Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997.
RFC 2587	IETF Request for Comments 2587, Internet X.509 Public Key Infrastructure LDAP v2 Schema, June 1999.
RFC 3369	Cryptographic Message Syntax, August 2002.
RFC 3280	IETF Request for Comments 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002.
X.509	ITU-T Recommendation X.509 (03/2000), Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks.

2.2 Acronyms

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

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RDN	Relative Distinguished Name
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions
ITU-T	International Telecommunication Union - Telecommunication Standardization

Sector

2.3 Definitions

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

CA Certificate	A public key certificate whose subject is a CA.
Certification Path	A chain of certificates starting with 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 zero or more **Intermediate Certificates** and one **End Certificate.** The first certificate in a Certification Path of length greater than one is also called an **Intermediate Certificate**. The first certificate in a Certification Path of length one is called an **End Certificate** since it is the last certificate in the Certification Path.
Distinguished Name	An unambiguous name that identifies an entity. A distinguished name is made up of one or more relative distinguished names (RDNs).
End Certificate	The last certificate in a **Certification Path.**
End Entity Certificate	A public key certificate whose subject is not a CA.
Intermediate Certificate	Any certificate in a **Certification Path** except for the **End Certificate**.

3 Initialization Procedures

This section contains the initialization parameters needed to be set when performing the test cases defined in this document.

Most of the test cases are designed for processing with the following inputs:

- Trusted certificate to use (a.k.a. trust anchor) is Trust Anchor Root Certificate;
- *initial-policy-set* is the special value *any-policy*[1];
- *initial-explicit-policy* indicator value is false;
- *initial-policy-mapping-inhibit* indicator value is false; and
- *initial-inhibit-any-policy* indicator value is false.

The inputs listed above are referred to as the *default settings*. In many of the tests, different values may be used for many of the inputs without affecting the results. In all of the tests that are not related to policy processing, each certificate in the path asserts the certificate policy 2.16.840.1.101.3.2.1.48.1. As long as either the *initial-policy-set* includes this value or the *initial-explicit-policy* indicator is not set, the test results will not be affected in the non-policy processing tests. Similarly, the value of *initial-policy-mapping-inhibit* will not affect any of the tests in which none of the certificates contain a **policyMappings** extension and the value of *initial-inhibit-any-policy* will not affect any of the tests in which none of the certificates contain a **certificatePolicies** extension that includes the **anyPolicy** OID.

[1] In RFC 3280, the *initial-policy-set* is referred to as the user-initial-policy-set and *initial-inhibit-any-policy* is initial-any-policy-inhibit.

If an implementation can not set the *initial-policy-set* to *any-policy*, the tester should set the *initial-policy-set* to the set of six policies listed in section 3.1 whenever the test procedures specify that the *initial-policy-set* should be *any-policy*.

3.1 Test Certificate Policies

Some of the test cases include a step that sets the *initial-policy-set* to one or more certificate policies. In the test descriptions, the certificate policies are referenced using notional names assigned to improve readability. The following table maps the names used in the test descriptions with their Object Identifiers (OIDs).

Object Identifier	Registered Name	Name used in Test Cases
2.5.29.32.0	**anyPolicy**	**anyPolicy**
2.16.840.1.101.3.2.1.48.1	NIST test-policy-1	NIST-test-policy-1
2.16.840.1.101.3.2.1.48.2	NIST test-policy-2	NIST-test-policy-2
2.16.840.1.101.3.2.1.48.3	NIST test-policy-3	NIST-test-policy-3
2.16.840.1.101.3.2.1.48.4	NIST test-policy-4	NIST-test-policy-4
2.16.840.1.101.3.2.1.48.5	NIST test-policy-5	NIST-test-policy-5
2.16.840.1.101.3.2.1.48.6	NIST test-policy-6	NIST-test-policy-6

4 Certification Path Validation Tests

The tests specified in this section are designed to verify an application's ability to perform certification path validation as specified in X.509 and RFC 3280. Each subsection includes a set of tests that covers a different aspect of the path validation algorithm (e.g., a subsection may exercise the various features of a particular extension). The test suite was designed to cover most of the features of each of the fields and standard extensions defined in X.509.

4.1 Signature Verification

An application must be able to verify digital signatures on each certificate in the certification path using the public key from the previous certificate in the path (or the public key of the trust anchor to verify the signature on the first certificate in the path). The following test cases involve validating the signatures in the certificates found in a certification path.

4.1.1 Valid Signatures Test1

The purpose of this test is to verify an application's ability to name chain, signature chain, and check validity dates, on certificates in a certification path. It also tests processing of the basic constraints and key usage extensions in intermediate certificates.

Procedure: Validate Valid Certificate Path Test1 EE using the default settings[2] or open and verify Signed Test Message 6.2.2.1 using the default settings.

Expected Result: The path should validate successfully as all names and signatures chain, validity dates are correct, the intermediate certificate includes a basic constraints extensions that asserts **cA** is TRUE, and the key usage extension asserts both **keyCertSign** and **cRLSign**.

[2] The default settings are specified in Section 3.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid Certificate Path Test1 EE

4.1.2 Invalid CA Signature Test2

The purpose of this test is to verify an application's ability to recognize an invalid signature on an intermediate certificate in a certification path.

Procedure: Validate Invalid CA Signature Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.2 using the default settings.

Expected Result: The path should not validate successfully as the signature on the intermediate certificate is invalid.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Bad Signed CA Cert, Bad Signed CA CRL
- Invalid CA Signature Test2 EE

4.1.3 Invalid EE Signature Test3

The purpose of this test is to verify an application's ability to recognize an invalid signature on an end entity certificate in a certification path.

Procedure: Validate Invalid EE Signature Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.3 using the default settings.

Expected Result: The path should not validate successfully as the signature on the end entity certificate is invalid.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid EE Signature Test3 EE

4.1.4 Valid DSA Signatures Test4

The purpose of this test is to verify an application's ability to validate certificate in which DSA signatures are used. The intermediate CA and the end entity have DSA key pairs.

Procedure: Validate Valid DSA Signatures Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.222 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- DSA CA Cert, DSA CA CRL
- Valid DSA Signatures Test4 EE

4.1.5 Valid DSA Parameter Inheritance Test5

The purpose of this test is to verify an application's ability to validate DSA signatures when the DSA parameters are not included in a certificate and need to be inherited from a previous certificate in the path. The intermediate CAs and the end entity have DSA key pairs.

Procedure: Validate Valid DSA Parameter Inheritance Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.223 using the default settings .

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- DSA CA Cert, DSA CA CRL
- DSA Parameters Inherited CA Cert, DSA Parameters Inherited CA CRL
- Valid DSA Parameter Inheritance Test5 EE

4.1.6 Invalid DSA Signature Test6

The purpose of this test is to verify an application's ability to determine when a DSA signature is invalid. The intermediate CA and the end entity have DSA key pairs.

Procedure: Validate Invalid DSA Signature Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.224 using the default settings .

Expected Result: The path should not validate successfully as the signature on the end entity certificate is invalid.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- DSA CA Cert, DSA CA CRL
- Invalid DSA Signature Test6 EE

4.2 Validity Periods

The application must ensure that the **notBefore** time of each certificate in the certification path is earlier than or equal to the current time and that the **notAfter** time of each certificate in the certification path is later than or equal to the current time. The following test cases involve validating the **notBefore** time and **notAfter** time in the certificates found in a certification path.

4.2.1 Invalid CA notBefore Date Test1

In this test, the intermediate certificate's **notBefore** date is after the current date.

Procedure: Validate Invalid CA notBefore Date Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.4 using the default settings.

Expected Result: The path should not validate successfully as the **notBefore** date in the intermediate certificate is after the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Bad notBefore Date CA Cert, Bad notBefore Date CA CRL
- Invalid CA notBefore Date Test1 EE

4.2.2 Invalid EE notBefore Date Test2

In this test, the end entity certificate's **notBefore** date is after the current date.

Procedure: Validate Invalid EE notBefore Date Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.5 using the default settings.

Expected Result: The path should not validate successfully as the **notBefore** date in the end entity certificate is after the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid EE notBefore Date Test2 EE

4.2.3 Valid pre2000 UTC notBefore Date Test3

In this test, the end entity certificate's **notBefore** date is set to 1950 and is encoded in **UTCTime**.

Procedure: Validate Valid pre2000 UTC notBefore Date Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.6 using the default settings.

Expected Result: The path should validate successfully as the **notBefore** date in the end entity certificate is before the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid pre2000 UTC notBefore Date Test3 EE

4.2.4 Valid GeneralizedTime notBefore Date Test4

In this test, the end entity certificate's **notBefore** date is specified in **GeneralizedTime**.

Procedure: Validate Valid GeneralizedTime notBefore Date Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.7 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid GeneralizedTime notBefore Date Test4 EE

4.2.5 Invalid CA notAfter Date Test5

In this test, the intermediate certificate's **notAfter** date is before the current date.

Procedure: Validate Invalid CA notAfter Date Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.8 using the default settings.

Expected Result: The path should not validate successfully as the **notAfter** date in the intermediate certificate is before the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Bad notAfter Date CA Cert, Bad notAfter Date CA CRL
- Invalid CA notAfter Date Test5 EE

4.2.6 Invalid EE notAfter Date Test6

In this test, the end entity certificate's **notAfter** date is before the current date.

Procedure: Validate Invalid EE notAfter Date Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.9 using the default settings.

Expected Result: The path should not validate successfully as the **notAfter** date in the end certificate is before the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid EE notAfter Date Test6 EE

4.2.7 Invalid pre2000 UTC EE notAfter Date Test7

In this test, the end entity certificate's **notAfter** date is 1999 and is encoded in **UTCTime**.

Procedure: Validate Invalid pre2000 UTC EE notAfter Date Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.10 using the default settings.

Expected Result: The path should not validate successfully as the **notAfter** date in the end certificate is before the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid pre2000 UTC EE notAfter Date Test7 EE

4.2.8 Valid GeneralizedTime notAfter Date Test8

In this test, the end entity certificate's **notAfter** date is 2050 and is encoded in **GeneralizedTime**.

Procedure: Validate Valid GeneralizedTime notAfter Date Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.11 using the default settings.

Expected Result: The path should validate successfully as the **notAfter** date in the end certificate is after the current date.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid GeneralizedTime notAfter Date Test8 EE

4.3 Verifying Name Chaining

X.509 states than an application must check that names chain correctly within a certification path. Correct chaining is when the issuer name in each certificate in the certification path matches the subject name of the previous certificate in the path. (In the case of the first certificate in the path, the issuer of the certificate must be equal to the trust anchor name). The following statements from X.509 and RFC 3280 apply:

> [X.509 10.5.1] (Check) that the certificate subject and certificate issuer names chain correctly.
>
> [RFC3280 4.1.2.4] Attribute values in PrintableString are compared after removing leading and trailing white space and converting internal substrings of one or more consecutive white space characters to a single space.

4.3.1 Invalid Name Chaining EE Test1

In this test, the common name (cn=) portion of the issuer's name in the end entity certificate does not match the common name portion of the subject's name in the preceding intermediate certificate.

Procedure: Validate Invalid Name Chaining Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.12 using the default settings.

Expected Result: The path should not validate successfully as the names do not chain.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid Name Chaining Test1 EE

4.3.2 Invalid Name Chaining Order Test2

In this test, the issuer's name in the end entity certificate and the subject's name in the preceding intermediate certificate contain the same relative distinguished names (RDNs), but their ordering is different.

Procedure: Validate Invalid Name Chaining Order Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.13 using the default settings.

Expected Result: The path should not validate successfully as the names do not chain.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Name Ordering CA Cert, Name Order CA CRL
- Invalid Name Chaining Order Test2 EE

4.3.3 Valid Name Chaining Whitespace Test3

In this test, the issuer's name in the end entity certificate and the subject's name in the preceding intermediate certificate differ in internal whitespace, but match once the internal whitespace is compressed.

Procedure: Validate Valid Name Chaining Whitespace Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.14 using the default settings.

Expected Result: The path should validate successfully as the names chain.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid Name Chaining Whitespace Test3 EE

4.3.4 Valid Name Chaining Whitespace Test4

In this test, the issuer's name in the end entity certificate and the subject's name in the preceding intermediate certificate differ in leading and trailing whitespace, but match once all leading and trailing whitespace is removed.

Procedure: Validate Valid Name Chaining Whitespace Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.15 using the default settings.

Expected Result: The path should validate successfully as the names chain.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid Name Chaining Whitespace Test4 EE

4.3.5 Valid Name Chaining Capitalization Test5

In this test, the issuer's name in the end entity certificate and the subject's name in the preceding intermediate certificate differ in capitalization, but match when a case insensitive match is performed.

Procedure: Validate Valid Name Chaining Capitalization Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.16 using the default settings.

Expected Result: The path should validate successfully as the names chain.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid Name Chaining Capitalization Test5 EE

4.3.6 Valid Name Chaining UIDs Test6

In this test, the intermediate certificate includes a **subjectUniqueID** and the end entity certificate includes a matching **issuerUniqueID**.

Procedure: Validate Valid Name UIDs Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.17 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- UID CA Cert, UID CA CRL
- Valid Name UIDs Test6 EE

4.3.7 Valid RFC3280 Mandatory Attribute Types Test7

In this test, this intermediate certificate includes a **subject** name that includes the attribute types distinguished name qualifier, state or province name, serial number, domain component, organization, and country.

Procedure: Validate Valid RFC3280 Mandatory Attribute Types Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.213 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- RFC3280 Mandatory Attribute Types CA Cert, RFC3280 Mandatory Attribute Types CA CRL
- Valid RFC3280 Mandatory Attribute Types Test7 EE

4.3.8 Valid RFC3280 Optional Attribute Types Test8

In this test, this intermediate certificate includes a **subject** name that includes the attribute types locality, title, surname, given name, initials, pseudonym, generation qualifier, organization, and country.

Procedure: Validate Valid RFC3280 Optional Attribute Types Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.214 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- RFC3280 Optional Attribute Types CA Cert, RFC3280 Optional Attribute Types CA CRL
- Valid RFC3280 Optional Attribute Types Test8 EE

4.3.9 Valid UTF8String Encoded Names Test9

In this test, the attribute values for the common name and organization attribute types in the **subject** fields of the intermediate and end certificates and the **issuer** fields of the end certificate and the intermediate certificate's CRL are encoded in **UTF8String**.

Procedure: Validate Valid UTF8String Encoded Names Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.215 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- UTF8String Encoded Names CA Cert, UTF8String Encoded Names CA CRL
- Valid UTF8String Encoded Names Test9 EE

4.3.10 Valid Rollover from PrintableString to UTF8String Test10

In this test, the attribute values for the common name and organization attribute types in the **issuer** and **subject** fields of the end certificate and the **issuer** field of the intermediate certificate's CRL are encoded in **UTF8String**. However, these attribute types are encoded in **PrintableString** in the **subject** field of the intermediate certificate.

Procedure: Validate Valid Rollover from PrintableString to UTF8String Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.216 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Rollover from PrintableString to UTF8String CA Cert, Rollover from PrintableString to UTF8String CA CRL
- Valid Rollover from PrintableString to UTF8String Test10 EE

4.3.11 Valid UTF8String Case Insensitive Match Test11

In this test, the attribute values for the common name and organization attribute types in the **subject** fields of the intermediate and end certificates and the **issuer** fields of the end certificate and the intermediate certificate's CRL are encoded in **UTF8String**. The **subject** of the intermediate certificate and the **issuer** of the end certificate differ in capitalization and whitespace, but match when a case insensitive match is performed.

Procedure: Validate Valid UTF8String Case Insensitive Match Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.217 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- UTF8String Case Insensitive Match CA Cert, UTF8String Case Insensitive Match CA CRL
- Valid UTF8String Case Insensitive Match Test11 EE

4.4 Basic Certificate Revocation Tests

The application must be able to retrieve valid revocation data for each certificate in the path. For a

CRL to be considered to contain valid revocation data for a certificate, the CRL must at a minimum: (1) be signed by the issuer of the certificate or by an entity that has been authorized by the certificate issuer to provide status information for the certificate; (2) have a scope that includes the certificate of interest; and (3) be sufficiently up-to-date.

In general, if the current time is before the time specified in the **nextUpdate** field of a CRL, then that CRL should be considered sufficiently up-to-date since the CRL issuer has indicated that this CRL may contain the most up-to-date information available. Similarly, if the current time is after the time specified in the **nextUpdate** field of a CRL, then the CRL should not be considered to be sufficiently up-to-date since the CRL issuer has indicated that more up-to-date information should be available.

Even if the current time is after the time specified in the **nextUpdate** field of a CRL, an application may still make a local decision to treat the CRL as being sufficiently up-to-date. The application may, for example, be configurable to allow CRLs to be treated as sufficiently up-to-date, even if the current time is after the **nextUpdate** time, if the CRL was issued recently (e.g., the user or administrator configuring the system could indicate that a CRL may be used as long as the current time is within 72 hours of the **thisUpdate** time in the CRL, no matter how frequently the CRL issuer chooses to issue CRLs).

In this section, there are only two tests in which the **nextUpdate** time in a CRL is before the current time. In each case, the **nextUpdate** time (and **thisUpdate** time) is more than a year before the current time. So, it is expected that applications will be configured so that these CRLs are not considered to be sufficiently up-to-date.

Even if an application is unable to find valid revocation data (that is considered to be sufficiently up-to-date) for every certificate in the path, the application may still make a local decision to use the certification path. The application may, for example, allow the user or an administrator to configure the application to ignore the unavailability of revocation data. In the case of an interactive application, the application may display a warning to the user and then allow the user to decide whether to proceed to use the certification path despite the lack of revocation data. However, the application may not be designed in such a way that the unavailability of revocation data is always ignored, whether the user (or administrator) wants the application to behave that way or not. When running the tests in this section, the application should be configured in such a way that the certification path is not accepted unless valid, up-to-date revocation data is available for every certificate in the path. Thus, when run in this configuration, when the application is unable to find valid, up-to-date revocation data for every certificate in the path, the application must either reject the certification path or at least display a warning to the user indicating that the status of the certificate can not be determined.

4.4.1 Missing CRL Test1

In this test, there is no revocation information available from the intermediate CA, making it impossible to determine the status of the end certificate.

Procedure: Validate Invalid Missing CRL Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.18 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- No CRL CA Cert
- Invalid Missing CRL Test1 EE

4.4.2 Invalid Revoked CA Test2

In this test, the CRL issued by the first intermediate CA indicates that the second intermediate certificate in the path has been revoked.

Procedure: Validate Invalid Revoked CA Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.19 using the default settings.

Expected Result: The path should not validate successfully since one of the intermediate certificates has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Revoked subCA Cert, Revoked subCA CRL
- Invalid Revoked CA Test2 EE

4.4.3 Invalid Revoked EE Test3

In this test, the CRL issued by the intermediate CA indicates that the end entity certificate has been revoked.

Procedure: Validate Invalid Revoked EE Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.20 using the default settings.

Expected Result: The path should not validate successfully since the end certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Invalid Revoked EE Test3 EE

4.4.4 Invalid Bad CRL Signature Test4

In this test, the signature on the CRL issued by the intermediate CA is invalid.

Procedure: Validate Invalid Bad CRL Signature Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.21 using the default settings.

Expected Result: The path should not validate successfully since no valid revocation information is available for the end entity's certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Bad CRL Signature CA Cert, Bad CRL Signature CA CRL
- Invalid Bad CRL Signature Test4 EE

4.4.5 Invalid Bad CRL Issuer Name Test5

In this test, the issuer name in the CRL signed by the intermediate CA does not match the issuer name in the end entity's certificate.

Procedure: Validate Invalid Bad CRL Issuer Name Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.22 using the default settings.

Expected Result: The path should not validate successfully since no valid revocation information is available for the end entity's certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Bad CRL Issuer Name CA Cert, Bad CRL Issuer Name CA CRL
- Invalid Bad CRL Issuer Name Test5 EE

4.4.6 Invalid Wrong CRL Test6

In this test, the wrong CRL is in the intermediate certificate's directory entry. There is no CRL available from the intermediate CA making it impossible to determine the status of the end entity's certificate.

Procedure: Validate Invalid Wrong CRL Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.23 using the default settings.

Expected Result: The path should not validate successfully since no valid revocation information is available for the end entity's certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Wrong CRL CA Cert, Wrong CRL CA CRL
- Invalid Wrong CRL Test6 EE

4.4.7 Valid Two CRLs Test7

In this test, there are two CRLs in the intermediate CAs directory entry, one that is correct and one that contains the wrong issuer name. The correct CRL does not list any certificates as revoked. The incorrect CRL includes the serial number of the end entity's certificate on its list of revoked certificates.

Procedure: Validate Valid Two CRLs Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.24 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Two CRLs CA Cert, Two CRLs CA Good CRL, Two CRLs CA Bad CRL
- Valid Two CRLs Test7 EE

4.4.8 Invalid Unknown CRL Entry Extension Test8

In this test, the end entity's certificate has been revoked. In the intermediate CA's CRL, there is a made up critical **crlEntryExtension** associated with the end entity certificate's serial number.

> [X.509 7.3] When an implementation processing a CRL encounters the serial number of the certificate of interest in a CRL entry, but does not recognize a critical extension in the **crlEntryExtensions** field from that CRL entry, that CRL cannot be used to determine the status of the certificate.

Procedure: Validate Invalid Unknown CRL Entry Extension Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.25 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Unknown CRL Entry Extension CA Cert, Unknown CRL Entry Extension CA CRL
- Invalid Unknown CRL Entry Extension Test8 EE

4.4.9 Invalid Unknown CRL Extension Test9

In this test, the end entity's certificate has been revoked. In the intermediate CA's CRL, there is a made up critical extension in the **crlExtensions** field.

> [X.509 7.3] When an implementation does not recognize a critical extension in the **crlExtensions** field, that CRL cannot be used to determine the status of the certificate, regardless of whether the serial number of the certificate of interest appears in that CRL or not.

Procedure: Validate Invalid Unknown CRL Extension Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.26 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Unknown CRL Extension CA Cert, Unknown CRL Extension CA CRL
- Invalid Unknown CRL Extension Test9 EE

4.4.10 Invalid Unknown CRL Extension Test10

In this test the intermediate CA's CRL contains a made up critical extension in the **crlExtensions** field. The end entity certificate's serial number is not listed on the CRL, however, due to the presence of an unknown critical CRL extension, the relying party can not be sure that the list of serial numbers on the **revokedCertificates** list includes all certificates that have been revoked by the intermediate CA. As a result, the relying party can not verify that the end entity's certificate has not been revoked.

Procedure: Validate Invalid Unknown CRL Extension Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.27 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity's certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Unknown CRL Extension CA Cert, Unknown CRL Extension CA CRL
- Invalid Unknown CRL Extension Test10 EE

4.4.11 Invalid Old CRL nextUpdate Test11

In this test the intermediate CA's CRL has a **nextUpdate** time that is far in the past (January 2010), indicating that the CA has already issued updated revocation information. Since the information in the CRL is out-of-date and a more up-to-date CRL (that should have already been issued) can not be obtained, the certification path should be treated as if the status of the end entity certificate can not be determined.[3]

Procedure: Validate Invalid Old CRL nextUpdate Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.28 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity's certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Old CRL nextUpdate CA Cert, Old CRL nextUpdate CA CRL
- Invalid Old CRL nextUpdate Test11 EE

4.4.12 Invalid pre2000 CRL nextUpdate Test12

In this test the intermediate CA's CRL has a **nextUpdate** time that is in 1999 indicating that the CA has already issued updated revocation information. Since the information in the CRL is out-of-date and a more up-to-date CRL (that should have already been issued) can not be obtained, the certification path should be treated as if the status of the end entity certificate can not be determined.

Procedure: Validate Invalid pre2000 CRL nextUpdate Test12 EE using the default settings or open and verify Signed Test Message 6.2.2.29 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity's certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pre2000 CRL nextUpdate CA Cert, pre2000 CRL nextUpdate CA CRL
- Invalid pre2000 CRL nextUpdate Test12 EE

[3] See the introduction to Section 4.4 for more information.

4.4.13 Valid GeneralizedTime CRL nextUpdate Test13

In this test the intermediate CA's CRL has a **nextUpdate** time that is in 2050. Since the **nextUpdate** time is in the future, this CRL may contain the most up-to-date certificate status information that is available from the intermediate CA and so the relying party may use this CRL to determine the status of the end entity certificate.

Procedure: Validate Valid GeneralizedTime CRL nextUpdate Test13 EE using the default settings or open and verify Signed Test Message 6.2.2.30 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- GeneralizedTime CRL nextUpdate CA Cert, GeneralizedTime CRL nextUpdate CA CRL
- Valid GeneralizedTime CRL nextUpdate Test13 EE

4.4.14 Valid Negative Serial Number Test14

RFC 3280 mandates that certificate serial numbers be positive integers, but states that relying parties should be prepared to gracefully handle certificates with serial numbers that are negative, or zero. In this test, the end entity's certificate has a serial number of 255 (DER encoded as "00 FF") and the corresponding CRL lists the certificate with serial number -1 (DER encoded as "FF") as revoked.

Procedure: Validate Valid Negative Serial Number Test14 EE using the default settings or open and verify Signed Test Message 6.2.2.31 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Negative Serial Number CA Cert, Negative Serial Number CA CRL
- Valid Negative Serial Number Test14 EE

4.4.15 Invalid Negative Serial Number Test15

RFC 3280 mandates that certificate serial numbers be positive integers, but states that relying parties should be prepared to gracefully handle certificates with serial numbers that are negative, or zero. In this test, the end entity's certificate has a serial number of -1 (DER encoded as "FF") and the corresponding CRL lists this certificate as revoked.

Procedure: Validate Invalid Negative Serial Number Test15 EE using the default settings or open and verify Signed Test Message 6.2.2.32 using the default settings.

Expected Result: The path should not validate successfully as the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Negative Serial Number CA Cert, Negative Serial Number CA CRL

- Invalid Negative Serial Number Test15 EE

4.4.16 Valid Long Serial Number Test16

RFC 3280 mandates that certificate users be able to handle serial number values up to 20 octets long. In this test, the end entity's certificate has a 20 octet serial number that is not listed on the corresponding CRL, but the serial number matches the serial number listed on the CRL in all but the least significant octet.

Procedure: Validate Valid Long Serial Number Test16 EE using the default settings or open and verify Signed Test Message 6.2.2.33 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Long Serial Number CA Cert, Long Serial Number CA CRL
- Valid Long Serial Number Test16 EE

4.4.17 Valid Long Serial Number Test17

RFC 3280 mandates that certificate users be able to handle serial number values up to 20 octets long. In this test, the end entity's certificate has a 20 octet serial number that is not listed on the corresponding CRL, but the serial number matches the serial number listed on the CRL in all but the most significant octet.

Procedure: Validate Valid Long Serial Number Test17 EE using the default settings or open and verify Signed Test Message 6.2.2.34 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Long Serial Number CA Cert, Long Serial Number CA CRL
- Valid Long Serial Number Test17 EE

4.4.18 Invalid Long Serial Number Test18

RFC 3280 mandates that certificate users be able to handle serial number values up to 20 octets long. In this test, the end entity's certificate has a 20 octet serial number and the certificate's serial number is listed on the corresponding CRL.

Procedure: Validate Invalid Long Serial Number Test18 EE using the default settings or open and verify Signed Test Message 6.2.2.35 using the default settings.

Expected Result: The path should not validate successfully since the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Long Serial Number CA Cert, Long Serial Number CA CRL
- Invalid Long Serial Number Test18 EE

4.4.19 Valid Separate Certificate and CRL Keys Test19

In this test, the intermediate CA uses different keys to sign certificates and CRLs. The Trust Anchor CA has issued two certificates to the intermediate CA, one for each key. The end entity's certificate was signed using the intermediate CA's certificate signing key.

Procedure: Validate Valid Separate Certificate and CRL Keys Test19 EE using the default settings or open and verify Signed Test Message 6.2.2.219 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Separate Certificate and CRL Keys Certificate Signing CA Cert, Separate Certificate and CRL Keys CRL Signing Cert, Separate Certificate and CRL Keys CRL
- Valid Separate Certificate and CRL Keys Test19 EE

4.4.20 Invalid Separate Certificate and CRL Keys Test20

In this test, the intermediate CA uses different keys to sign certificates and CRLs. The Trust Anchor CA has issued two certificates to the intermediate CA, one for each key. The end entity's certificate was signed using the intermediate CA's certificate signing key. The CRL issued by the intermediate CA lists the end entity's certificate as revoked.

Procedure: Validate Invalid Separate Certificate and CRL Keys Test20 EE using the default settings or open and verify Signed Test Message 6.2.2.220 using the default settings.

Expected Result: The path not should validate successfully since the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Separate Certificate and CRL Keys Certificate Signing CA Cert, Separate Certificate and CRL Keys CRL Signing Cert, Separate Certificate and CRL Keys CRL
- Invalid Separate Certificate and CRL Keys Test20 EE

4.4.21 Invalid Separate Certificate and CRL Keys Test21

In this test, the intermediate CA uses different keys to sign certificates and CRLs. The Trust Anchor CA has issued two certificates to the intermediate CA, one for each key. The certificate issued to the intermediate CA's CRL verification key has been revoked. The end entity's certificate was signed using the intermediate CA's certificate signing key.

Procedure: Validate Invalid Separate Certificate and CRL Keys Test21 EE using the default settings or open and verify Signed Test Message 6.2.2.221 using the default settings.

Expected Result: The path not should validate successfully since the status of the end entity's certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert, Separate Certificate and CRL Keys CA2 CRL Signing Cert, Separate Certificate and CRL Keys CA2 CRL
- Invalid Separate Certificate and CRL Keys Test21 EE

4.5 Verifying Paths with Self-Issued Certificates

CA's certificate signing keys are used for finite periods of time. Typically, at the time that a CA rekeys, the previous public key is still considered to be valid. This allows relying parties to continue to validate certificates that were signed using the previous private signing key. In order facilitate continuity of operations, the CA, at the time of rekey, will issue two self-issued certificates: one certificate that contains the new public key that is signed using the old private key and one certificate that contains the old public key that is signed using the new private key.

While the CA will only use its new private key to sign certificates, the CA may continue to use the previous private key to sign CRLs that cover the certificates that were signed with that key. Using this technique, the CRL that covers a certificate can always be verified using the same public key that is used to verify the certificate.

Some CAs, for security reasons, will choose to destroy all copies of its private certificate signing key immediately after rekey, even if there are still valid certificates that were signed using this key. In this case, the CRLs that cover the certificates signed with the old private key must be signed using a different private key (e.g., the private key that is currently being used to sign certificates).

A CA may also choose to use two key pairs at the same time: one for certificate signing and one for CRL signing. In this case, the CA will typically issue a self-issued certificate that contains the CRL signing key that is signed using the certificate signing key.

4.5.1 Valid Basic Self-Issued Old With New Test1

In this test, the Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's new public key. The end entity's certificate was signed using the intermediate CA's old private key, requiring the relying party to use the CA's old-signed-with-new self-issued certificate in order to validate the end entity's certificate. The intermediate CA issues one CRL, signed with its new private key, that covers all of the unexpired certificates that it has issued.

Procedure: Validate Valid Basic Self-Issued Old With New Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.36 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued New Key CA Cert, Basic Self-Issued New Key CA CRL
- Basic Self-Issued New Key OldWithNew CA Cert
- Valid Basic Self-Issued Old With New Test1 EE

4.5.2 Invalid Basic Self-Issued Old With New Test2

In this test, the Trust Anchor CA has issued a certificate to the intermediate CA that contains the

intermediate CA's new public key. The end entity's certificate was signed using the intermediate CA's old private key, requiring the relying party to use the CA's old-signed-with-new self-issued certificate in order to validate the end entity's certificate. The intermediate CA issues one CRL, signed with its new private key, that covers all of the unexpired certificates that it has issued. This CRL indicates that the end entity's certificate has been revoked.

Procedure: Validate Invalid Basic Self-Issued Old With New Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.37 using the default settings.

Expected Result: The path should not validate successfully as the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued New Key CA Cert, Basic Self-Issued New Key CA CRL
- Basic Self-Issued New Key OldWithNew CA Cert
- Invalid Basic Self-Issued Old With New Test2 EE

4.5.3 Valid Basic Self-Issued New With Old Test3

In this test, the Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's old public key. The end entity's certificate and a CRL covering all certificates issued by the intermediate CA was signed using the intermediate CA's new private key, requiring the relying party to use the CA's new-signed-with-old self-issued certificate in order to validate both the end entity's certificate and the intermediate CA's CRL. There is a second CRL, signed using the intermediate CA's old private key that only covers the new-signed-with-old self-issued certificate.

Procedure: Validate Valid Basic Self-Issued New With Old Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.38 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key Self-Issued Cert CRL
- Basic Self-Issued Old Key NewWithOld CA Cert, Basic Self-Issued Old Key CA CRL
- Valid Basic Self-Issued New With Old Test3 EE

4.5.4 Valid Basic Self-Issued New With Old Test4

In this test, the Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's old public key. The end entity's certificate was signed using the intermediate CA's old private key, so there is no need to use a self-issued certificate to create a certification path from the Trust Anchor to the end entity. However, the CRL covering all certificates issued by the intermediate CA was signed using the intermediate CA's new private key, requiring the relying party to use the CA's new-signed-with-old self-issued certificate in order to validate the intermediate CA's CRL. This CRL must be validated in order to determine the status of the end entity's certificate. There is a second CRL, signed using the intermediate CA's old private key that only covers the new-signed-with-old self-issued certificate.

Procedure: Validate Valid Basic Self-Issued New With Old Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.39 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key Self-Issued Cert CRL
- Basic Self-Issued Old Key NewWithOld CA Cert, Basic Self-Issued Old Key CA CRL
- Valid Basic Self-Issued New With Old Test4 EE

4.5.5 Invalid Basic Self-Issued New With Old Test5

In this test, the Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's old public key. The end entity's certificate was signed using the intermediate CA's old private key, so there is no need to use a self-issued certificate to create a certification path from the Trust Anchor to the end entity. However, the CRL covering all certificates issued by the intermediate CA was signed using the intermediate CA's new private key, requiring the relying party to use the CA's new-signed-with-old self-issued certificate in order to validate the intermediate CA's CRL. This CRL must be validated in order to determine the status of the end entity's certificate. There is a second CRL, signed using the intermediate CA's old private key that only covers the new-signed-with-old self-issued certificate. The end entity's certificate has been revoked.

Procedure: Validate Invalid Basic Self-Issued New With Old Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.40 using the default settings.

Expected Result: The path should not validate successfully as the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key Self-Issued Cert CRL
- Basic Self-Issued Old Key NewWithOld CA Cert, Basic Self-Issued Old Key CA CRL
- Invalid Basic Self-Issued New With Old Test5 EE

4.5.6 Valid Basic Self-Issued CRL Signing Key Test6

In this test, the intermediate CA maintains two key pairs, one for signing certificates and the other for signing CRLs. The Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's certificate verification public key, and the intermediate CA has issued a self-issued certificate that contains its CRL verification key. The intermediate CA's certificate signing private key has been used to sign a CRL that only covers the self-issued certificate.

Procedure: Validate Valid Basic Self-Issued CRL Signing Key Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.41 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert CRL
- Basic Self-Issued CRL Signing Key CRL Cert, Basic Self-Issued CRL Signing Key CA CRL
- Valid Basic Self-Issued CRL Signing Key Test6 EE

4.5.7 Invalid Basic Self-Issued CRL Signing Key Test7

In this test, the intermediate CA maintains two key pairs, one for signing certificates and the other for signing CRLs. The Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's certificate verification public key, and the intermediate CA has issued a self-issued certificate that contains its CRL verification key. The intermediate CA's certificate signing private key has been used to sign a CRL that only covers the self-issued certificate. The end entity's certificate has been revoked.

Procedure: Validate Invalid Basic Self-Issued CRL Signing Key Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.42 using the default settings.

Expected Result: The path should not validate successfully since the end entity's certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert CRL
- Basic Self-Issued CRL Signing Key CRL Cert, Basic Self-Issued CRL Signing Key CA CRL
- Invalid Basic Self-Issued CRL Signing Key Test7 EE

4.5.8 Invalid Basic Self-Issued CRL Signing Key Test8

In this test, the intermediate CA maintains two key pairs, one for signing certificates and the other for signing CRLs. The Trust Anchor CA has issued a certificate to the intermediate CA that contains the intermediate CA's certificate verification public key, and the intermediate CA has issued a self-issued certificate that contains its CRL verification key. The intermediate CA's certificate signing private key has been used to sign a CRL that only covers the self-issued

certificate. The end entity's certificate was signed using the CRL signing key.

Procedure: Validate Invalid Basic Self-Issued CRL Signing Key Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.43 using the default settings.

Expected Result: The path should not validate successfully since the certificate that contains the public key needed to verify the end entity's certificate is not an intermediate certificate. The certificate does not have a **basicConstraints** extension and the **keyUsage** extension only asserts **cRLSign**.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert CRL
- Basic Self-Issued CRL Signing Key CRL Cert, Basic Self-Issued CRL Signing Key CA CRL
- Invalid Basic Self-Issued CRL Signing Key Test8 EE

4.6 Verifying Basic Constraints

The tests in this section can be used to determine if an application properly processes the **basicConstraints** extension as specified in X.509:

> [X.509 8.4.2.1] If [the **basicConstraints**] extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then:
>
> — if the value of **cA** is not set to true then the certified public key shall not be used to verify a certificate signature;
>
> — if the value of **cA** is set to true and **pathLenConstraint** is present then the certificate-using system shall check that the certification path being processed is consistent with the value of **pathLenConstraint**.
>
> NOTE 1 — If this 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.

4.6.1 Invalid Missing basicConstraints Test1

In this test, the intermediate certificate does not have a **basicConstraints** extension.

Procedure: Validate Invalid Missing basicConstraints Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.44 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate does not have a **basicConstraints** extension.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Missing basicConstraints CA Cert, Missing basicConstraints CA CRL
- Invalid Missing basicConstraints Test1 EE

4.6.2 Invalid cA False Test2

In this test, the **basicConstraints** extension is present in the intermediate certificate and is marked critical, but the **cA** component is false, indicating that the subject public key may not be used to verify signatures on certificates.

Procedure: Validate Invalid cA False Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.45 using the default settings.

Expected Result: The path should not validate successfully since the **basicConstraints** extension in the intermediate certificate indicates that the subject public key in that certificate may not be used to verify signatures on certificates.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- basicConstraints Critical cA False CA Cert, basicConstraints Critical cA False CA CRL
- Invalid cA False Test2 EE

4.6.3 Invalid cA False Test3

In this test, the **basicConstraints** extension is present in the intermediate certificate and is marked not critical, but the **cA** component is false, indicating that the subject public key may not be used to verify signatures on certificates. As specified in section 8.4.2.1 of X.509, the application must reject the path either because the application does not recognize the **basicConstraints** extension or because **cA** is set to false.

Procedure: Validate Invalid cA False Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.46 using the default settings.

Expected Result: The path should not validate successfully since the **basicConstraints** extension in the intermediate certificate indicates that the subject public key in that certificate may not be used to verify signatures on certificates.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- basicConstraints Not Critical cA False CA Cert, basicConstraints Not Critical cA False CA CRL
- Invalid cA False Test3 EE

4.6.4 Valid basicConstraints Not Critical Test4

In this test, the **basicConstraints** extension is present in the intermediate certificate and the **cA** component is true, but the extension is marked not critical.

Procedure: Validate Valid basicConstraints Not Critical Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.47 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- basicConstraints Not Critical CA Cert, basicConstraints Not Critical CA CRL
- Valid basicConstraints Not Critical Test4 EE

4.6.5 Invalid pathLenConstraint Test5

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional intermediate certificates in the path). This is followed by a second intermediate certificate and a end entity certificate.

Procedure: Validate Invalid pathLenConstraint Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.48 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the first certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- pathLenConstraint0 subCA Cert, pathLenConstraint0 subCA CRL
- Invalid pathLenConstraint Test5 EE

4.6.6 Invalid pathLenConstraint Test6

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional intermediate certificates in the path). This is followed by two more CA certificates, the second of which is the end certificate in the path.

Procedure: Validate Invalid pathLenConstraint Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.49 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the first certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- pathLenConstraint0 subCA Cert, pathLenConstraint0 subCA CRL
- Invalid pathLenConstraint Test6 EE

4.6.7 Valid pathLenConstraint Test7

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional intermediate certificates in the path). This is followed by the end entity certificate.

Procedure: Validate Valid pathLenConstraint Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.50 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- Valid pathLenConstraint Test7 EE

4.6.8 Valid pathLenConstraint Test8

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional intermediate certificates in the path). This is followed by the end entity certificate, which is a CA certificate.

Procedure: Validate Valid pathLenConstraint Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.51 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- Valid pathLenConstraint Test8 EE

4.6.9 Invalid pathLenConstraint Test9

This test consists of a certification path of length 4. The first certificate in the path includes a **pathLenConstraint** of 6, the second a **pathLenConstraint** of 0, and the third a **pathLenConstraint** of 0. The fourth certificate is an end entity certificate.

Procedure: Validate Invalid pathLenConstraint Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.52 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the second certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA0 Cert, pathLenConstraint6 subCA0 CRL
- pathLenConstraint6 subsubCA00 Cert, pathLenConstraint6 subsubCA00 CRL
- Invalid pathLenConstraint Test9 EE

4.6.10 Invalid pathLenConstraint Test10

This test consists of a certification path of length 4. The first certificate in the path includes a **pathLenConstraint** of 6, the second a **pathLenConstraint** of 0, and the third a **pathLenConstraint** of 0. The end entity certificate is a CA certificate.

Procedure: Validate Invalid pathLenConstraint Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.53 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the second certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA0 Cert, pathLenConstraint6 subCA0 CRL
- pathLenConstraint6 subsubCA00 Cert, pathLenConstraint6 subsubCA00 CRL
- Invalid pathLenConstraint Test10 EE

4.6.11 Invalid pathLenConstraint Test11

This test consists of a certification path of length 5. The first certificate in the path includes a **pathLenConstraint** of 6, the second a **pathLenConstraint** of 1, and the third a **pathLenConstraint** of 1. The fourth certificate does not include a **pathLenConstraint**. The fifth certificate is an end entity certificate.

Procedure: Validate Invalid pathLenConstraint Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.54 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the second certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA1 Cert, pathLenConstraint6 subCA1 CRL
- pathLenConstraint6 subsubCA11 Cert, pathLenConstraint6 subsubCA11 CRL
- pathLenConstraint6 subsubsubCA11X Cert, pathLenConstraint6 subsubsubCA11X CRL
- Invalid pathLenConstraint Test11 EE

4.6.12 Invalid pathLenConstraint Test12

This test consists of a certification path of length 5. The first certificate in the path includes a **pathLenConstraint** of 6, the second a **pathLenConstraint** of 1, and the third a **pathLenConstraint** of 1. The fourth certificate does not include a **pathLenConstraint**. The end entity certificate is a CA certificate.

Procedure: Validate Invalid pathLenConstraint Test12 EE using the default settings or open and verify Signed Test Message 6.2.2.55 using the default settings.

Expected Result: The path should not validate successfully as the length of the path violates the **pathLenConstraint** in the second certificate in the path.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA1 Cert, pathLenConstraint6 subCA1 CRL
- pathLenConstraint6 subsubCA11 Cert, pathLenConstraint6 subsubCA11 CRL
- pathLenConstraint6 subsubsubCA11X Cert, pathLenConstraint6 subsubsubCA11X CRL
- Invalid pathLenConstraint Test12 EE

4.6.13 Valid pathLenConstraint Test13

This test consists of a certification path of length 5. The first certificate in the path includes a

pathLenConstraint of 6, the second a **pathLenConstraint** of 4, and the third a **pathLenConstraint** of 1. The fourth certificate does not include a **pathLenConstraint**. The fifth certificate is an end entity certificate.

Procedure: Validate Valid pathLenConstraint Test13 EE using the default settings or open and verify Signed Test Message 6.2.2.56 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA4 Cert, pathLenConstraint6 subCA4 CRL
- pathLenConstraint6 subsubCA41 Cert, pathLenConstraint6 subsubCA41 CRL
- pathLenConstraint6 subsubsubCA41X Cert, pathLenConstraint6 subsubsubCA41X CRL
- Valid pathLenConstraint Test13 EE

4.6.14 Valid pathLenConstraint Test14

This test consists of a certification path of length 5. The first certificate in the path includes a **pathLenConstraint** of 6, the second a **pathLenConstraint** of 4, and the third a **pathLenConstraint** of 1. The fourth certificate does not include a **pathLenConstraint**. The end entity certificate is a CA certificate.

Procedure: Validate Valid pathLenConstraint Test14 EE using the default settings or open and verify Signed Test Message 6.2.2.57 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint6 CA Cert, pathLenConstraint6 CA CRL
- pathLenConstraint6 subCA4 Cert, pathLenConstraint6 subCA4 CRL
- pathLenConstraint6 subsubCA41 Cert, pathLenConstraint6 subsubCA41 CRL
- pathLenConstraint6 subsubsubCA41X Cert, pathLenConstraint6 subsubsubCA41X CRL
- Valid pathLenConstraint Test14 EE

4.6.15 Valid Self-Issued pathLenConstraint Test15

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional non-self-issued intermediate certificates in the path). This is followed by a self-issued certificate and the end entity certificate.

Procedure: Validate Valid Self-Issued pathLenConstraint Test15 EE using the default settings or open and verify Signed Test Message 6.2.2.58 using the default settings.

Expected Result: The path should validate successfully since the only intermediate certificate following the certificate that imposes the path length constraint is self-issued and self-issued certificates do not count when determining whether a path length constraint has been violated.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- pathLenConstraint0 Self-Issued CA Cert
- Valid Self-Issued pathLenConstraint Test15 EE

4.6.16 Invalid Self-Issued pathLenConstraint Test16

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 0 (allowing 0 additional non-self-issued intermediate certificates in the path). This is followed by a self-issued certificate, an non-self-issued certificate, and the end entity certificate.

Procedure: Validate Invalid Self-Issued pathLenConstraint Test16 EE using the default settings or open and verify Signed Test Message 6.2.2.59 using the default settings.

Expected Result: The path should not validate successfully since the first certificate imposes a path length constraint of 0 and this certificate is followed by a non-self-issued intermediate certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- pathLenConstraint0 CA Cert, pathLenConstraint0 CA CRL
- pathLenConstraint0 Self-Issued CA Cert
- pathLenConstraint0 subCA2 Cert, pathLenConstraint0 subCA2 CRL
- Invalid Self-Issued pathLenConstraint Test16 EE

4.6.17 Valid Self-Issued pathLenConstraint Test17

In this test, the first certificate in the path includes a **basicConstraints** extension with a **pathLenConstraint** of 1 (allowing 1 additional non-self-issued intermediate certificate in the path). This is followed by a self-issued certificate, a non-self-issued certificate, another self-issued certificate, and the end entity certificate.

Procedure: Validate Valid Self-Issued pathLenConstraint Test17 EE using the default settings or open and verify Signed Test Message 6.2.2.60 using the default settings.

Expected Result: The path should validate successfully since the first certificate imposes a path length constraint of 1 and this certificate is followed by only 1 non-self-issued intermediate certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- pathLenConstraint1 CA Cert, pathLenConstraint1 CA CRL
- pathLenConstraint1 Self-Issued CA Cert
- pathLenConstraint1 subCA Cert, pathLenConstraint1 subCA CRL
- pathLenConstraint1 Self-Issued subCA Cert
- Valid Self-Issued pathLenConstraint Test17 EE

4.7 Key Usage

The tests in this section can be used to determine whether an application properly processes the **keyUsage** extension in a certificate when the subject public key in that certificate is to be used to verify signatures on either certificates or CRLs.

4.7.1 Invalid keyUsage Critical keyCertSign False Test1

In this test, the intermediate certificate includes a critical **keyUsage** extension in which **keyCertSign** is false.

Procedure: Validate Invalid keyUsage Critical keyCertSign False Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.61 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a **keyUsage** extension which specifies that the subject public key may not be used to verify signatures on certificates.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- keyUsage Critical keyCertSign False CA Cert, keyUsage Critical keyCertSign False CA CRL
- Invalid keyUsage Critical keyCertSign False Test1 EE

4.7.2 Invalid keyUsage Not Critical keyCertSign False Test2

In this test, the intermediate certificate includes a non-critical **keyUsage** extension in which **keyCertSign** is false.

Procedure: Validate Invalid keyUsage Not Critical keyCertSign False Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.62 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a **keyUsage** extension which specifies that the subject public key may not be used to verify signatures on certificates.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- keyUsage Not Critical keyCertSign False CA Cert, keyUsage Not Critical keyCertSign False CA CRL
- Invalid keyUsage Not Critical keyCertSign False Test2 EE

4.7.3 Valid keyUsage Not Critical Test3

In this test, the intermediate certificate includes a non-critical **keyUsage** extension.

Procedure: Validate Valid keyUsage Not Critical Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.63 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- keyUsage Not Critical CA Cert, keyUsage Not Critical CA CRL
- Valid keyUsage Not Critical Test3 EE

4.7.4 Invalid keyUsage Critical cRLSign False Test4

In this test, the intermediate certificate includes a critical **keyUsage** extension in which **cRLSign** is false.

Procedure: Validate Invalid keyUsage Critical cRLSign False Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.64 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a **keyUsage** extension which specifies that the subject public key may not be used to verify signatures on CRLs. This prevents validation of the CRL needed to determine the status of the end entity certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- keyUsage Critical cRLSign False CA Cert, keyUsage Critical cRLSign False CA CRL
- Invalid keyUsage Critical cRLSign False Test4 EE

4.7.5 Invalid keyUsage Not Critical cRLSign False Test5

In this test, the intermediate certificate includes a non-critical **keyUsage** extension in which **cRLSign** is false.

Procedure: Validate Invalid keyUsage Not Critical cRLSign False Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.65 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a **keyUsage** extension which specifies that the subject public key may not be used to verify signatures on CRLs. This prevents validation of the CRL needed to determine the status of the end entity certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- keyUsage Not Critical cRLSign False CA Cert, keyUsage Not Critical cRLSign False CA CRL
- Invalid keyUsage Not Critical cRLSign False Test5 EE

4.8 Certificate Policies

The tests in this section are designed to verify an application's ability to process the **certificatePolicies** extension, including the ability to process policy qualifiers and the special policy OID **anyPolicy**.

In each of the tests, the "Expected Result" indicates the results of path validation (e.g., the values of the *explicit-policy-indicator*, *authorities-constrained-policy-set*, and *user-constrained-policy-set* and whether path validation should fail or succeed) as a function of the inputs[4]. All of the tests in this section should validate successfully if the *explicit-policy-indicator* is not set during path validation. In many of the tests, however, in order to simplify testing, one of the certificates in the path includes a non-critical **policyConstraints** extension in which **requireExplicitPolicy** is present with a **SkipCerts** value of 0. With this, many of the tests in this section can be run using the default settings in applications that can process the **policyConstraints** extension, and the tester can determine whether the application processed the path correctly by simply checking whether path validation succeeded or failed. For those tests in which the path includes a certificate with a **policyConstraints** extension, applications that can not process the **policyConstraints** extension can achieve the same results by setting *initial-explicit-policy* to true. If the application can not process the **policyConstraints** extension and it is not possible to set *initial-explicit-policy* to true, then it will be necessary to look at the value of *user-constrained-policy-set* that is output by the path validation code to determine if the path was processed correctly.

If the application can not process the **policyConstraints** extension, and it is not possible to set *initial-explicit-policy*, and it is not possible to examine the value of the *user-constrained-policy-set*, then it will not be possible to determine whether the application can process the **certificatePolicies** extension correctly. One may, however, still run the tests in this section in which no certificate in the path includes a **policyConstraints** extension and the value of *initial-explicit-policy* is false.

Many of the tests in this section suggest that the path be validated using inputs other than the default settings. As a general rule, each of the tests should be run using each of the suggested input settings unless the application can not be configured as specified. Where it is suggested that a path be validated with *initial-explicit-policy* set to true, these sub-tests may be skipped when testing applications that do not allow *initial-explicit-policy* to be set to true. These sub-tests are only present to determine if applications that allow *initial-explicit-policy* to be set produce the correct results when this input has been set.

If it is not possible to set the *initial-policy-set* to a value other than *any-policy*, then the sub-tests in which *initial-policy-set* is set to a different value may be skipped. However, in this case, it will be necessary, when running the corresponding sub-tests in which *initial-policy-set* is set to *any-policy*, to examine the *user-constrained-policy-set* to determine that it has been calculated correctly. If the *initial-policy-set* can be set, then the proper calculation of the *user-constrained-policy-set* may be inferred if path validation succeeds or fails as indicated for each of the sub-tests in which the *initial-policy-set* is other than *any-policy*.

---

[4] In RFC 3280, explicit_policy will be 0 if *explicit-policy-indicator* is set. The *user-constrained-policy-set* may be computed from the valid_policy_tree as follows. If the valid_policy_tree includes a leaf node with a valid_policy of **anyPolicy**, then the *user-constrained-policy-set* is *any-policy*. Otherwise, the *user-constrained-policy-set* consists of the set containing the valid_policy from each node in the valid_policy_tree in which the valid_policy is not **anyPolicy** and the valid_policy of that node's parent is **anyPolicy**. The *authorities-constrained-policy-set* may be computed using the same procedure on the valid_policy_tree before its intersection with the user-initial-policy-set has been computed (in step g of section 6.1.5).

The final six tests in this section deal with policy qualifiers. Since all of the **certificatePolicies** extensions in these tests are marked non-critical, the policy qualifiers may be ignored by applications that are unable to process them. Applications that can not process policy qualifiers should be able to process the certification paths in the policy qualifier tests by processing the **certificatePolicies** extension the same as if they did not include qualifiers. If certification path processing library code is being tested, and the library processes policy qualifiers, then it will be necessary to look at the *authorities-constrained-policy-set* and/or *user-constrained-policy-set* to determine that the correct qualifiers have been associated with each of the policies in the set.

4.8.1 All Certificates Same Policy Test1

In this test, every certificate in the path asserts the same policy, NIST-test-policy-1. The certification path in this test is the same certification path as in Valid Signatures Test1. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-explicit-policy* set. The path should validate successfully.
2. default settings, but with *initial-explicit-policy* set and *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
3. default settings, but with *initial-explicit-policy* set and *initial-policy-set* = {NIST-test-policy-2}. The path should not validate successfully.
4. default settings, but with *initial-explicit-policy* set and *initial-policy-set* = {NIST-test-policy-1, NIST-test-policy-2}. The path should validate successfully.

Procedure: Validate Valid Certificate Path Test1 EE or open and verify Signed Test Message 6.2.2.66 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Valid Certificate Path Test1 EE

4.8.2 All Certificates No Policies Test2

In this test, the **certificatePolicies** extension is omitted from every certificate in the path. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-explicit-policy* set . The path should not validate

successfully.

Procedure: Validate All Certificates No Policies Test2 EE or open and verify Signed Test Message 6.2.2.67.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is not set then the path should validate successfully. If the *initial-explicit-policy* indicator is set, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- No Policies CA Cert, No Policies CA CRL
- All Certificates No Policies Test2 EE

4.8.3 Different Policies Test3

In this test, every certificate in the path asserts the same certificate policy except the first certificate in the path. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-explicit-policy* set . The path should not validate successfully.
3. default settings, but with *initial-explicit-policy* set and *initial-policy-set* = {NIST-test-policy-1, NIST-test-policy-2}. The path should not validate successfully.

Procedure: Validate Different Policies Test3 EE or open and verify Signed Test Message 6.2.2.68.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is not set then the path should validate successfully. If the *initial-explicit-policy* indicator is set, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Policies P2 subCA Cert, Policies P2 subCA CRL
- Different Policies Test3 EE

4.8.4 Different Policies Test4

In this test, every certificate in the path asserts the same certificate policy except the end entity certificate.

Procedure: Validate Different Policies Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.69 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the

application can process the **policyConstraints** extension then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Good subCA Cert, Good subCA CRL
- Different Policies Test4 EE

4.8.5 Different Policies Test5

In this test, every certificate in the path except the second certificate asserts the same policy.

Procedure: Validate Different Policies Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.70 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the application can process the **policyConstraints** extension then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Policies P2 subCA2 Cert, Policies P2 subCA2 CRL
- Different Policies Test5 EE

4.8.6 Overlapping Policies Test6

The following path is such that the intersection of certificate policies among all the certificates has exactly one policy, NIST-test-policy-1. The final certificate in the path is a CA certificate. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
3. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should not validate successfully.

Procedure: Validate Overlapping Policies Test6 EE or open and verify Signed Test Message 6.2.2.71.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1}. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-*

constrained-policy-set will be empty. If the *explicit-policy-indicator* is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P1234 CA Cert, Policies P1234 CA CRL
- Policies P1234 subCAP123 Cert, Policies P1234 subCAP123 CRL
- Policies P1234 subsubCAP123P12 Cert, Policies P1234 subsubCAP123P12 CRL
- Overlapping Policies Test6 EE

4.8.7 Different Policies Test7

The following path is such that the intersection of certificate policies among all the certificates is empty. The final certificate in the path is a CA certificate.

Procedure: Validate Different Policies Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.72 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. If the *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the application can process the **policyConstraints** extension, then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P123 CA Cert, Policies P123 CA CRL
- Policies P123 subCAP12 Cert, Policies P123 subCAP12 CRL
- Policies P123 subsubCAP12P1 Cert, Policies P123 subsubCAP12P1 CRL
- Different Policies Test7 EE

4.8.8 Different Policies Test8

The following path is such that the intersection of certificate policies among all the certificates is empty. The final certificate in the path is a CA certificate.

Procedure: Validate Different Policies Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.73 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the application can process the **policyConstraints** extension then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- Policies P12 CA Cert, Policies P12 CA CRL
- Policies P12 subCAP1 Cert, Policies P12 subCAP1 CRL
- Policies P12 subsubCAP1P2 Cert, Policies P12 subsubCAP1P2 CRL
- Different Policies Test8 EE

4.8.9 Different Policies Test9

The following path is such that the intersection of certificate policies among all the certificates is empty.

Procedure: Validate Different Policies Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.74 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the application can process the **policyConstraints** extension, then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P123 CA Cert, Policies P123 CA CRL
- Policies P123 subCAP12 Cert, Policies P123 subCAP12 CRL
- Policies P123 subsubCAP12P2 Cert, Policies P123 subsubCAP2P2 CRL
- Policies P123 subsubsubCAP12P2P1 Cert, Policies P123 subsubsubCAP12P2P1 CRL
- Different Policies Test9 EE

4.8.10 All Certificates Same Policies Test10

In this test, every certificate in the path asserts the same policies, NIST-test-policy-1 and NIST-test-policy-2. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
3. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should validate successfully.

Procedure: Validate All Certificates Same Policies Test10 EE or open and verify Signed Test Message 6.2.2.75 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1, NIST-test-policy-2}. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the *initial-policy-set* is *any-policy* or otherwise includes either NIST-test-policy-1 or NIST-test-policy-2, then the *user-constrained-policy-set* will not be empty. If not, the *user-constrained-policy-set* will be empty. If the *explicit-policy-indicator* is set and the *initial-policy-set*

does not include either NIST-test-policy-1 or NIST-test-policy-2, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P12 CA Cert, Policies P12 CA CRL
- All Certificates Same Policies Test10 EE

4.8.11 All Certificates AnyPolicy Test11

In this test, every certificate in the path asserts the special policy **anyPolicy**. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.

Procedure: Validate All Certificates anyPolicy Test11 EE or open and verify Signed Test Message 6.2.2.76 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be *any-policy*, the *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension, and the *user-constrained-policy-set* will be the same as the *initial-policy-set*. The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- anyPolicy CA Cert, anyPolicy CA CRL
- All Certificates anyPolicy Test11 EE

4.8.12 Different Policies Test12

In this test, the path consists of two certificates, each of which asserts a different certificate policy.

Procedure: Validate Different Policies Test12 EE using the default settings or open and verify Signed Test Message 6.2.2.77 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the application can process the **policyConstraints** extension, then the path should not validate successfully. If the application can not process the **policyConstraints** extension, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P3 CA Cert, Policies P3 CA CRL
- Different Policies Test12 EE

4.8.13 All Certificates Same Policies Test13

In this test, every certificate in the path asserts the same policies, NIST-test-policy-1, NIST-test-policy-2, and NIST-test-policy-3. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should validate successfully.
3. default settings, but with *initial-policy-set* = {NIST-test-policy-3}. The path should validate successfully.

Procedure: Validate All Certificates Same Policies Test13 EE or open and verify Signed Test Message 6.2.2.78 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1, NIST-test-policy-2, NIST-test-policy-3}. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the *initial-policy-set* is *any-policy* or otherwise includes either NIST-test-policy-1, NIST-test-policy-2, or NIST-test-policy-3, then the *user-constrained-policy-set* will not be empty. If not, the *user-constrained-policy-set* will be empty. If the *explicit-policy-indicator* is set and the *initial-policy-set* does not include either NIST-test-policy-1, NIST-test-policy-2, or NIST-test-policy-3, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P123 CA Cert, Policies P123 CA CRL
- All Certificates Same Policies Test13 EE

4.8.14 AnyPolicy Test14

In this test, the intermediate certificate asserts **anyPolicy** and the end entity certificate asserts NIST-test-policy-1. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should not validate successfully.

Procedure: Validate AnyPolicy Test14 EE or open and verify Signed Test Message 6.2.2.79 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1}. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-*

constrained-policy-set will be empty. If the *explicit-policy-indicator* is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- anyPolicy CA Cert, anyPolicy CA CRL
- AnyPolicy Test14 EE

4.8.15 User Notice Qualifier Test15

In this test, the path consists of a single certificate. The certificate asserts the policy NIST-test-policy-1 and includes a user notice policy qualifier.

Procedure: Validate User Notice Qualifier Test15 EE using the default settings or open and verify Signed Test Message 6.2.2.80 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully. If the path validates successfully, then the application should display the user notice.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- User Notice Qualifier Test15 EE

4.8.16 User Notice Qualifier Test16

In this test, the path consists of an intermediate certificate and an end entity certificate. The intermediate certificate asserts the policy NIST-test-policy-1. The end entity certificate asserts both NIST-test-policy-1 and NIST-test-policy-2. Each policy in the end entity certificate has a different user notice qualifier associated with it.

Procedure: Validate User Notice Qualifier Test16 EE using the default settings or open and verify Signed Test Message 6.2.2.81 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully. If

the path validates successfully, then the application should display the user notice associated with NIST-test-policy-1. The user notice associated with NIST-test-policy-2 should not be displayed.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- User Notice Qualifier Test16 EE

4.8.17 User Notice Qualifier Test17

In this test, the path consists of an intermediate certificate and an end entity certificate. The intermediate certificate asserts the policy NIST-test-policy-1. The end entity certificate asserts **anyPolicy**. There is a user notice policy qualifier associated with **anyPolicy** in the end entity certificate.

Procedure: Validate User Notice Qualifier Test17 EE using the default settings or open and verify Signed Test Message 6.2.2.82 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully. If the path validates successfully, then the application should display the user notice associated with **anyPolicy**.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- User Notice Qualifier Test17 EE

4.8.18 User Notice Qualifier Test18

In this test, the intermediate certificate asserts policies NIST-test-policy-1 and NIST-test-policy-2. The end certificate asserts NIST-test-policy-1 and **anyPolicy**. Each of the policies in the end entity certificate asserts a different user notice policy qualifier. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully and the qualifier associated with NIST-test-policy-1 in the end entity certificate should be displayed.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should validate successfully and the qualifier associated with **anyPolicy** in the end entity certificate should be displayed.

Procedure: Validate User Notice Qualifier Test18 EE or open and verify Signed Test Message 6.2.2.83 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1, NIST-test-policy-2}. The *explicit-policy-indicator* will be set if the application can process the **policyConstraints** extension. If the *initial-policy-set* is *any-policy* or otherwise includes either NIST-test-policy-1 or NIST-test-policy-2, then the *user-constrained-policy-set* will not be empty. If not, the *user-constrained-policy-set* will be empty. If the *explicit-policy-indicator* is set and the *initial-policy-set* does not include either NIST-test-policy-1 or NIST-test-policy-2, then the path should be rejected, otherwise it should validate successfully. If NIST-test-policy-1 is in the *user-constrained-policy-set*, then the user notice associated with that policy in the end entity certificate should be displayed. If NIST-test-policy-2 is in the *user-constrained-policy-set*, then the user notice associated with **anyPolicy** in the end entity certificate should be displayed.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Policies P12 CA Cert, Policies P12 CA CRL
- User Notice Qualifier Test18 EE

4.8.19 User Notice Qualifier Test19

In this test, the path consists of a single certificate. The certificate asserts the policy NIST-test-policy-1 and includes a user notice policy qualifier. The user notice qualifier contains explicit text that is longer than 200 bytes.

> [RFC 3280 4.2.1.5] Note: While the explicitText has a maximum size of 200 characters, some non-conforming CAs exceed this limit. Therefore, certificate users SHOULD gracefully handle explicitText with more than 200 characters.

Procedure: Validate User Notice Qualifier Test19 EE using the default settings or open and verify Signed Test Message 6.2.2.84 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully. Since the **explicitText** exceeds the maximum size of 200 characters, the application may choose to reject the certificate. If the application accepts the certificate, display of the user notice is optional.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- User Notice Qualifier Test19 EE

4.8.20 CPS Pointer Qualifier Test20

In this test, the path consists of an intermediate certificate and an end entity certificate, both of which assert the policy NIST-test-policy-1. There is a CPS pointer policy qualifier associated with NIST-test-policy-1 in the end entity certificate.

Procedure: Validate CPS Pointer Qualifier Test20 EE using the default settings or open and verify Signed Test Message 6.2.2.85 using the default settings. (If possible, it is recommended that this test be run with the *initial-explicit-policy* indicator set. If this can not be done, manually check that the *authorities-constrained-policy-set* and *user-constrained-policy-set* are correct.)

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be the same as the *initial-explicit-policy* indicator. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-explicit-policy* indicator is set and the *initial-policy-set* does not include NIST-test-policy-1, then the path should be rejected, otherwise it should validate successfully. The CPS pointer in the qualifier should be associated with NIST-test-policy-1 in the *authorities-constrained-policy-set* (and in the *user-constrained-policy-set* if NIST-test-policy-1 is in that set). There are no processing requirements associated with the CPS pointer qualifier.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- CPS Pointer Qualifier Test20 EE

4.9 Require Explicit Policy

The tests in this section can be used to determine if an application can process the **requireExplicitPolicy** field of the **policyConstraints** extension. In most of these tests, at least one certificate in the path does not include a **certificatePolicies** extension so that the *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty. In these tests, the path will validate successfully if the *explicit-policy-indicator* is not set by path validation and the path will not validate successfully if the *explicit-policy-indicator* is set. So, in order to run these tests, it is important that *initial-explicit-policy* be set to false.

4.9.1 Valid RequireExplicitPolicy Test1

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 10. This is followed by three more intermediate certificates and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Valid requireExplicitPolicy Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.86 using the default settings.

Expected Result: The path should validate successfully since the *explicit-policy-indicator* is not set.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy10 CA Cert, requireExplicitPolicy10 CA CRL
- requireExplicitPolicy10 subCA Cert, requireExplicitPolicy10 subCA CRL
- requireExplicitPolicy10 subsubCA Cert, requireExplicitPolicy10 subsubCA CRL
- requireExplicitPolicy10 subsubsubCA Cert, requireExplicitPolicy10 subsubsubCA CRL
- Valid requireExplicitPolicy Test1 EE

4.9.2 Valid RequireExplicitPolicy Test2

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 5. This is followed by three more intermediate certificates and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Valid requireExplicitPolicy Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.87 using the default settings.

Expected Result: The path should validate successfully since the *explicit-policy-indicator* is not set.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy5 CA Cert, requireExplicitPolicy5 CA CRL
- requireExplicitPolicy5 subCA Cert, requireExplicitPolicy5 subCA CRL
- requireExplicitPolicy5 subsubCA Cert, requireExplicitPolicy5 subsubCA CRL
- requireExplicitPolicy5 subsubsubCA Cert, requireExplicitPolicy5 subsubsubCA CRL
- Valid requireExplicitPolicy Test2 EE

4.9.3 Invalid RequireExplicitPolicy Test3

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 4. This is followed by three more intermediate certificates and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Invalid requireExplicitPolicy Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.88 using the default settings.

Expected Result: The path not should validate successfully since the *explicit-policy-indicator* is set and the *authorities-constrained-policy-set* is empty.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- requireExplicitPolicy4 CA Cert, requireExplicitPolicy4 CA CRL
- requireExplicitPolicy4 subCA Cert, requireExplicitPolicy4 subCA CRL
- requireExplicitPolicy4 subsubCA Cert, requireExplicitPolicy4 subsubCA CRL
- requireExplicitPolicy4 subsubsubCA Cert, requireExplicitPolicy4 subsubsubCA CRL
- Invalid requireExplicitPolicy Test3 EE

4.9.4 Valid RequireExplicitPolicy Test4

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 0. This is followed by three more intermediate certificates and an end entity certificate.

Procedure: Validate Valid requireExplicitPolicy Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.89 using the default settings.

Expected Result: The path should validate successfully (as long as the *initial-policy-set* is either *any-policy* or otherwise includes NIST-test-policy-1) since the *user-constrained-policy-set* is not empty.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy0 CA Cert, requireExplicitPolicy0 CA CRL
- requireExplicitPolicy0 subCA Cert, requireExplicitPolicy0 subCA CRL
- requireExplicitPolicy0 subsubCA Cert, requireExplicitPolicy0 subsubCA CRL
- requireExplicitPolicy0 subsubsubCA Cert, requireExplicitPolicy0 subsubsubCA CRL
- Valid requireExplicitPolicy Test4 EE

4.9.5 Invalid RequireExplicitPolicy Test5

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 7. The second certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 2. The third certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 4. This is followed by one more intermediate certificate and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Invalid requireExplicitPolicy Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.90 using the default settings.

Expected Result: The path should not validate successfully since the *explicit-policy-indicator* is set and the *authorities-constrained-policy-set* is empty.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy7 CA Cert, requireExplicitPolicy7 CA CRL
- requireExplicitPolicy7 subCARE2 Cert, requireExplicitPolicy7 subCARE2 CRL
- requireExplicitPolicy7 subsubCARE2RE4 Cert, requireExplicitPolicy7 subsubCARE2RE4 CRL
- requireExplicitPolicy7 subsubsubCARE2RE4 Cert, requireExplicitPolicy7

subsubsubCARE2RE4 CRL
- Invalid requireExplicitPolicy Test5 EE

4.9.6 Valid Self-Issued requireExplicitPolicy Test6

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 2. This is followed by a self-issued intermediate certificate and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Valid Self-Issued requireExplicitPolicy Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.91 using the default settings.

Expected Result: The path should validate successfully since the *explicit-policy-indicator* is not set.

Certification Path: The certification path is composed of the following objects:
- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 CA CRL
- requireExplicitPolicy2 Self-Issued CA Cert
- Valid Self-Issued requireExplicitPolicy Test6 EE

4.9.7 Invalid Self-Issued requireExplicitPolicy Test7

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 2. This is followed by a self-issued intermediate certificate, a non-self-issued intermediate certificate, and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Invalid Self-Issued requireExplicitPolicy Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.92 using the default settings.

Expected Result: The path should not validate successfully since the *explicit-policy-indicator* is set and the *authorities-constrained-policy-set* is empty.

Certification Path: The certification path is composed of the following objects:
- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 CA CRL
- requireExplicitPolicy2 Self-Issued CA Cert
- requireExplicitPolicy2 subCA Cert, requireExplicitPolicy2 subCA CRL
- Invalid Self-Issued requireExplicitPolicy Test7 EE

4.9.8 Invalid Self-Issued requireExplicitPolicy Test8

In this test, the first certificate in the path includes a **policyConstraints** extension with **requireExplicitPolicy** set to 2. This is followed by a self-issued intermediate certificate, a non-self-issued intermediate certificate, a self-issued intermediate certificate, and an end entity certificate. The end entity certificate does not include a **certificatePolicies** extension.

Procedure: Validate Invalid Self-Issued requireExplicitPolicy Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.93 using the default settings.

Expected Result: The path should not validate successfully since the *explicit-policy-indicator* is set and the *authorities-constrained-policy-set* is empty.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 CA CRL
- requireExplicitPolicy2 Self-Issued CA Cert
- requireExplicitPolicy2 subCA Cert, requireExplicitPolicy2 subCA CRL
- requireExplicitPolicy2 Self-Issued subCA Cert
- Invalid Self-Issued requireExplicitPolicy Test8 EE

4.10 Policy Mappings

The tests in this section are designed to verify an application's ability to process the **policyMappings** extension. Most of the tests in this section indicate that the path should be validated using the default settings. Where this is the case, it is important that *initial-policy-mapping-inhibit* be set to false. For those applications that are capable of setting *initial-policy-mapping-inhibit* to true, two sub-tests have been included that can be used to determine if the application processes paths correctly when *initial-policy-mapping-inhibit* is set to true.

Some of the tests also recommend validating paths using values of *initial-policy-set* other than *any-policy*. These tests are included to verify that applications compute the *user-constrained-policy-set* correctly in the face of policy mappings. If it is not possible to set the *initial-policy-set* to a value other than *any-policy*, then it will be necessary to examine the *user-constrained-policy-set* to verify that it is being computed correctly.

As with the certificate policies tests, many of the tests in this section include paths in which one of the certificates includes a non-critical **policyConstraints** extension with **requireExplicitPolicy** present with a **SkipCerts** value of 0. If the application can process the **policyConstraints** extension, then tests in which the *user-constrained-policy-set* is empty should simply fail (obviating the need to look at the *user-constrained-policy-set*). If the application can not process the **policyConstraints** extension, then *initial-explicit-policy* should be set whenever the path includes a certificate that includes the **policyConstraints** extension. If the application can not process the **policyConstraints** extension and *initial-explicit-policy* can not be set, then it will be necessary to check the *user-constrained-policy-set* in all cases to ensure that its value has been correctly computed.

4.10.1 Valid Policy Mapping Test1

In this test, the intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-2. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should not validate successfully.

3. default settings, but with *initial-policy-mapping-inhibit* set. The path should not validate successfully.

Procedure: Validate Valid Policy Mapping Test1 EE or open and verify Signed Test Message 6.2.2.94 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Mapping 1to2 CA Cert, Mapping 1to2 CA CRL
- Valid Policy Mapping Test1 EE

4.10.2 Invalid Policy Mapping Test2

In this test, the intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-1. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should not validate successfully.
2. default settings, but with *initial-policy-mapping-inhibit* set. The path should not validate successfully.

Procedure: Validate Invalid Policy Mapping Test2 EE or open and verify Signed Test Message 6.2.2.95.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Mapping 1to2 CA Cert, Mapping 1to2 CA CRL
- Invalid Policy Mapping Test2 EE

4.10.3 Valid Policy Mapping Test3

In this test, the path is valid under NIST-test-policy-2 as a result of policy mappings. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should not validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path

should validate successfully.

Procedure: Validate Valid Policy Mapping Test3 EE or open and verify Signed Test Message 6.2.2.96 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-2} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-2, then the *user-constrained-policy-set* will be {NIST-test-policy-2}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-2 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P12 Mapping 1to3 CA Cert, P12 Mapping 1to3 CA CRL
- P12 Mapping 1to3 subCA Cert, P12 Mapping 1to3 subCA CRL
- P12 Mapping 1to3 subsubCA Cert, P12 Mapping 1to3 subsubCA CRL
- Valid Policy Mapping Test3 EE

4.10.4 Invalid Policy Mapping Test4

In this test, the policy asserted in the end entity certificate is not in the *authorities-constrained-policy-set*.

Procedure: Validate Invalid Policy Mapping Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.97 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P12 Mapping 1to3 CA Cert, P12 Mapping 1to3 CA CRL
- P12 Mapping 1to3 subCA Cert, P12 Mapping 1to3 subCA CRL
- P12 Mapping 1to3 subsubCA Cert, P12 Mapping 1to3 subsubCA CRL
- Invalid Policy Mapping Test4 EE

4.10.5 Valid Policy Mapping Test5

In this test, the path is valid under NIST-test-policy-1 as a result of policy mappings. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-6}. The path should not validate successfully.

Procedure: Validate Valid Policy Mapping Test5 EE or open and verify Signed Test Message 6.2.2.98 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P1 Mapping 1to234 CA Cert, P1 Mapping 1to234 CA CRL
- P1 Mapping 1to234 subCA Cert, P1 Mapping 1to234 subCA CRL
- Valid Policy Mapping Test5 EE

4.10.6 Valid Policy Mapping Test6

In this test, the path is valid under NIST-test-policy-1 as a result of policy mappings. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-6}. The path should not validate successfully.

Procedure: Validate Valid Policy Mapping Test6 EE or open and verify Signed Test Message 6.2.2.99 using the settings specified above.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P1 Mapping 1to234 CA Cert, P1 Mapping 1to234 CA CRL
- P1 Mapping 1to234 subCA Cert, P1 Mapping 1to234 subCA CRL
- Valid Policy Mapping Test6 EE

4.10.7 Invalid Mapping From anyPolicy Test7

In this test, the intermediate certificate includes a **policyMappings** extension that includes a mapping in which the **issuerDomainPolicy** is **anyPolicy**. The intermediate certificate also includes a critical **policyConstraints** extension with **requireExplicitPolicy** set to 0.

[RFC 3280 6.1.4] (a) If a policy mapping extension is present, verify that the special value anyPolicy does not appear as an issuerDomainPolicy or a subjectDomainPolicy.

Procedure: Validate Invalid Mapping From anyPolicy Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.100 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a policy mapping extension in which **anyPolicy** appears as an **issuerDomainPolicy**.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Mapping From anyPolicy CA Cert, Mapping From anyPolicy CA CRL
- Invalid Mapping From anyPolicy Test7 EE

4.10.8 Invalid Mapping To anyPolicy Test8

In this test, the intermediate certificate includes a **policyMappings** extension that includes a mapping in which the **subjectDomainPolicy** is **anyPolicy**. The intermediate certificate also includes a critical **policyConstraints** extension with **requireExplicitPolicy** set to 0.

[RFC 3280 6.1.4] (a) If a policy mapping extension is present, verify that the special value anyPolicy does not appear as an issuerDomainPolicy or a subjectDomainPolicy.

Procedure: Validate Invalid Mapping To anyPolicy Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.101 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate includes a policy mapping extension in which **anyPolicy** appears as an **subjectDomainPolicy**.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Mapping To anyPolicy CA Cert, Mapping To anyPolicy CA CRL
- Invalid Mapping To anyPolicy Test8 EE

4.10.9 Valid Policy Mapping Test9

In this test, the intermediate certificate asserts **anyPolicy** and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Valid Policy Mapping Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.102 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- PanyPolicy Mapping 1to2 CA Cert, PanyPolicy Mapping 1to2 CA CRL
- Valid Policy Mapping Test9 EE

4.10.10 Invalid Policy Mapping Test10

In this test, the first intermediate certificate asserts NIST-test-policy-1. The second intermediate certificate asserts **anyPolicy** and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Invalid Policy Mapping Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.103 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Good subCA PanyPolicy Mapping 1to2 CA Cert, Good subCA PanyPolicy Mapping 1to2 CA CRL
- Invalid Policy Mapping Test10 EE

4.10.11 Valid Policy Mapping Test11

In this test, the first intermediate certificate asserts NIST-test-policy-1. The second intermediate certificate asserts **anyPolicy** and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Valid Policy Mapping Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.104 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1}

and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Good CA Cert, Good CA CRL
- Good subCA PanyPolicy Mapping 1to2 CA Cert, Good subCA PanyPolicy Mapping 1to2 CA CRL
- Valid Policy Mapping Test11 EE

4.10.12 Valid Policy Mapping Test12

In this test, the intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and maps NIST-test-policy-1 to NIST-test-policy-3. The end entity certificate asserts **anyPolicy** and NIST-test-policy-3, each with a different user notice policy qualifier. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings, but with *initial-policy-set* = {NIST-test-policy-1}. The path should validate successfully and the application should display the user notice associated with NIST-test-policy-3 in the end entity certificate.
2. default settings, but with *initial-policy-set* = {NIST-test-policy-2}. The path should validate successfully and the application should display the user notice associated with **anyPolicy** in the end entity certificate.

Procedure: Validate Valid Policy Mapping Test12 EE or open and verify Signed Test Message 6.2.2.105.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1, NIST-test-policy-2} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1 or NIST-test-policy-2, then the *user-constrained-policy-set* will be not be empty. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 or NIST-test-policy-2 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P12 Mapping 1to3 CA Cert, P12 Mapping 1to3 CA CRL
- Valid Policy Mapping Test12 EE

4.10.13 Valid Policy Mapping Test13

In this test, the intermediate certificate asserts NIST-test-policy-1 and **anyPolicy** and maps NIST-test-policy-1 to NIST-test-policy-2. There is a user notice policy qualifier associated with each of

the policies. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Valid Policy Mapping Test13 EE using the default settings or open and verify Signed Test Message 6.2.2.106 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully. If the path is accepted, the application should display the user notice associated with NIST-test-policy-1 in the intermediate certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P1anyPolicy Mapping 1to2 CA Cert, P1anyPolicy Mapping 1to2 CA CRL
- Valid Policy Mapping Test13 EE

4.10.14 Valid Policy Mapping Test14

In this test, the intermediate certificate asserts NIST-test-policy-1 and **anyPolicy** and maps NIST-test-policy-1 to NIST-test-policy-2. There is a user notice policy qualifier associated with each of the policies. The end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Valid Policy Mapping Test14 EE using the default settings or open and verify Signed Test Message 6.2.2.107 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}. If not, the *user-constrained-policy-set* will be empty. If the *initial-policy-set* does not include NIST-test-policy-1 (and the application can process the **policyConstraints** extension), then the path should be rejected, otherwise it should validate successfully. If the path is accepted, the application should display the user notice associated with **anyPolicy** in the intermediate certificate.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- P1anyPolicy Mapping 1to2 CA Cert, P1anyPolicy Mapping 1to2 CA CRL
- Valid Policy Mapping Test14 EE

4.11 Inhibit Policy Mapping

The tests in this section are designed to verify an application's ability to process the **inihibitPolicyMapping** field of the **policyConstraints** extension and to verify that policy mappings are processed correctly after policy mapping has been inhibited. In order to make each of the tests pass/fail, at least one certificate in the certification path of each of the tests includes a **policyConstraints** extension with **requireExplicitPolicy** policy present with **SkipCerts** set to 0. Since a prerequisite for running the tests in this section is the ability to process the **policyConstraints** extension, the extension is made critical.

Each of the tests in this section was designed to be run using the default settings. Since the *explicit-policy-indicator* is set in each of the tests, the value of *initial-explicit-policy* should not affect the results of the tests. However, the *initial-policy-mapping-inhibit* indicator must be set to false and *initial-inhibit-any-policy* must be set to false for any test in which one or more certificates in the path includes the **anyPolicy** OID.

It is believed that the proper processing of **inhibitPolicyMapping** may be determined by running each of these tests and determining whether each path is validated successfully or rejected as indicated. However, for those paths that validate successfully, it is recommended that the value of the *user-constrained-policy-set* be checked as well, if possible.

4.11.1 Invalid inhibitPolicyMapping Test1

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 0. The second intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-1 and NIST-test-policy-2.

Procedure: Validate Invalid inhibitPolicyMapping Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.108 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty. The *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping0 CA Cert, inhibitPolicyMapping0 CA CRL
- inhibitPolicyMapping0 subCA Cert, inhibitPolicyMapping0 subCA CRL
- Invalid inhibitPolicyMapping Test1 EE

4.11.2 Valid inhibitPolicyMapping Test2

In this test, the first intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and maps NIST-test-policy-1 to NIST-test-policy-3 and NIST-test-policy-2 to NIST-test-policy-4. The end entity certificate asserts NIST-test-policy-3.

Procedure: Validate Valid inhibitPolicyMapping Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.109 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 CA CRL
- inhibitPolicyMapping1 P12 subCA Cert, inhibitPolicyMapping1 P12 subCA CRL
- Valid inhibitPolicyMapping Test2 EE

4.11.3 Invalid inhibitPolicyMapping Test3

In this test, the first intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and maps NIST-test-policy-1 to NIST-test-policy-3 and NIST-test-policy-2 to NIST-test-policy-4. The third intermediate certificate asserts NIST-test-policy-3 and NIST-test-policy-4 and maps NIST-test-policy-3 to NIST-test-policy-5. The end entity certificate asserts NIST-test-policy-5.

Procedure: Validate Invalid inhibitPolicyMapping Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.110 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 CA CRL
- inhibitPolicyMapping1 P12 subCA Cert, inhibitPolicyMapping1 P12 subCA CRL
- inhibitPolicyMapping1 P12 subsubCA Cert, inhibitPolicyMapping1 P12 subsubCA CRL
- Invalid inhibitPolicyMapping Test3 EE

4.11.4 Valid inhibitPolicyMapping Test4

In this test, the first intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and maps NIST-test-policy-1 to NIST-test-policy-3 and NIST-test-policy-2 to NIST-test-policy-4. The third intermediate certificate asserts NIST-test-policy-3 and NIST-test-policy-4 and maps NIST-test-policy-3 to NIST-test-policy-5. The end entity certificate asserts NIST-test-policy-4.

Procedure: Validate Valid inhibitPolicyMapping Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.111 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-2} and the *explicit-policy-indicator* will be set. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-2, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 CA CRL
- inhibitPolicyMapping1 P12 subCA Cert, inhibitPolicyMapping1 P12 subCA CRL
- inhibitPolicyMapping1 P12 subsubCA Cert, inhibitPolicyMapping1 P12 subsubCA CRL
- Valid inhibitPolicyMapping Test4 EE

4.11.5 Invalid inhibitPolicyMapping Test5

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 5. The second intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The third intermediate certificate asserts NIST-test-policy-1. The fourth intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Invalid inhibitPolicyMapping Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.112 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping5 CA Cert, inhibitPolicyMapping5 CA CRL
- inhibitPolicyMapping5 subCA Cert, inhibitPolicyMapping5 subCA CRL
- inhibitPolicyMapping5 subsubCA Cert, inhibitPolicyMapping5 subsubCA CRL
- inhibitPolicyMapping5 subsubsubCA Cert, inhibitPolicyMapping5 subsubsubCA CRL
- Invalid inhibitPolicyMapping Test5 EE

4.11.6 Invalid inhibitPolicyMapping Test6

In this test, the first intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 5. The third intermediate certificate asserts NIST-test-policy-1 and NIST-test-policy-2 and maps NIST-test-policy-1 to NIST-test-policy-3. The end entity certificate asserts NIST-test-policy-3.

Procedure: Validate Invalid inhibitPolicyMapping Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.113 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 CA CRL
- inhibitPolicyMapping1 P12 subCAIPM5 Cert, inhibitPolicyMapping1 P12 subCAIPM5 CRL
- inhibitPolicyMapping1 P12 subsubCAIPM5 Cert, inhibitPolicyMapping1 P12 subsubCAIPM5 CRL
- Invalid inhibitPolicyMapping Test6 EE

4.11.7 Valid Self-Issued inhibitPolicyMapping Test7

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Valid Self-Issued inhibitPolicyMapping Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.114 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 CA CRL
- inhibitPolicyMapping1 P1 Self-Issued CA Cert
- inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subCA CRL
- Valid Self-Issued inhibitPolicyMapping Test7 EE

4.11.8 Invalid Self-Issued inhibitPolicyMapping Test8

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The fourth intermediate certificate asserts NIST-test-policy-2 and maps NIST-test-policy-2 to NIST-test-policy-3. The end entity certificate asserts NIST-test-policy-3.

Procedure: Validate Invalid Self-Issued inhibitPolicyMapping Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.115 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 CA CRL
- inhibitPolicyMapping1 P1 Self-Issued CA Cert
- inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subCA CRL
- inhibitPolicyMapping1 P1 subsubCA Cert, inhibitPolicyMapping1 P1 subsubCA CRL
- Invalid Self-Issued inhibitPolicyMapping Test8 EE

4.11.9 Invalid Self-Issued inhibitPolicyMapping Test9

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The fourth intermediate certificate asserts NIST-test-policy-2 and maps NIST-test-policy-2 to NIST-test-policy-3. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Invalid Self-Issued inhibitPolicyMapping Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.116 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 CA CRL
- inhibitPolicyMapping1 P1 Self-Issued CA Cert
- inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subCA CRL
- inhibitPolicyMapping1 P1 subsubCA Cert, inhibitPolicyMapping1 P1 subsubCA CRL
- Invalid Self-Issued inhibitPolicyMapping Test9 EE

4.11.10 Invalid Self-Issued inhibitPolicyMapping Test10

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The fourth intermediate certificate is a self-issued certificate that asserts NIST-test-policy-2 and maps NIST-test-policy-2 to NIST-test-policy-3. The end entity certificate asserts NIST-test-policy-3.

Procedure: Validate Invalid Self-Issued inhibitPolicyMapping Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.117 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 CA CRL
- inhibitPolicyMapping1 P1 Self-Issued CA Cert
- inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subCA CRL
- inhibitPolicyMapping1 P1 Self-Issued subCA Cert
- Invalid Self-Issued inhibitPolicyMapping Test10 EE

4.11.11 Invalid Self-Issued inhibitPolicyMapping Test11

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes a **policyConstraints** extension with **inhibitPolicyMapping** set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts NIST-test-policy-1 and maps NIST-test-policy-1 to NIST-test-policy-2. The fourth intermediate certificate is a self-issued certificate that asserts NIST-test-policy-2 and maps NIST-test-policy-2 to NIST-test-policy-3. The end entity certificate asserts NIST-test-policy-2.

Procedure: Validate Invalid Self-Issued inhibitPolicyMapping Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.118 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set. The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 CA CRL
- inhibitPolicyMapping1 P1 Self-Issued CA Cert
- inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subCA CRL
- inhibitPolicyMapping1 P1 Self-Issued subCA Cert
- Invalid Self-Issued inhibitPolicyMapping Test11 EE

4.12 Inhibit Any Policy

The tests in this section were designed to verify an application's ability to process the **inhibitAnyPolicy** extension and to process certificates (including self-issued certificates) that assert the **anyPolicy** OID once the use of **anyPolicy** has been inhibited. In order to make these tests pass/fail, at least one certificate in each of the certification paths for each of of the tests includes a non-critical **policyConstraints** extension with **requireExplicitPolicy** present with a **SkipCerts** value of 0. If the application being tested can not process the **policyConstraints** extension, then the same results may be achieved by setting *initial-explicit-policy* to true. If the application can not process the **policyConstraints** extension and it is not possible to set *initial-explicit-policy* to true, then the results of the test will need to be determined by examining the *user-constrained-policy-set*.

Each of the tests in this section was designed to be run using the default settings. Since the purpose of these tests is to determine if the application can process the **inhibitAnyPolicy** extension, *initial-inhibit-any-policy* must be set to false in order for the correct results to be obtained. In one or more of the tests in this section, it is recommend that the test also be run with *initial-inhibit-any-policy* set to true. These subtests were only included for completeness in testing applications that allow *initial-inhibit-any-policy* to be set to true. If the application does not allow for *initial-inhibit-any-policy* to be set to true, then these subtests may be skipped.

4.12.1 Invalid inhibitAnyPolicy Test1

In this test, the intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 0. The end entity certificate asserts **anyPolicy**.

Procedure: Validate Invalid inhibitAnyPolicy Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.119 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy0 CA Cert, inhibitAnyPolicy0 CA CRL
- Invalid inhibitAnyPolicy Test1 EE

4.12.2 Valid inhibitAnyPolicy Test2

In this test, the intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 0. The end entity certificate asserts **anyPolicy** and NIST-test-policy-1.

Procedure: Validate Valid inhibitAnyPolicy Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.120 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can

process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}and the path should validate successfully. If not, then the *user-constrained-policy-set* will be empty. If the *user-constrained-policy-set* is empty and the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy0 CA Cert, inhibitAnyPolicy0 CA CRL
- Valid inhibitAnyPolicy Test2 EE

4.12.3 inhibitAnyPolicy Test3

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate asserts **anyPolicy**. The end entity certificate asserts NIST-test-policy-1. If possible, it is recommended that the certification path in this test be validated using the following inputs:

1. default settings. The path should validate successfully.
2. default settings, but with *initial-inhibit-any-policy* set. The path should not validate successfully.

Procedure: Validate inhibitAnyPolicy Test3 EE or open and verify Signed Test Message 6.2.2.121.

Expected Result: The *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If *initial-inhibit-any-policy* is set, then the *authorities-constrained-policy-set* and the *user-constrained-policy-set* will be empty and the path should not validate successfully. Otherwise, the *authorities-constrained-policy-set* will be {NIST-test-policy-1}. If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}and the path should validate successfully. If not, then the *user-constrained-policy-set* will be empty. If the *user-constrained-policy-set* is empty and the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 subCA1 Cert, inhibitAnyPolicy1 subCA1 CRL
- inhibitAnyPolicy Test3 EE

4.12.4 Invalid inhibitAnyPolicy Test4

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate asserts **anyPolicy**. The end entity certificate asserts **anyPolicy**.

Procedure: Validate Invalid inhibitAnyPolicy Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.122 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 subCA1 Cert, inhibitAnyPolicy1 subCA1 CRL
- Invalid inhibitAnyPolicy Test4 EE

4.12.5 Invalid inhibitAnyPolicy Test5

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 5. The second intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The third intermediate certificate asserts NIST-test-policy-1 and the end entity certificate asserts **anyPolicy**.

Procedure: Validate Invalid inhibitAnyPolicy Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.123 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy5 CA Cert, inhibitAnyPolicy5 CA CRL
- inhibitAnyPolicy5 subCA Cert, inhibitAnyPolicy5 subCA CRL
- inhibitAnyPolicy5 subsubCA Cert, inhibitAnyPolicy5 subsubCA CRL
- Invalid inhibitAnyPolicy Test5 EE

4.12.6 Invalid inhibitAnyPolicy Test6

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 5. The end entity certificate asserts **anyPolicy**.

Procedure: Validate Invalid inhibitAnyPolicy Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.124 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the

application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 subCAIAP5 Cert, inhibitAnyPolicy1 subCAIAP5 CRL
- Invalid inhibitAnyPolicy Test6 EE

4.12.7 Valid Self-Issued inhibitAnyPolicy Test7

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts **anyPolicy** and the end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Valid Self-Issued inhibitAnyPolicy Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.125 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}and the path should validate successfully. If not, then the *user-constrained-policy-set* will be empty. If the *user-constrained-policy-set* is empty and the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 Self-Issued CA Cert
- inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 subCA2 CRL
- Valid Self-Issued inhibitAnyPolicy Test7 EE

4.12.8 Invalid Self-Issued inhibitAnyPolicy Test8

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third and fourth intermediate certificates assert **anyPolicy** and the end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Invalid Self-Issued inhibitAnyPolicy Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.126 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 Self-Issued CA Cert
- inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 subCA2 CRL
- inhibitAnyPolicy1 subsubCA2 Cert, inhibitAnyPolicy1 subsubCA2 CRL
- Invalid Self-Issued inhibitAnyPolicy Test8 EE

4.12.9 Valid Self-Issued inhibitAnyPolicy Test9

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts **anyPolicy**. The fourth intermediate certificate is a self-issued certificate that asserts **anyPolicy**. The end entity certificate asserts NIST-test-policy-1.

Procedure: Validate Valid Self-Issued inhibitAnyPolicy Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.127 using the default settings.

Expected Result: The *authorities-constrained-policy-set* will be {NIST-test-policy-1} and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the *initial-policy-set* is *any-policy* or otherwise includes NIST-test-policy-1, then the *user-constrained-policy-set* will be {NIST-test-policy-1}and the path should validate successfully. If not, then the *user-constrained-policy-set* will be empty. If the *user-constrained-policy-set* is empty and the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 Self-Issued CA Cert
- inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 subCA2 CRL
- inhibitAnyPolicy1 Self-Issued subCA2 Cert
- Valid Self-Issued inhibitAnyPolicy Test9 EE

4.12.10 Invalid Self-Issued inhibitAnyPolicy Test10

In this test, the first intermediate certificate asserts NIST-test-policy-1 and includes an **inhibitAnyPolicy** extension set to 1. The second intermediate certificate is a self-issued certificate that asserts NIST-test-policy-1. The third intermediate certificate asserts **anyPolicy**. The end

entity certificate is a self-issued CA certificate that asserts **anyPolicy**.

Procedure: Validate Invalid Self-Issued inhibitAnyPolicy Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.128 using the default settings.

Expected Result: The *authorities-constrained-policy-set* and *user-constrained-policy-set* will be empty and the *explicit-policy-indicator* will be set (if the application can process the **policyConstraints** extension). If the application can process the **policyConstraints** extension, then the path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 CA CRL
- inhibitAnyPolicy1 Self-Issued CA Cert
- inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 subCA2 CRL
- Invalid Self-Issued inhibitAnyPolicy Test10 EE

4.13 Name Constraints

The tests in this section were designed to verify an application's ability to process the **nameConstraints** extension. The tests in this section include certification paths in which one or more certificates include a **nameConstraints** extension with permitted and/or excluded subtrees of type **directoryName**, **rfc822Name**, **dNSName**, and **uniformResourceIdentifier**. For each of these name forms, a few tests have been included to determine if an application can determine whether a name of that type falls within a specified subtree. Some more extensive tests have been included to verify that an application can process name constraints when a certificate includes a **nameConstraints** extension that specifies more than one subtree or the path includes more than one certificate with a **nameConstraints** extension. The permitted and excluded subtrees in these tests specify subtrees of type **directoryName**, since it is anticipated that this will be the most widely used name form for which name constraints will be applied and thus the most likely to be implemented. There are also some tests in which name constraints for both **directoryName**s and **rfc822Name**s have been applied.

If an application can process the name constraints extension, but can not process all four of the name forms used in these tests, then the outcomes for some of the tests may vary from the outcomes indicated below. In particular, if a certificate includes a **nameConstraints** extension that includes a permitted or excluded subtree for a name form for which the application can not process name constraints, and a name of that name form appears in the **subject** field or **subjectAltName** extension or a subsequent certificate, then the application must reject the path. If the application being processed is capable of processing name constraints for all four of the name forms used in the tests below, then it will not be possible to use this test suite to determine how the application handles the presence of a critical **nameConstraints** extension that includes a name form that the application can not process.

4.13.1 Valid DN nameConstraints Test1

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.

Procedure: Validate Valid DN nameConstraints Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.129 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- Valid DN nameConstraints Test1 EE

4.13.2 Invalid DN nameConstraints Test2

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.

Procedure: Validate Invalid DN nameConstraints Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.130 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- Invalid DN nameConstraints Test2 EE

4.13.3 Invalid DN nameConstraints Test3

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and a **subjectAltName** extension with a DN that falls outside the subtree.

Procedure: Validate Invalid DN nameConstraints Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.131 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- Invalid DN nameConstraints Test3 EE

4.13.4 Valid DN nameConstraints Test4

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and a **subjectAltName** extension with an e-mail address.

Procedure: Validate Valid DN nameConstraints Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.132 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- Valid DN nameConstraints Test4 EE

4.13.5 Valid DN nameConstraints Test5

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies two permitted subtrees. The end entity certificate includes a subject name that falls within one of the subtrees and a **subjectAltName** extension with a DN that falls within the other subtree.

Procedure: Validate Valid DN nameConstraints Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.133 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN2 CA Cert, nameConstraints DN2 CA CRL
- Valid DN nameConstraints Test5 EE

4.13.6 Valid DN nameConstraints Test6

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a subject name that falls outside that subtree.

Procedure: Validate Valid DN nameConstraints Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.134 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- Valid DN nameConstraints Test6 EE

4.13.7 Invalid DN nameConstraints Test7

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a subject name that falls within that subtree.

Procedure: Validate Invalid DN nameConstraints Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.135 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- Invalid DN nameConstraints Test7 EE

4.13.8 Invalid DN nameConstraints Test8

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies two excluded subtrees. The end entity certificate includes a subject name that falls within the first subtree.

Procedure: Validate Invalid DN nameConstraints Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.136 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN4 CA Cert, nameConstraints DN4 CA CRL
- Invalid DN nameConstraints Test8 EE

4.13.9 Invalid DN nameConstraints Test9

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies two excluded subtrees. The end entity certificate includes a subject name that falls within the second subtree.

Procedure: Validate Invalid DN nameConstraints Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.137 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN4 CA Cert, nameConstraints DN4 CA CRL
- Invalid DN nameConstraints Test9 EE

4.13.10 Invalid DN nameConstraints Test10

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a permitted subtree and an excluded subtree. The excluded subtree specifies a subset of the name space specified by the permitted subtree. The end entity certificate includes a subject name that falls within both the permitted and excluded subtrees.

Procedure: Validate Invalid DN nameConstraints Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.138 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN5 CA Cert, nameConstraints DN5 CA CRL
- Invalid DN nameConstraints Test10 EE

4.13.11 Valid DN nameConstraints Test11

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a permitted subtree and an excluded subtree. The excluded subtree specifies a subset of the name space specified by the permitted subtree. The end entity certificate includes a subject name that falls within the permitted subtree but falls outside the excluded subtree.

Procedure: Validate Valid DN nameConstraints Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.139 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN5 CA Cert, nameConstraints DN5 CA CRL
- Valid DN nameConstraints Test11 EE

4.13.12 Invalid DN nameConstraints Test12

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The second intermediate certificate includes a subject name that falls within that subtree and a **nameConstraints** extension that specifies a permitted subtree that is a subtree of the constraint specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the subtree specified by the first intermediate certificate but outside the subtree specified by the second intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test12 EE using the default settings or open and verify Signed Test Message 6.2.2.140 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA1 Cert, nameConstraints DN1 subCA1 CRL
- Invalid DN nameConstraints Test12 EE

4.13.13 Invalid DN nameConstraints Test13

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The second intermediate certificate includes a subject name that falls

within that subtree and a **nameConstraints** extension that specifies a permitted subtree that does not overlap with the permitted subtree specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the subtree specified by the first intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test13 EE using the default settings or open and verify Signed Test Message 6.2.2.141 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA2 Cert, nameConstraints DN1 subCA2 CRL
- Invalid DN nameConstraints Test13 EE

4.13.14 Valid DN nameConstraints Test14

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The second intermediate certificate includes a subject name that falls within that subtree and a **nameConstraints** extension that specifies a permitted subtree that does not overlap with the permitted subtree specified in the first intermediate certificate. The end entity certificate has a null subject name (i.e., the subject name is a sequence of zero relative distinguished names) and a critical **subjectAltName** extension with an e-mail address.

Procedure: Validate Valid DN nameConstraints Test14 EE using the default settings or open and verify Signed Test Message 6.2.2.142 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA2 Cert, nameConstraints DN1 subCA2 CRL
- Valid DN nameConstraints Test14 EE

4.13.15 Invalid DN nameConstraints Test15

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The second intermediate certificate has a subject name that falls outside that subtree and includes a **nameConstraints** extension that specifies an excluded subtree that does not overlap with the subtree specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the subtree specified in the first intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test15 EE using the default settings or open and verify Signed Test Message 6.2.2.143 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- nameConstraints DN3 subCA1 Cert, nameConstraints DN3 subCA1 CRL
- Invalid DN nameConstraints Test15 EE

4.13.16 Invalid DN nameConstraints Test16

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The second intermediate certificate has a subject name that falls outside that subtree and includes a **nameConstraints** extension that specifies an excluded subtree that does not overlap with the subtree specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the subtree specified in the second intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test16 EE using the default settings or open and verify Signed Test Message 6.2.2.144 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- nameConstraints DN3 subCA1 Cert, nameConstraints DN3 subCA1 CRL
- Invalid DN nameConstraints Test16 EE

4.13.17 Invalid DN nameConstraints Test17

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The second intermediate certificate has a subject name that falls outside that subtree and includes a **nameConstraints** extension that specifies a permitted subtree that is a superset of the subtree specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the excluded subtree specified in the first intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test17 EE using the default settings or open and verify Signed Test Message 6.2.2.145 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- nameConstraints DN3 subCA2 Cert, nameConstraints DN3 subCA2 CRL
- Invalid DN nameConstraints Test17 EE

4.13.18 Valid DN nameConstraints Test18

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The second intermediate certificate has a subject name that falls outside that subtree and includes a **nameConstraints** extension that specifies a permitted subtree that is a superset of the subtree specified in the first intermediate certificate. The end entity certificate

includes a subject name that falls within the permitted subtree specified in the second intermediate certificate but outside the excluded subtree specified in the first intermediate certificate.

Procedure: Validate Valid DN nameConstraints Test18 EE using the default settings or open and verify Signed Test Message 6.2.2.146 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN3 CA Cert, nameConstraints DN3 CA CRL
- nameConstraints DN3 subCA2 Cert, nameConstraints DN3 subCA2 CRL
- Valid DN nameConstraints Test18 EE

4.13.19 Valid Self-Issued DN nameConstraints Test19

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The second intermediate certificate is a self-issued certificate. The subject name in the self-issued certificate does not fall within the permitted subtree specified in the first intermediate certificate. The end entity certificate includes a subject name that falls within the permitted subtree specified in the first intermediate certificate.

Procedure: Validate Valid DN nameConstraints Test19 EE using the default settings or open and verify Signed Test Message 6.2.2.147 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 Self-Issued CA Cert
- Valid DN nameConstraints Test19 EE

4.13.20 Invalid Self-Issued DN nameConstraints Test20

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate is a self-issued certificate. The subject name in the self-issued certificate does not fall within the permitted subtree specified in the intermediate certificate.

Procedure: Validate Invalid DN nameConstraints Test20 EE using the default settings or open and verify Signed Test Message 6.2.2.148 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- Invalid DN nameConstraints Test20 EE

4.13.21 Valid RFC822 nameConstraints Test21

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls within that subtree.

Procedure: Validate Valid RFC822 nameConstraints Test21 EE using the default settings or open and verify Signed Test Message 6.2.2.149 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA1 Cert, nameConstraints RFC822 CA1 CRL
- Valid RFC822 nameConstraints Test21 EE

4.13.22 Invalid RFC822 nameConstraints Test22

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls outside that subtree.

Procedure: Validate Invalid RFC822 nameConstraints Test22 EE using the default settings or open and verify Signed Test Message 6.2.2.150 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA1 Cert, nameConstraints RFC822 CA1 CRL
- Invalid RFC822 nameConstraints Test22 EE

4.13.23 Valid RFC822 nameConstraints Test23

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls within that subtree.

Procedure: Validate Valid RFC822 nameConstraints Test23 EE using the default settings or open and verify Signed Test Message 6.2.2.151 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA2 Cert, nameConstraints RFC822 CA2 CRL
- Valid RFC822 nameConstraints Test23 EE

4.13.24 Invalid RFC822 nameConstraints Test24

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls outside that subtree.

Procedure: Validate Invalid RFC822 nameConstraints Test24 EE using the default settings or open and verify Signed Test Message 6.2.2.152 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA2 Cert, nameConstraints RFC822 CA2 CRL
- Invalid RFC822 nameConstraints Test24 EE

4.13.25 Valid RFC822 nameConstraints Test25

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls outside that subtree.

Procedure: Validate Valid RFC822 nameConstraints Test25 EE using the default settings or open and verify Signed Test Message 6.2.2.153 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA3 Cert, nameConstraints RFC822 CA3 CRL
- Valid RFC822 nameConstraints Test25 EE

4.13.26 Invalid RFC822 nameConstraints Test26

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with an e-mail address that falls within that subtree.

Procedure: Validate Invalid RFC822 nameConstraints Test26 EE using the default settings or open and verify Signed Test Message 6.2.2.154 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints RFC822 CA3 Cert, nameConstraints RFC822 CA3 CRL
- Invalid RFC822 nameConstraints Test26 EE

4.13.27 Valid DN and RFC822 nameConstraints Test27

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree of type **directoryName**. The second intermediate certificate includes a

subject name that falls within that subtree and a **nameConstraints** extension that specifies a permitted subtree of type **rfc822Name**. The end entity certificate includes a subject name that falls within the subtree specified by the first intermediate certificate and an e-mail address that falls within the permitted subtree specified by the second intermediate certificate.

Procedure: Validate Valid DN and RFC822 nameConstraints Test27 EE using the default settings or open and verify Signed Test Message 6.2.2.155 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA3 Cert, nameConstraints DN1 subCA3 CRL
- Valid DN and RFC822 nameConstraints Test27 EE

4.13.28 Invalid DN and RFC822 nameConstraints Test28

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree of type **directoryName**. The second intermediate certificate includes a subject name that falls within that subtree and a **nameConstraints** extension that specifies a permitted subtree of type **rfc822Name**. The end entity certificate includes a subject name that falls within the subtree specified by the first intermediate certificate and an e-mail address that falls outside the permitted subtree specified by the second intermediate certificate.

Procedure: Validate Invalid DN and RFC822 nameConstraints Test28 EE using the default settings or open and verify Signed Test Message 6.2.2.156 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA3 Cert, nameConstraints DN1 subCA3 CRL
- Invalid DN and RFC822 nameConstraints Test28 EE

4.13.29 Invalid DN and RFC822 nameConstraints Test29

In this test, the first intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree of type **directoryName**. The second intermediate certificate includes a subject name that falls within that subtree and a **nameConstraints** extension that specifies a permitted subtree of type **rfc822Name**. The end entity certificate includes a subject name that falls within the subtree specified by the first intermediate certificate but the subject name includes an attribute of type **EmailAddress** whose value falls outside the permitted subtree specified in the second intermediate certificate.

Procedure: Validate Invalid DN and RFC822 nameConstraints Test29 EE using the default settings or open and verify Signed Test Message 6.2.2.157 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DN1 CA Cert, nameConstraints DN1 CA CRL
- nameConstraints DN1 subCA3 Cert, nameConstraints DN1 subCA3 CRL
- Invalid DN and RFC822 nameConstraints Test29 EE

4.13.30 Valid DNS nameConstraints Test30

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with a **dNSName** that falls within that subtree.

Procedure: Validate Valid DNS nameConstraints Test30 EE using the default settings or open and verify Signed Test Message 6.2.2.158 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DNS1 CA Cert, nameConstraints DNS1 CA CRL
- Valid DNS nameConstraints Test30 EE

4.13.31 Invalid DNS nameConstraints Test31

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with a **dNSName** that falls outside that subtree.

Procedure: Validate Invalid DNS nameConstraints Test31 EE using the default settings or open and verify Signed Test Message 6.2.2.159 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DNS1 CA Cert, nameConstraints DNS1 CA CRL
- Invalid DNS nameConstraints Test31 EE

4.13.32 Valid DNS nameConstraints Test32

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with a **dNSName** that falls outside that subtree.

Procedure: Validate Valid DNS nameConstraints Test32 EE using the default settings or open and verify Signed Test Message 6.2.2.160 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DNS2 CA Cert, nameConstraints DNS2 CA CRL

- Valid DNS nameConstraints Test32 EE

4.13.33 Invalid DNS nameConstraints Test33

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with a **dNSName** that falls within that subtree.

Procedure: Validate Invalid DNS nameConstraints Test33 EE using the default settings or open and verify Signed Test Message 6.2.2.161 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DNS2 CA Cert, nameConstraints DNS2 CA CRL
- Invalid DNS nameConstraints Test33 EE

4.13.34 Valid URI nameConstraints Test34

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with a **uniformResourceIdentifier** that falls within that subtree.

Procedure: Validate Valid URI nameConstraints Test34 EE using the default settings or open and verify Signed Test Message 6.2.2.162 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints URI1 CA Cert, nameConstraints URI1 CA CRL
- Valid URI nameConstraints Test34 EE

4.13.35 Invalid URI nameConstraints Test35

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with a **uniformResourceIdentifier** that falls outside that subtree.

Procedure: Validate Invalid URI nameConstraints Test35 EE using the default settings or open and verify Signed Test Message 6.2.2.163 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints URI1 CA Cert, nameConstraints URI1 CA CRL
- Invalid URI nameConstraints Test35 EE

4.13.36 Valid URI nameConstraints Test36

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with a **uniformResourceIdentifier** that falls outside that subtree.

Procedure: Validate Valid URI nameConstraints Test36 EE using the default settings or open and verify Signed Test Message 6.2.2.164 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints URI2 CA Cert, nameConstraints URI2 CA CRL
- Valid URI nameConstraints Test36 EE

4.13.37 Invalid URI nameConstraints Test37

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single excluded subtree. The end entity certificate includes a **subjectAltName** extension with a **uniformResourceIdentifier** that falls within that subtree.

Procedure: Validate Invalid URI nameConstraints Test37 EE using the default settings or open and verify Signed Test Message 6.2.2.165 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints URI2 CA Cert, nameConstraints URI2 CA CRL
- Invalid URI nameConstraints Test37 EE

4.13.38 Invalid DNS nameConstraints Test38

In this test, the intermediate certificate includes a **nameConstraints** extension that specifies a single permitted subtree. The end entity certificate includes a **subjectAltName** extension with a **dNSName** that falls outside that subtree. The permitted subtree is "testcertificates.gov" and the **subjectAltName** is "mytestcertificates.gov".

Procedure: Validate Invalid DNS nameConstraints Test38 EE using the default settings or open and verify Signed Test Message 6.2.2.218 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- nameConstraints DNS1 CA Cert, nameConstraints DNS1 CA CRL
- Invalid DNS nameConstraints Test38 EE

4.14 Distribution Points

The tests in this section were designed to verify an application's ability to process the **cRLDistributionPoints** certificate extension and the **issuingDistributionPoint** CRL extension. These two extensions may be used for multiple purposes: to spread certificate status information about the certificates issued by a CA among multiple CRLs, to have certificates listed on different CRLs depending on the reason that they were revoked, or to have the CRL that indicates the status of a certificate be issued by a different entity from the CA that issued the certificate.

In many of the tests in this section, the certification path includes a certificate for which there is no valid, up-to-date certificate status information available. For these tests, the application must either reject the certification path or warn the user that the status of the certificate can not be determined (as described in section 4.4).

Some applications may be able to process some of the fields in these extensions, but not all of them. If an application is unable to determine the status of a certificate in one or more of the tests below as a result of being unable to process all aspects of the **cRLDistributionPoints** extension or **issuingDistributionPoint** extension, then the application must reject the path or provide a warning to the user that it is unable to determine the status of the certificate.

4.14.1 Valid distributionPoint Test1

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**.

Procedure: Validate Valid distributionPoint Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.166 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint1 CA Cert, distributionPoint1 CA CRL
- Valid distributionPoint Test1 EE

4.14.2 Invalid distributionPoint Test2

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**. The CRL lists the end entity certificate as being revoked.

Procedure: Validate Invalid distributionPoint Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.167 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- distributionPoint1 CA Cert, distributionPoint1 CA CRL
- Invalid distributionPoint Test2 EE

4.14.3 Invalid distributionPoint Test3

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The only CRL available from the issuer of the end entity certificate includes an **issuingDistributionPoint** extension with a **distributionPoint** that does not match the **distributionPoint** specified in the end entity certificate.

Procedure: Validate Invalid distributionPoint Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.168 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint1 CA Cert, distributionPoint1 CA CRL
- Invalid distributionPoint Test3 EE

4.14.4 Valid distributionPoint Test4

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**. The **distributionPoint** in the end entity certificate is specified as a **nameRelativeToCRLIssuer** while the **distributionPoint** in the CRL is specified as a **fullName**.

Procedure: Validate Valid distributionPoint Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.169 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint1 CA Cert, distributionPoint1 CA CRL
- Valid distributionPoint Test4 EE

4.14.5 Valid distributionPoint Test5

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**. The **distributionPoint** in both the end entity certificate and the CRL are specified as a **nameRelativeToCRLIssuer**.

Procedure: Validate Valid distributionPoint Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.170 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint2 CA Cert, distributionPoint2 CA CRL
- Valid distributionPoint Test5 EE

4.14.6 Invalid distributionPoint Test6

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**. The **distributionPoint** in both the end entity certificate and the CRL are specified as a **nameRelativeToCRLIssuer**. The CRL lists the end entity certificate as being revoked.

Procedure: Validate Invalid distributionPoint Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.171 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint2 CA Cert, distributionPoint2 CA CRL
- Invalid distributionPoint Test6 EE

4.14.7 Valid distributionPoint Test7

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a matching **distributionPoint**. The **distributionPoint** in the CRL is specified as a **nameRelativeToCRLIssuer** and the **distributionPoint** in the end entity certificate is specified as a **fullName**.

Procedure: Validate Valid distributionPoint Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.172 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint2 CA Cert, distributionPoint2 CA CRL
- Valid distributionPoint Test7 EE

4.14.8 Invalid distributionPoint Test8

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a single **DistributionPoint** consisting of a **distributionPoint** with a distinguished name. The CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a **distributionPoint** that does not match. The **distributionPoint** in the CRL is specified as a **nameRelativeToCRLIssuer** and the **distributionPoint** in the end entity certificate is specified as a **fullName**.

Procedure: Validate Invalid distributionPoint Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.173 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint2 CA Cert, distributionPoint2 CA CRL
- Invalid distributionPoint Test8 EE

4.14.9 Invalid distributionPoint Test9

In this test, the CRL that covers the end entity certificate includes an **issuingDistributionPoint** extension with a **distributionPoint**. The **distributionPoint** does not match the CRL issuer's name. The end entity certificate does not include a **cRLDistributionPoints** extension

Procedure: Validate Invalid distributionPoint Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.174 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- distributionPoint2 CA Cert, distributionPoint2 CA CRL
- Invalid distributionPoint Test9 EE

4.14.10 Valid No issuingDistributionPoint Test10

In this test, the CRL that covers the end entity certificate does not include an **issuingDistributionPoint** extension. The end entity certificate includes a **cRLDistributionPoints** extension with a **distributionPoint** name.

Procedure: Validate Valid No issuingDistributionPoint Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.175 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- No issuingDistributionPoint CA Cert, No issuingDistributionPoint CA CRL
- Valid No issuingDistributionPoint Test10 EE

4.14.11 Invalid onlyContainsUserCerts CRL Test11

In this test, the only CRL issued by the intermediate CA includes an **issuingDistributionPoint** extension with **onlyContainsUserCerts** set to TRUE. The final certificate in the path is a CA certificate.

Procedure: Validate Invalid onlyContainsUserCerts Test11 EE using the default settings or open and verify Signed Test Message 6.2.2.176 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlyContainsUserCerts CA Cert, onlyContainsUserCerts CA CRL
- Invalid onlyContainsUserCerts Test11 EE

4.14.12 Invalid onlyContainsCACerts CRL Test12

In this test, the only CRL issued by the intermediate CA includes an **issuingDistributionPoint** extension with **onlyContainsCACerts** set to TRUE.

Procedure: Validate Invalid onlyContainsCACerts Test12 EE using the default settings or open and verify Signed Test Message 6.2.2.177 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlyContainsCACerts CA Cert, onlyContainsCACerts CA CRL
- Invalid onlyContainsCACerts Test12 EE

4.14.13 Valid onlyContainsCACerts CRL Test13

In this test, the only CRL issued by the intermediate CA includes an **issuingDistributionPoint** extension with **onlyContainsCACerts** set to TRUE. The final certificate in the path is a CA certificate.

Procedure: Validate Valid onlyContainsCACerts Test13 EE using the default settings or open and verify Signed Test Message 6.2.2.178 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlyContainsCACerts CA Cert, onlyContainsCACerts CA CRL
- Valid onlyContainsCACerts Test13 EE

4.14.14 Invalid onlyContainsAttributeCerts Test14

In this test, the only CRL issued by the intermediate CA includes an **issuingDistributionPoint** extension with **onlyContainsAttributeCerts** set to TRUE.

Procedure: Validate Invalid onlyContainsAttributeCerts Test14 EE using the default settings or open and verify Signed Test Message 6.2.2.179 using the default settings.

Expected Result: The path should not validate successfully since the status of the end certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlyContainsAttributeCerts CA Cert, onlyContainsAttributeCerts CA CRL
- Invalid onlyContainsAttributeCerts Test14 EE

4.14.15 Invalid onlySomeReasons Test15

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. The end entity certificate has been revoked for key compromise.

Procedure: Validate Invalid onlySomeReasons Test15 EE using the default settings or open and verify Signed Test Message 6.2.2.180 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA1 Cert, onlySomeReasons CA1 compromise CRL, onlySomeReasons CA1 other reasons CRL
- Invalid onlySomeReasons Test15 EE

4.14.16 Invalid onlySomeReasons Test16

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. The end entity certificate has been placed on hold.

Procedure: Validate Invalid onlySomeReasons Test16 EE using the default settings or open and verify Signed Test Message 6.2.2.181 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate is on hold.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA1 Cert, onlySomeReasons CA1 compromise CRL, onlySomeReasons CA1 other reasons CRL
- Invalid onlySomeReasons Test16 EE

4.14.17 Invalid onlySomeReasons Test17

In this test, the intermediate certificate has issued two CRLs, one covering the **affiliationChanged** and **superseded** reason codes and the other covering the **cessationOfOperation** and **certificateHold** reason codes. The end entity certificate is not listed on either CRL.

Procedure: Validate Invalid onlySomeReasons Test17 EE using the default settings or open and verify Signed Test Message 6.2.2.182 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA2 Cert, onlySomeReasons CA2 CRL1, onlySomeReasons CA2 CRL2
- Invalid onlySomeReasons Test17 EE

4.14.18 Valid onlySomeReasons Test18

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. Both CRLs include an **issuingDistributionPoint** extension with the same **distributionPoint** name. The end entity certificate includes a **cRLDistributionPoints** extension with the same **distributionPoint** name.

Procedure: Validate Valid onlySomeReasons Test18 EE using the default settings or open and verify Signed Test Message 6.2.2.183 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA3 Cert, onlySomeReasons CA3 compromise CRL, onlySomeReasons CA3 other reasons CRL
- Valid onlySomeReasons Test18 EE

4.14.19 Valid onlySomeReasons Test19

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. Both CRLs include an **issuingDistributionPoint** extension with a different **distributionPoint** name. The end entity certificate includes a **cRLDistributionPoints** extension with two **DistributionPoint**s, one for each CRL.

Procedure: Validate Valid onlySomeReasons Test19 EE using the default settings or open and verify Signed Test Message 6.2.2.184 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- onlySomeReasons CA4 Cert, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
- Valid onlySomeReasons Test19 EE

4.14.20 Invalid onlySomeReasons Test20

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. Both CRLs include an **issuingDistributionPoint** extension with a different **distributionPoint** name. The end entity certificate includes a **cRLDistributionPoints** extension with two **DistributionPoint**s, one for each CRL. The end entity certificate has been revoked for key compromise.

Procedure: Validate Invalid onlySomeReasons Test20 EE using the default settings or open and verify Signed Test Message 6.2.2.185 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA4 Cert, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
- Invalid onlySomeReasons Test20 EE

4.14.21 Invalid onlySomeReasons Test21

In this test, the intermediate certificate has issued two CRLs, one covering the **keyCompromise** and **cACompromise** reason codes and the other covering the remaining reason codes. Both CRLs include an **issuingDistributionPoint** extension with a different **distributionPoint** name. The end entity certificate includes a **cRLDistributionPoints** extension with two **DistributionPoint**s, one for each CRL. The end entity certificate has been revoked as a result of a change in affiliation.

Procedure: Validate Invalid onlySomeReasons Test21 EE using the default settings or open and verify Signed Test Message 6.2.2.186 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- onlySomeReasons CA4 Cert, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
- Invalid onlySomeReasons Test21 EE

4.14.22 Valid IDP with indirectCRL Test22

In this test, the intermediate CA has issued a CRL that contains an **issuingDistributionPoint** extension with the **indirectCRL** flag set. The end entity certificate was issued by the intermediate CA.

Procedure: Validate Valid IDP with indirectCRL Test22 EE using the default settings or open and verify Signed Test Message 6.2.2.187 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA1 Cert, indirectCRL CA1 CRL
- Valid IDP with indirectCRL Test22 EE

4.14.23 Invalid IDP with indirectCRL Test23

In this test, the intermediate CA has issued a CRL that contains an **issuingDistributionPoint** extension with the **indirectCRL** flag set. The end entity certificate was issued by the intermediate CA and is listed as revoked on the CRL.

Procedure: Validate Invalid IDP with indirectCRL Test23 EE using the default settings or open and verify Signed Test Message 6.2.2.188 using the default settings.

Expected Result: The path should not validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA1 Cert, indirectCRL CA1 CRL
- Invalid IDP with indirectCRL Test23 EE

4.14.24 Valid IDP with indirectCRL Test24

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The public key needed to validate the indirect CRL is in a certificate issued by the Trust Anchor.

Procedure: Validate Valid IDP with indirectCRL Test24 EE using the default settings or open and verify Signed Test Message 6.2.2.189 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA2 Cert
- indirectCRL CA1 Cert, indirectCRL CA1 CRL
- Valid IDP with indirectCRL Test24 EE

4.14.25 Valid IDP with indirectCRL Test25

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The public key needed to validate the indirect CRL is in a certificate issued by the Trust Anchor. The end entity's serial number is listed on the CRL, but there is no **certificateIssuer** CRL entry extension, indicating that the revoked certificate was one issued by the CRL issuer.

Procedure: Validate Valid IDP with indirectCRL Test25 EE using the default settings or open and verify Signed Test Message 6.2.2.190 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA2 Cert
- indirectCRL CA1 Cert, indirectCRL CA1 CRL
- Valid IDP with indirectCRL Test25 EE

4.14.26 Invalid IDP with indirectCRL Test26

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The entity specified in the **cRLIssuer** field does not exist.

Procedure: Validate Invalid IDP with indirectCRL Test26 EE using the default settings or open and verify Signed Test Message 6.2.2.191 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA2 Cert
- indirectCRL CA1 Cert, indirectCRL CA1 CRL
- Invalid IDP with indirectCRL Test26 EE

4.14.27 Invalid cRLIssuer Test27

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The CRL issued by the entity specified in the **cRLIssuer** field does not include an **issuingDistributionPoint** extension.

Procedure: Validate Invalid cRLIssuer Test27 EE using the default settings or open and verify Signed Test Message 6.2.2.192 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA2 Cert
- Good CA Cert, Good CA CRL
- Invalid cRLIssuer Test27 EE

4.14.28 Valid cRLIssuer Test28

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a

cRLIssuer field indicating that the CRL is issued by an entity other than the certificate issuer. The indirect CRL issuer has been issued a certificate by the issuer of the end entity certificate. The certificate issued to the CRL issuer is covered by a CRL issued by the issuer of the end entity certificate.

Procedure: Validate Valid cRLIssuer Test28 EE using the default settings or open and verify Signed Test Message 6.2.2.193 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA3 Cert, indirectCRL CA3 CRL
- indirectCRL CA3 cRLIssuer Cert, indirectCRL CA3 cRLIssuer CRL
- Valid cRLIssuer Test28 EE

4.14.29 Valid cRLIssuer Test29

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The **distributionPoint** in the end entity certificate is specified as **nameRelativeToCRLIssuer**. The indirect CRL issuer has been issued a certificate by the issuer of the end entity certificate. The certificate issued to the CRL issuer is covered by a CRL issued by the issuer of the end entity certificate.

Procedure: Validate Valid cRLIssuer Test29 EE using the default settings or open and verify Signed Test Message 6.2.2.194 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA3 Cert, indirectCRL CA3 CRL
- indirectCRL CA3 cRLIssuer Cert, indirectCRL CA3 cRLIssuer CRL
- Valid cRLIssuer Test29 EE

4.14.30 Valid cRLIssuer Test30

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The indirect CRL issuer has been issued a certificate by the issuer of the end entity certificate. Both the end entity certificate and the certificate issued to the CRL issuer are covered by the indirect CRL issued by the CRL issuer.

Procedure: Validate Valid cRLIssuer Test30 EE using the default settings or open and verify Signed Test Message 6.2.2.195 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA4 Cert
- indirectCRL CA4 cRLIssuer Cert, indirectCRL CA4 cRLIssuer CRL
- Valid cRLIssuer Test30 EE

4.14.31 Invalid cRLIssuer Test31

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The indirect CRL contains a CRL entry listing the end entity certificate's serial number that includes a **certificateIssuer** extension specifying the end entity certificate's issuer.

Procedure: Validate Invalid cRLIssuer Test31 EE using the default settings or open and verify Signed Test Message 6.2.2.196 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA5 Cert, indirectCRL CA5 CRL
- indirectCRL CA6 Cert
- Invalid cRLIssuer Test31 EE

4.14.32 Invalid cRLIssuer Test32

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The indirect CRL contains a CRL entry listing the end entity certificate's serial number and the preceding CRL entry includes a **certificateIssuer** extension specifying the end entity certificate's issuer.

Procedure: Validate Invalid cRLIssuer Test32 EE using the default settings or open and verify Signed Test Message 6.2.2.197 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA5 Cert, indirectCRL CA5 CRL
- indirectCRL CA6 Cert
- Invalid cRLIssuer Test32 EE

4.14.33 Valid cRLIssuer Test33

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. The indirect CRL contains a CRL entry listing the end entity certificate's serial number, but the most recent CRL entry to include a **certificateIssuer** extension specified a different certificate issuer.

Procedure: Validate Valid cRLIssuer Test33 EE using the default settings or open and verify Signed Test Message 6.2.2.198 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA5 Cert, indirectCRL CA5 CRL
- indirectCRL CA6 Cert
- Valid cRLIssuer Test33 EE

4.14.34 Invalid cRLIssuer Test34

In this test, the end entity certificate is issued by the same CA that issues the corresponding CRL, but the CRL is also an indirect CRL for other CAs. The end entity certificate's serial number is listed on the CRL and the most recent CRL entry to include a **certificateIssuer** extension specifies the end entity certificate's issuer.

Procedure: Validate Invalid cRLIssuer Test34 EE using the default settings or open and verify Signed Test Message 6.2.2.199 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA5 Cert, indirectCRL CA5 CRL
- Invalid cRLIssuer Test34 EE

4.14.35 Invalid cRLIssuer Test35

In this test, the end entity certificate includes a **cRLDistributionPoints** extension with both a **distributionPoint** name and a **cRLIssuer** field indicating that the CRL is issued by an entity other than the certificate issuer. There is no CRL available from the entity specified in **cRLIssuer**, but the certificate issuer has issued a CRL with an **issuingDistributionPoint** extension that includes a **distributionPoint** that matches the **distributionPoint** in the certificate.

Procedure: Validate Invalid cRLIssuer Test35 EE using the default settings or open and verify Signed Test Message 6.2.2.200 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- indirectCRL CA5 Cert, indirectCRL CA5 CRL
- Invalid cRLIssuer Test35 EE

4.15 Delta-CRLs

The tests in this section are designed to verify that an application can process the **deltaCRLIndicator** extension. All applications should be able to process the first test in this section. Applications that can not process the **deltaCRLIndicator** extension should reject the path in the first test since the CRL issued by the intermediate CA includes a critical extension that the application can not process. The remaining tests in this section are only relevant to those applications that can process the **deltaCRLIndicator** extension.

In order to enable the processing of delta-CRLs, each certificate that is covered by a delta-CRL includes a **FreshestCRL** extension that points to the directory entry where the delta-CRL is located. The **FreshestCRL** extension is also included in each complete CRL for which a corresponding delta-CRL has been issued. The **FreshestCRL** extension has been made non-critical in each of the certificates and CRLs, as is mandated by RFC 3280. According to X.509, the application may decide based on local policy whether to obtain and check a CRL that is pointed to by a non-critical **FreshestCRL** extension. So, it may be necessary with some applications that can process delta-CRLs to make changes to the local configuration in order to get them to obtain and process the delta-CRLs used in the tests in this section.

When a certification path is invalid as a result of certificate status information not being available, the application may choose to provide a warning to the user rather than reject the path (as described in section 4.4).

4.15.1 Invalid deltaCRLIndicator No Base Test1

In this test, the CRL covering the end entity certificate includes a **deltaCRLIndicator** extension, but no other CRLs are available for the intermediate certificate.

Procedure: Validate Invalid deltaCRLIndicator No Base Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.201 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRLIndicator No Base CA Cert, deltaCRLIndicator No Base CA CRL
- Invalid deltaCRLIndicator No Base Test1 EE

4.15.2 Valid delta-CRL Test2

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL.

Procedure: Validate Valid deltaCRL Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.202 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Valid deltaCRL Test2 EE

4.15.3 Invalid delta-CRL Test3

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL. The end entity certificate is listed as revoked on the complete CRL.

Procedure: Validate Invalid deltaCRL Test3 EE using the default settings or open and verify Signed Test Message 6.2.2.203 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Invalid deltaCRL Test3 EE

4.15.4 Invalid delta-CRL Test4

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL. The end entity certificate is listed as revoked on the delta-CRL.

Procedure: Validate Invalid deltaCRL Test4 EE using the default settings or open and verify Signed Test Message 6.2.2.204 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Invalid deltaCRL Test4 EE

4.15.5 Valid delta-CRL Test5

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL. The end entity certificate is listed as on hold on the complete CRL, but the delta-CRL indicates that it should be removed from the CRL.

Procedure: Validate Valid deltaCRL Test5 EE using the default settings or open and verify Signed Test Message 6.2.2.205 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Valid deltaCRL Test5 EE

4.15.6 Invalid delta-CRL Test6

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL. The end entity certificate is listed as on hold on the complete CRL and the delta-CRL indicates that it has been revoked.

Procedure: Validate Invalid deltaCRL Test6 EE using the default settings or open and verify Signed Test Message 6.2.2.206 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Invalid deltaCRL Test6 EE

4.15.7 Valid delta-CRL Test7

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to the complete CRL as its base CRL. The end entity certificate is not listed on the complete CRL and is listed on the delta-CRL as **removeFromCRL**.

Procedure: Validate Valid deltaCRL Test7 EE using the default settings or open and verify Signed Test Message 6.2.2.207 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA1 Cert, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
- Valid deltaCRL Test7 EE

4.15.8 Valid delta-CRL Test8

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to a CRL that was issued earlier than the complete CRL as its base CRL. The end entity certificate is not listed on either the complete CRL or the delta-CRL.

Procedure: Validate Valid deltaCRL Test8 EE using the default settings or open and verify Signed Test Message 6.2.2.208 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA2 Cert, deltaCRL CA2 CRL, deltaCRL CA2 deltaCRL
- Valid deltaCRL Test8 EE

4.15.9 Invalid delta-CRL Test9

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to a CRL that was issued earlier than the complete CRL as its base CRL. The end entity certificate is listed as revoked on both the complete CRL and the delta-CRL.

Procedure: Validate Invalid deltaCRL Test9 EE using the default settings or open and verify Signed Test Message 6.2.2.209 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA2 Cert, deltaCRL CA2 CRL, deltaCRL CA2 deltaCRL
- Invalid deltaCRL Test9 EE

4.15.10 Invalid delta-CRL Test10

In this test, the intermediate CA has issued a complete CRL and a delta-CRL. The delta-CRL refers to a CRL that was issued later than the complete CRL as its base CRL. The end entity certificate is not listed as revoked on either the complete CRL or the delta-CRL, but the delta-CRL can not be used in conjunction with the provided complete CRL. The complete CRL has a **nextUpdate** time that is in the past.

Procedure: Validate Invalid deltaCRL Test10 EE using the default settings or open and verify Signed Test Message 6.2.2.210 using the default settings.

Expected Result: The path should not validate successfully since the status of the end entity certificate can not be determined.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- deltaCRL CA3 Cert, deltaCRL CA3 CRL, deltaCRL CA3 deltaCRL
- Invalid deltaCRL Test10 EE

4.16 Private Certificate Extensions

The tests in this section are designed to verify an application's ability to process certificates that include unknown extensions. Unknown extensions that are marked non-critical may be ignored whereas an application must reject a certificate that includes an unknown extension that is marked critical.

4.16.1 Valid Unknown Not Critical Certificate Extension Test1

In this test, the end entity certificate contains a private, non-critical certificate extension.

Procedure: Validate Valid Unknown Not Critical Certificate Extension Test1 EE using the default settings or open and verify Signed Test Message 6.2.2.211 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL
- Valid Unknown Not Critical Certificate Extension Test1 EE

4.16.2 Invalid Unknown Critical Certificate Extension Test2

In this test, the end entity certificate contains a private, critical certificate extension.

Procedure: Validate Invalid Unknown Critical Certificate Extension Test2 EE using the default settings or open and verify Signed Test Message 6.2.2.212 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate includes a unknown, critical extension.

Certification Path: The certification path is composed of the following objects:

- Trust Anchor Root Certificate, Trust Anchor Root CRL

- Invalid Unknown Critical Certificate Extension Test2 EE

5 Relationship to Previous Test Suite

The tests in this test suite incorporate the tests that were originally included in "Conformance Testing of Relying Party Client Certificate Path Processing Logic", version 1.07. The table below indicates the relationship between the tests in the 1.07 test suite and the tests in this test suite.

1.07	*PKITS*
Test 1: TE:CP.01.01	Valid Signatures Test1
Test 2: TE:CP.01.02	Invalid CA Signature Test2
Test 3: TE:CP.01.03	Invalid EE Signature Test3
Test 4: TE:CP.02.01	Valid Signatures Test1
Test 5: TE:CP.02.02	Invalid CA notBefore Date Test1
Test 6:TE:CP.02.03	Invalid EE notBefore Date Test2
Test 7: TE:CP.02.04	Valid pre2000 UTC notBefore Date Test3
Test 8: TE:CP.02.05	Replaced by Valid GeneralizedTime notBefore Date Test4
Test 9: TE:CP.03.01	Invalid CA notAfter Date Test5
Test 10: TE:CP.03.03	Invalid EE notAfter Date Test6
Test 11: TE:CP.03.03	Invalid pre2000 UTC EE notAfter Date Test7
Test 12: TE:CP.03.04	Valid GeneralizedTime notAfter Date Test8
Test 13: TE:CP.04.01	Invalid Name Chaining EE Test1
Test 14: TE:CP.04.02	Invalid Name Chaining Order Test2
Test 15: TE:CP.04.03	Not included. Covered by Valid Name Chaining Whitespace Test3, Valid Name Chaining Whitespace Test4, and Valid Name Chaining Capitalization Test5.
Test 16: TE:CP.04.04	Valid Name Chaining Whitespace Test3
Test 17: TE:CP.04.05	Valid Name Chaining Whitespace Test4
Test 18: TE:CP.04.06	Valid Name Chaining Capitalization Test5
Test 19: TE:CP.05.01	Missing CRL Test1
Test 20: TE:CP.06.01	Invalid Revoked CA Test2
Test 21: TE:CP.06.02	Invalid Revoked EE Test3
Test 22: TE:IC.01.01	Invalid Missing basicConstraints Test1
Test 23: TE:IC.02.01	Invalid cA False Test2
Test 24: TE:IC.02.02	Valid Signatures Test1
Test 25: TE:IC.02.03	Invalid cA False Test3
Test 26: TE:IC.02.04	Valid basicConstraints Not Critical Test4

1.07	*PKITS*
Test 27: TE:IC.04.01	Valid Signatures Test1
Test 28: TE:IC.05.01	Invalid keyUsage Critical keyCertSign False Test1
Test 29: TE:IC.05.02	Invalid keyUsage Not Critical keyCertSign False Test2
Test 30: TE:IC.05.03	Valid keyUsage Not Critical Test3
Test 31: TE:IC.06.01	Invalid keyUsage Critical cRLSign False Test4
Test 32: TE:IC.06.02	Invalid keyUsage Not Critical cRLSign False Test5
Test 33: TE:IC.06.03	Valid keyUsage Not Critical Test3
Test 34: TE:PP.01.01	All Certificates Same Policy Test1
Test 35: TE:PP.01.02	All Certificates No Policies Test2
Test 36: TE:PP.01.03	Different Policies Test3
Test 37: TE:PP.01.04	Different Policies Test4
Test 38: TE:PP.01.05	Different Policies Test5
Test 39: TE:PP.01.06	Overlapping Policies Test6
Test 40: TE:PP.01.07	Different Policies Test7
Test 41: TE:PP.01.08	Different Policies Test8
Test 42: TE:PP.01.09	Different Policies Test9
Test 43: TE:PP.06.01	Valid RequireExplicitPolicy Test1
Test 44: TE:PP.06.02	Valid RequireExplicitPolicy Test2
Test 45: TE:PP.06.03	Invalid RequireExplicitPolicy Test3
Test 46: TE:PP.06.04	Valid RequireExplicitPolicy Test4
Test 47: TE:PP.06.05	Invalid RequireExplicitPolicy Test5
Test 48: TE:PP.08.01	All Certificates Same Policy Test1
Test 49: TE:PP.08.02	All Certificates Same Policies Test10
Test 50: TE:PP.08.03	All Certificates AnyPolicy Test11
Test 51: TE:PP.08.04	Different Policies Test12
Test 52: TE:PP.08.05	All Certificates Same Policy Test1
Test 53: TE:PP.08.06	All Certificates Same Policies Test13
Test 54: TE:PL.01.01	Invalid pathLenConstraint Test5
Test 55: TE:PL.01.02	Invalid pathLenConstraint Test6
Test 56: TE:PL.01.03	Valid pathLenConstraint Test7
Test 57: TE:PL.01.04	Valid pathLenConstraint Test8
Test 58: TE:PL.01.05	Invalid pathLenConstraint Test9
Test 59: TE:PL.01.06	Invalid pathLenConstraint Test10

1.07	*PKITS*
Test 60: TE:PL.01.07	Invalid pathLenConstraint Test11
Test 61: TE:PL.01.08	Invalid pathLenConstraint Test12
Test 62: TE:PL.01.09	Valid pathLenConstraint Test13
Test 63: TE:PL.01.10	Valid pathLenConstraint Test14
Test 64: TE:RL.02.01	Invalid Bad CRL Signature Test4
Test 65: TE:RL.03.01	Invalid Wrong CRL Test6
Test 66: TE:RL.03.02	Invalid Bad CRL Issuer Name Test5
Test 67: TE:RL.03.03	Valid Two CRLs Test7
Test 68: TE:RL.05.01	Not included. Covered by Invalid Unknown CRL Entry Extension Test8.
Test 69: TE:RL.05.02	Invalid Unknown CRL Entry Extension Test8
Test 70: TE:RL.06.01	Not included. Covered by Invalid Unknown CRL Extension Test9
Test 71: TE:RL.06.02	Invalid Unknown CRL Extension Test9
Test 72: TE:RL.07.01	Invalid Old CRL nextUpdate Test11
Test 73: TE:RL.07.02	Invalid pre2000 CRL nextUpdate Test12
Test 74: TE:RL.07.03	Valid GeneralizedTime CRL nextUpdate Test13
Test 75: TE:RL.08.01	Invalid deltaCRLIndicator No Base Test1
Test 76: TE:RL.09.01	Invalid onlyContainsCACerts CRL Test12

6 Test Data Descriptions

This section describes the entire test data (certificates, CRLs, etc.,) used in the test procedures.

Each of the different types of test data is described in the following sections.

6.1 X.509 Certificates and CRLs

Each test certificate is based on one of several general certificates. These general, or base certificates, contain fields and values typically found in all of the certificates. Each test certificate will refer to exactly one base certificate. Only the differences between the test certificate and the base certificate will be listed so as not to have to repeat the same information in this document.

6.1.1 Base Root Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer value of "2" indicates a version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified

signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	Uses RFC 2253 format.
validity			
notBefore			
Time			
UTCTime		100101083000Z	01 January 2010, 08:30:00 GMT
notAfter			
Time			
UTCTime		301231083000Z	31 Dec. 2030, 08:30:00 GMT
subject			
Name		{ Always specified – no default }	Uses RFC 2253 format.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey			
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
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	
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
signatureValue		BIT STRING	Signature calculated

6.1.2 Base Intermediate Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the certificate.
validity			
notBefore			
Time			
UTCTime		100101083000Z	01 January 2010, 08:30:00 GMT
notAfter			
Time			
UTCTime		301231083000Z	31 Dec. 2030, 08:30:00 GMT
subject			
Name		{ Always specified – no default }	X.500 Distinguished name of the owner of the certificate.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey		BIT STRING	Contains the subject public key
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
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		NIST-test-policy-1	id-test-certificate-policy-1
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
signatureValue		BIT STRING	Signature calculated

6.1.3 Base End Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the certificate.
validity			
notBefore			
Time			
UTCTime		100101083000Z	01 January 2010, 08:30:00 GMT
notAfter			
Time			
UTCTime		301231083000Z	31 Dec. 2030, 08:30:00 GMT
subject			
Name		{ Always specified – no default }	X.500 Distinguished name of the owner of the certificate.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey		BIT STRING	Contains the subject public key
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
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	FALSE		this extension absent unless otherwise specified
cA		FALSE	
pathLenConstraint		{ Absent }	

keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		1	
dataEncipherment		1	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		No policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		NIST-test-policy-1	id-test-certificate-policy-1
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters			
signatureValue		BIT STRING	Signature calculated

6.1.4 Base CRL

Field	Critical Flag	Value	Comments
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the CRL.
thisUpdate			
Time			
UTCTime		100101083000Z	01 January 2010, 08:30:00 GMT
nextUpdate			
Time			
UTCTime		301231083000Z	31 Dec. 2030, 08:30:00 GMT
revokedCertificates			absent unless otherwise specified
userCertificate			
CertificateSerialNumber			
revocationDate			
Time			
UTCTime		100101083000Z	01 January 2010, 08:30:00 GMT
crlEntryExtensions			
reasonCode	FALSE		
CRLReason		keyCompromise	
crlExtensions			
crlNumber	FALSE	1	
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.11	SHA-256WithRSAEncryption
parameters		NULL	
signatureValue		BIT STRING	signature calculated

6.1.5 Certificate and CRL Test Data

6.1.5.1 Trust Anchor Root Certificate:

base: Base Root Certificate
serial number: 1
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
self-signed

6.1.5.2 Trust Anchor Root CRL:

base: Base CRL
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 104
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Trust Anchor Root Certificate
post to certificateRevocationList

6.1.5.3 Good CA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Good CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.4 Good CA CRL:

base: Base CRL
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 14
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
serialNumber: 15
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Good CA Cert
post to certificateRevocationList

6.1.5.5 Valid Certificate Path Test1 EE:

base: Base End Certificate
serial number: 1

issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.6 Bad Signed CA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Bad Signed CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate (one or more bits in the signature is modified)

6.1.5.7 Bad Signed CA CRL:

base: Base CRL
issuer: "cn=Bad Signed CA, o=Test Certificates 2011, c=US"
signed by Bad Signed CA Cert
post to certificateRevocationList

6.1.5.8 Invalid CA Signature Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Bad Signed CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid CA Signature Test2, o=Test Certificates 2011, c=US"
signed by Bad Signed CA Cert

6.1.5.9 Invalid EE Signature Test3 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid EE Signature Test3, o=Test Certificates 2011, c=US"
signed by Good CA Cert (one or more bits in the signature is modified)

6.1.5.10 Bad notBefore Date CA Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
notBefore: UTC: "470101120100Z"
notAfter: UTC: "490101120100Z"
subject: "cn=Bad notBefore Date CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.11 Bad notBefore Date CA CRL:

base: Base CRL
issuer: "cn=Bad notBefore Date CA, o=Test Certificates 2011, c=US"
signed by Bad notBefore Date CA Cert
post to certificateRevocationList

6.1.5.12 Invalid CA notBefore Date Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Bad notBefore Date CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid CA notBefore Date EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by Bad notBefore Date CA Cert

6.1.5.13 Invalid EE notBefore Date Test2 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notBefore: UTC: "470101120100Z"
notAfter: UTC: "490101120100Z"
subject: "cn=Invalid EE notBefore Date EE Certificate Test2, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.14 Valid pre2000 UTC notBefore Date Test3 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notBefore: UTC: "500101120100Z"
subject: "cn=Valid pre2000 UTC notBefore Date EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.15 Valid GeneralizedTime notBefore Date Test4 EE:

base: Base End Certificate
serial number: 5
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notBefore: GT: "20020101120100Z"
subject: "cn=Valid GeneralizedTime notBefore Date EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.16 Bad notAfter Date CA Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
notAfter: UTC: "110101083000Z"
subject: "cn=Bad notAfter Date CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.17 Bad notAfter Date CA CRL:

base: Base CRL
issuer: "cn=Bad notAfter Date CA, o=Test Certificates 2011, c=US"
signed by Bad notAfter Date CA Cert
post to certificateRevocationList

6.1.5.18 Invalid CA notAfter Date Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Bad notAfter Date CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid CA notAfter Date EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by Bad notAfter Date CA Cert

6.1.5.19 Invalid EE notAfter Date Test6 EE:

base: Base End Certificate
serial number: 6
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notAfter: UTC: "110101083000Z"
subject: "cn=Invalid EE notAfter Date EE Certificate Test6, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.20 Invalid pre2000 UTC EE notAfter Date Test7 EE:

base: Base End Certificate
serial number: 7
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notBefore: GT: "19970101120100Z"
notAfter: UTC: "990101120100Z"
subject: "cn=Invalid pre2000 UTC EE notAfter Date EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.21 Valid GeneralizedTime notAfter Date Test8 EE:

base: Base End Certificate
serial number: 8
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
notAfter: GT: "20500101120100Z"
subject: "cn=Valid GeneralizedTime notAfter Date EE Certificate Test8, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.22 Invalid Name Chaining Test1 EE:

base: Base End Certificate
serial number: 9
issuer: "cn=Good CA Root, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Name Chaining EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.23 Name Ordering CA Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Name Ordering CA, ou=Organizational Unit Name 2, ou=Organizational Unit Name 1, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.24 Name Order CA CRL:

base: Base CRL
issuer: "cn=Name Ordering CA, ou=Organizational Unit Name 2, ou=Organizational Unit Name 1, o=Test Certificates 2011, c=US"
signed by Name Ordering CA Cert
post to certificateRevocationList

6.1.5.25 Invalid Name Chaining Order Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Name Ordering CA, ou=Organizational Unit Name 1, ou=Organizational Unit Name 2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Name Chaining Order EE Certificate Test2, o=Test Certificates 2011, c=US"
signed by Name Ordering CA Cert

6.1.5.26 Valid Name Chaining Whitespace Test3 EE:

base: Base End Certificate
serial number: 11
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Name Chaining Whitespace EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.27 Valid Name Chaining Whitespace Test4 EE:

base: Base End Certificate
serial number: 12
issuer: "cn=\20\20\20Good CA, o=Test Certificates 2011\20\20\20, c=US"
subject: "cn=Valid Name Chaining Whitespace EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.28 Valid Name Chaining Capitalization Test5 EE:

base: Base End Certificate
serial number: 13
issuer: "cn=GOOD CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Name Chaining Capitalization EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.29 UID CA Cert:

base: Base Intermediate Certificate
serial number: 1001
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=UID CA, o=Test Certificates 2011, c=US"
subjectUniqueID: '0010'B
signed by Trust Anchor Root Certificate

6.1.5.30 UID CA CRL:

base: Base CRL
issuer: "cn=UID CA, o=Test Certificates 2011, c=US"
signed by UID CA Cert
post to certificateRevocationList

6.1.5.31 Valid Name UIDs Test6 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=UID CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid UIDs EE Certificate Test6, o=Test Certificates 2011, c=US"
issuerUniqueID: '0010'B
signed by UID CA Cert

6.1.5.32 No CRL CA Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=No CRL CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.33 Invalid Missing CRL Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=No CRL CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Missing CRL EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by No CRL CA Cert

6.1.5.34 Revoked subCA Cert:

base: Base Intermediate Certificate
serial number: 14
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Revoked subCA, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.35 Revoked subCA CRL:

base: Base CRL
issuer: "cn=Revoked subCA, o=Test Certificates 2011, c=US"
signed by Revoked subCA Cert
post to certificateRevocationList

6.1.5.36 Invalid Revoked CA Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Revoked subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Revoked CA Certificate Test2, o=Test Certificates 2011, c=US"
signed by Revoked subCA Cert

6.1.5.37 Invalid Revoked EE Test3 EE:

base: Base End Certificate
serial number: 15
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Revoked EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by Good CA Cert

6.1.5.38 Bad CRL Signature CA Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Bad CRL Signature CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.39 Bad CRL Signature CA CRL:

base: Base CRL
issuer: "cn=Bad CRL Signature CA, o=Test Certificates 2011, c=US"
signed by Bad CRL Signature CA Cert (one or more bits in the signature is modified)
post to certificateRevocationList

6.1.5.40 Invalid Bad CRL Signature Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Bad CRL Signature CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Bad CRL Signature EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by Bad CRL Signature CA Cert

6.1.5.41 Bad CRL Issuer Name CA Cert:

base: Base Intermediate Certificate
serial number: 9
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Bad CRL Issuer Name CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.42 Bad CRL Issuer Name CA CRL:

base: Base CRL
issuer: "cn=Incorrect CRL Issuer Name, o=Test Certificates 2011, c=US"
signed by Bad CRL Issuer Name CA Cert
post to certificateRevocationList at "cn=Bad CRL Issuer Name CA, o=Test Certificates 2011, c=US"

6.1.5.43 Invalid Bad CRL Issuer Name Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Bad CRL Issuer Name CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Bad CRL Issuer Name EE Certificate Test5, o=Test Certificates 2011, c=US"

signed by Bad CRL Issuer Name CA Cert

6.1.5.44 Wrong CRL CA Cert:

base: Base Intermediate Certificate
serial number: 10
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Wrong CRL CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.45 Wrong CRL CA CRL:

base: Base CRL
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 104
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Trust Anchor Root Certificate
post to certificateRevocationList at "cn=Wrong CRL CA, o=Test Certificates 2011, c=US"

6.1.5.46 Invalid Wrong CRL Test6 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Wrong CRL CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Wrong CRL EE Certificate Test6, o=Test Certificates 2011, c=US"
signed by Wrong CRL CA Cert

6.1.5.47 Two CRLs CA Cert:

base: Base Intermediate Certificate
serial number: 11
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Two CRLs CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.48 Two CRLs CA Good CRL:

base: Base CRL
issuer: "cn=Two CRLs CA, o=Test Certificates 2011, c=US"
signed by Two CRLs CA Cert
post to certificateRevocationList

6.1.5.49 Two CRLs CA Bad CRL:

base: Base CRL
issuer: "cn=Bad CRL for Two CRLs CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 1
crlEntryExtensions:
reasonCodeExtension: not critical

reasons:
keyCompromise
signed by Two CRLs CA Cert
post to certificateRevocationList at "cn=Two CRLs CA, o=Test Certificates 2011, c=US"

6.1.5.50 Valid Two CRLs Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Two CRLs CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Two CRLs EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by Two CRLs CA Cert

6.1.5.51 Unknown CRL Entry Extension CA Cert:

base: Base Intermediate Certificate
serial number: 12
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Unknown CRL Entry Extension CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.52 Unknown CRL Entry Extension CA CRL:

base: Base CRL
issuer: "cn=Unknown CRL Entry Extension CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 1
crlEntryExtensions:
privateExtension: critical
privateNumber: 0
signed by Unknown CRL Entry Extension CA Cert
post to certificateRevocationList

6.1.5.53 Invalid Unknown CRL Entry Extension Test8 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Unknown CRL Entry Extension CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Unknown CRL Entry Extension EE Certificate Test8, o=Test Certificates 2011, c=US"
signed by Unknown CRL Entry Extension CA Cert

6.1.5.54 Unknown CRL Extension CA Cert:

base: Base Intermediate Certificate
serial number: 13
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Unknown CRL Extension CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.55 Unknown CRL Extension CA CRL:

base: Base CRL
issuer: "cn=Unknown CRL Extension CA, o=Test Certificates 2011, c=US"

revokedCertificates:
serialNumber: 1
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
crlExtension:
privateExtension: critical
privateNumber: 0
signed by Unknown CRL Extension CA Cert
post to certificateRevocationList

6.1.5.56 Invalid Unknown CRL Extension Test9 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Unknown CRL Extension CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Unknown CRL Extension EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by Unknown CRL Extension CA Cert

6.1.5.57 Invalid Unknown CRL Extension Test10 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Unknown CRL Extension CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Unknown CRL Extension EE Certificate Test10, o=Test Certificates 2011, c=US"
signed by Unknown CRL Extension CA Cert

6.1.5.58 Old CRL nextUpdate CA Cert:

base: Base Intermediate Certificate
serial number: 14
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Old CRL nextUpdate CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.59 Old CRL nextUpdate CA CRL:

base: Base CRL
issuer: "cn=Old CRL nextUpdate CA, o=Test Certificates 2011, c=US"
nextUpdate: UTC: "100102083000Z"
signed by Old CRL nextUpdate CA Cert
post to certificateRevocationList

6.1.5.60 Invalid Old CRL nextUpdate Test11 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Old CRL nextUpdate CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Old CRL nextUpdate EE Certificate Test11, o=Test Certificates 2011, c=US"

signed by Old CRL nextUpdate CA Cert

6.1.5.61 pre2000 CRL nextUpdate CA Cert:

base: Base Intermediate Certificate
serial number: 15
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=pre2000 CRL nextUpdate CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.62 pre2000 CRL nextUpdate CA CRL:

base: Base CRL
issuer: "cn=pre2000 CRL nextUpdate CA, o=Test Certificates 2011, c=US"
thisUpdate: UTC: "980101120100Z"
nextUpdate: UTC: "990101120100Z"
signed by pre2000 CRL nextUpdate CA Cert
post to certificateRevocationList

6.1.5.63 Invalid pre2000 CRL nextUpdate Test12 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pre2000 CRL nextUpdate CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pre2000 CRL nextUpdate EE Certificate Test12, o=Test Certificates 2011, c=US"
signed by pre2000 CRL nextUpdate CA Cert

6.1.5.64 GeneralizedTime CRL nextUpdate CA Cert:

base: Base Intermediate Certificate
serial number: 16
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=GenerizedTime CRL nextUpdate CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.65 GeneralizedTime CRL nextUpdate CA CRL:

base: Base CRL
issuer: "cn=GenerizedTime CRL nextUpdate CA, o=Test Certificates 2011, c=US"
nextUpdate: GT: "20500101120100Z"
signed by GeneralizedTime CRL nextUpdate CA Cert
post to certificateRevocationList

6.1.5.66 Valid GeneralizedTime CRL nextUpdate Test13 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=GenerizedTime CRL nextUpdate CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid GeneralizedTime CRL nextUpdate EE Certificate Test13, o=Test Certificates 2011, c=US"
signed by GeneralizedTime CRL nextUpdate CA Cert

6.1.5.67 Negative Serial Number CA Cert:

base: Base Intermediate Certificate
serial number: 17
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Negative Serial Number CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.68 Negative Serial Number CA CRL:

base: Base CRL
issuer: "cn=Negative Serial Number CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: -1
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Negative Serial Number CA Cert
post to certificateRevocationList

6.1.5.69 Valid Negative Serial Number Test14 EE:

base: Base End Certificate
serial number: 255
issuer: "cn=Negative Serial Number CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Negative Serial Number EE Certificate Test14, o=Test Certificates 2011, c=US"
signed by Negative Serial Number CA Cert

6.1.5.70 Invalid Negative Serial Number Test15 EE:

base: Base End Certificate
serial number: -1
issuer: "cn=Negative Serial Number CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Negative Serial Number EE Certificate Test15, o=Test Certificates 2011, c=US"
signed by Negative Serial Number CA Cert

6.1.5.71 Long Serial Number CA Cert:

base: Base Intermediate Certificate
serial number: 18
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Long Serial Number CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.72 Long Serial Number CA CRL:

base: Base CRL
issuer: "cn=Long Serial Number CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 0x7F0102030405060708090A0B0C0D0E0F10111213
crlEntryExtensions:

reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Long Serial Number CA Cert
post to certificateRevocationList

6.1.5.73 Valid Long Serial Number Test16 EE:

base: Base End Certificate
serial number: 0x7F0102030405060708090A0B0C0D0E0F10111212
issuer: "cn=Long Serial Number CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Long Serial Number EE Certificate Test16, o=Test Certificates 2011, c=US"
signed by Long Serial Number CA Cert

6.1.5.74 Valid Long Serial Number Test17 EE:

base: Base End Certificate
serial number: 0x7E0102030405060708090A0B0C0D0E0F10111213
issuer: "cn=Long Serial Number CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Long Serial Number EE Certificate Test17, o=Test Certificates 2011, c=US"
signed by Long Serial Number CA Cert

6.1.5.75 Invalid Long Serial Number Test18 EE:

base: Base End Certificate
serial number: 0x7F0102030405060708090A0B0C0D0E0F10111213
issuer: "cn=Long Serial Number CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Long Serial Number EE Certificate Test18, o=Test Certificates 2011, c=US"
signed by Long Serial Number CA Cert

6.1.5.76 Basic Self-Issued New Key CA Cert:

base: Base Intermediate Certificate
serial number: 19
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.77 Basic Self-Issued New Key CA CRL:

base: Base CRL
issuer: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic Self-Issued New Key CA Cert
post to certificateRevocationList

6.1.5.78 Basic Self-Issued New Key OldWithNew CA Cert:

base: Base Intermediate Certificate

serial number: 1
issuer: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued New Key CA Cert

6.1.5.79 Valid Basic Self-Issued Old With New Test1 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Basic Self-Issued Old With New EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued New Key OldWithNew CA Cert

6.1.5.80 Invalid Basic Self-Issued Old With New Test2 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Self-Issued New Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Basic Self-Issued Old With New EE Certificate Test2, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued New Key OldWithNew CA Cert

6.1.5.81 Basic Self-Issued Old Key CA Cert:

base: Base Intermediate Certificate
serial number: 20
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.82 Basic Self-Issued Old Key Self-Issued Cert CRL:

base: Base CRL
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=Self-Issued Cert DP for Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued Old Key CA Cert
post to certificateRevocationList at "cn=Self-Issued Cert DP for Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"

6.1.5.83 Basic Self-Issued Old Key NewWithOld CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
directoryName: "cn=Self-Issued Cert DP for Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued Old Key CA Cert

6.1.5.84 Basic Self-Issued Old Key CA CRL:

base: Base CRL
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 4
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic Self-Issued Old Key NewWithOld CA Cert
post to certificateRevocationList

6.1.5.85 Valid Basic Self-Issued New With Old Test3 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Basic Self-Issued New With Old EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued Old Key NewWithOld CA Cert

6.1.5.86 Valid Basic Self-Issued New With Old Test4 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Basic Self-Issued New With Old EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued Old Key CA Cert

6.1.5.87 Invalid Basic Self-Issued New With Old Test5 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=Basic Self-Issued Old Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Basic Self-Issued New With Old EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued Old Key CA Cert

6.1.5.88 Basic Self-Issued CRL Signing Key CA Cert:

base: Base Intermediate Certificate
serial number: 21
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.89 Basic Self-Issued CRL Signing Key CRL Cert CRL:

base: Base CRL
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=Self-Issued Cert DP for Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued CRL Signing Key CA Cert
post to certificateRevocationList at "cn=Self-Issued Cert DP for Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"

6.1.5.90 Basic Self-Issued CRL Signing Key CRL Cert:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: True
digitalSignature: False
nonRepudiation: False
keyEncipherment: False
dataEncipherment: False
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=Self-Issued Cert DP for Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued CRL Signing Key CA Cert

6.1.5.91 Basic Self-Issued CRL Signing Key CA CRL:

base: Base CRL
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic Self-Issued CRL Signing Key CRL Cert
post to certificateRevocationList

6.1.5.92 Valid Basic Self-Issued CRL Signing Key Test6 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Basic Self-Issued CRL Signing Key EE Certificate Test6, o=Test Certificates 2011, c=US"

signed by Basic Self-Issued CRL Signing Key CA Cert

6.1.5.93 Invalid Basic Self-Issued CRL Signing Key Test7 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Basic Self-Issued CRL Signing Key EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued CRL Signing Key CA Cert

6.1.5.94 Invalid Basic Self-Issued CRL Signing Key Test8 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=Basic Self-Issued CRL Signing Key CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Basic Self-Issued CRL Signing Key EE Certificate Test8, o=Test Certificates 2011, c=US"
signed by Basic Self-Issued CRL Signing Key CRL Cert

6.1.5.95 Missing basicConstraints CA Cert:

base: Base Intermediate Certificate
serial number: 22
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Missing basicConstraints CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: absent
signed by Trust Anchor Root Certificate

6.1.5.96 Missing basicConstraints CA CRL:

base: Base CRL
issuer: "cn=Missing basicConstraints CA, o=Test Certificates 2011, c=US"
signed by Missing basicConstraints CA Cert
post to certificateRevocationList

6.1.5.97 Invalid Missing basicConstraints Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Missing basicConstraints CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Missing basicConstraints EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by Missing basicConstraints CA Cert

6.1.5.98 basicConstraints Critical cA False CA Cert:

base: Base Intermediate Certificate
serial number: 23
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=basicConstraints Critical cA False CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: FALSE
signed by Trust Anchor Root Certificate

6.1.5.99 basicConstraints Critical cA False CA CRL:

base: Base CRL
issuer: "cn=basicConstraints Critical cA False CA, o=Test Certificates 2011, c=US"
signed by basicConstraints Critical cA False CA Cert
post to certificateRevocationList

6.1.5.100 Invalid cA False Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=basicConstraints Critical cA False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cA False EE Certificate Test2, o=Test Certificates 2011, c=US"
signed by basicConstraints Critical cA False CA Cert

6.1.5.101 basicConstraints Not Critical cA False CA Cert:

base: Base Intermediate Certificate
serial number: 24
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=basicConstraints Not Critical cA False CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: not critical
cA: FALSE
signed by Trust Anchor Root Certificate

6.1.5.102 basicConstraints Not Critical cA False CA CRL:

base: Base CRL
issuer: "cn=basicConstraints Not Critical cA False CA, o=Test Certificates 2011, c=US"
signed by basicConstraints Not Critical cA False CA Cert
post to certificateRevocationList

6.1.5.103 Invalid cA False Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=basicConstraints Not Critical cA False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cA False EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by basicConstraints Not Critical cA False CA Cert

6.1.5.104 basicConstraints Not Critical CA Cert:

base: Base Intermediate Certificate
serial number: 25
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=basicConstraints Not Critical CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: not critical
cA: TRUE
signed by Trust Anchor Root Certificate

6.1.5.105 basicConstraints Not Critical CA CRL:

base: Base CRL
issuer: "cn=basicConstraints Not Critical CA, o=Test Certificates 2011, c=US"

signed by basicConstraints Not Critical CA Cert
post to certificateRevocationList

6.1.5.106 Valid basicConstraints Not Critical Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=basicConstraints Not Critical CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid basicConstraints Not Critical EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by basicConstraints Not Critical CA Cert

6.1.5.107 pathLenConstraint0 CA Cert:

base: Base Intermediate Certificate
serial number: 26
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 0

signed by Trust Anchor Root Certificate

6.1.5.108 pathLenConstraint0 CA CRL:

base: Base CRL
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 CA Cert
post to certificateRevocationList

6.1.5.109 pathLenConstraint0 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint0 subCA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 CA Cert

6.1.5.110 pathLenConstraint0 subCA CRL:

base: Base CRL
issuer: "cn=pathLenConstraint0 subCA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 subCA Cert
post to certificateRevocationList

6.1.5.111 Invalid pathLenConstraint Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pathLenConstraint0 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 subCA Cert

6.1.5.112 Invalid pathLenConstraint Test6 EE:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint0 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test6, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by pathLenConstraint0 subCA Cert

6.1.5.113 Valid pathLenConstraint Test7 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid pathLenConstraint EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 CA Cert

6.1.5.114 Valid pathLenConstraint Test8 EE:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid pathLenConstraint EE Certificate Test8, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by pathLenConstraint0 CA Cert

6.1.5.115 pathLenConstraint6 CA Cert:

base: Base Intermediate Certificate
serial number: 27
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 6

signed by Trust Anchor Root Certificate

6.1.5.116 pathLenConstraint6 CA CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 CA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 CA Cert
post to certificateRevocationList

6.1.5.117 pathLenConstraint6 subCA0 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subCA0, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 0

signed by pathLenConstraint6 CA Cert

6.1.5.118 pathLenConstraint6 subCA0 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subCA0, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subCA0 Cert
post to certificateRevocationList

6.1.5.119 pathLenConstraint6 subsubCA00 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subCA0, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subsubCA00, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 0

signed by pathLenConstraint6 subCA0 Cert

6.1.5.120 pathLenConstraint6 subsubCA00 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subsubCA00, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA00 Cert
post to certificateRevocationList

6.1.5.121 Invalid pathLenConstraint Test9 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subsubCA00, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA00 Cert

6.1.5.122 Invalid pathLenConstraint Test10 EE:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint6 subsubCA00, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test10, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True

keyEncipherment: True
dataEncipherment: True
signed by pathLenConstraint6 subsubCA00 Cert

6.1.5.123 pathLenConstraint6 subCA1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint6 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subCA1, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 1

signed by pathLenConstraint6 CA Cert

6.1.5.124 pathLenConstraint6 subCA1 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subCA1, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subCA1 Cert
post to certificateRevocationList

6.1.5.125 pathLenConstraint6 subsubCA11 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subCA1, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subsubCA11, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 1

signed by pathLenConstraint6 subCA1 Cert

6.1.5.126 pathLenConstraint6 subsubCA11 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subsubCA11, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA11 Cert
post to certificateRevocationList

6.1.5.127 pathLenConstraint6 subsubsubCA11X Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subsubCA11, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subsubsubCA11X, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA11 Cert

6.1.5.128 pathLenConstraint6 subsubsubCA11X CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subsubsubCA11X, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubsubCA11X Cert

post to certificateRevocationList

6.1.5.129 Invalid pathLenConstraint Test11 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subsubsubCA11X, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test11, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubsubCA11X Cert

6.1.5.130 Invalid pathLenConstraint Test12 EE:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint6 subsubsubCA11X, o=Test Certificates 2011, c=US"
subject: "cn=Invalid pathLenConstraint EE Certificate Test12, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by pathLenConstraint6 subsubsubCA11X Cert

6.1.5.131 pathLenConstraint6 subCA4 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=pathLenConstraint6 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subCA4, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 4

signed by pathLenConstraint6 CA Cert

6.1.5.132 pathLenConstraint6 subCA4 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subCA4, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subCA4 Cert
post to certificateRevocationList

6.1.5.133 pathLenConstraint6 subsubCA41 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subCA4, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subsubCA41, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 1

signed by pathLenConstraint6 subCA4 Cert

6.1.5.134 pathLenConstraint6 subsubCA41 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subsubCA41, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA41 Cert
post to certificateRevocationList

6.1.5.135 pathLenConstraint6 subsubsubCA41X Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subsubCA41, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint6 subsubsubCA41X, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubCA41 Cert

6.1.5.136 pathLenConstraint6 subsubsubCA41X CRL:

base: Base CRL
issuer: "cn=pathLenConstraint6 subsubsubCA41X, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubsubCA41X Cert
post to certificateRevocationList

6.1.5.137 Valid pathLenConstraint Test13 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pathLenConstraint6 subsubsubCA41X, o=Test Certificates 2011, c=US"
subject: "cn=Valid pathLenConstraint EE Certificate Test13, o=Test Certificates 2011, c=US"
signed by pathLenConstraint6 subsubsubCA41X Cert

6.1.5.138 Valid pathLenConstraint Test14 EE:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint6 subsubsubCA41X, o=Test Certificates 2011, c=US"
subject: "cn=Valid pathLenConstraint EE Certificate Test14, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by pathLenConstraint6 subsubsubCA41X Cert

6.1.5.139 pathLenConstraint0 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 CA Cert

6.1.5.140 Valid Self-Issued pathLenConstraint Test15 EE:

base: Base End Certificate

serial number: 5
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued pathLenConstraint EE Certificate Test15, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 Self-Issued CA Cert

6.1.5.141 pathLenConstraint0 subCA2 Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "cn=pathLenConstraint0 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint0 subCA2, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 Self-Issued CA Cert

6.1.5.142 pathLenConstraint0 subCA2 CRL:

base: Base CRL
issuer: "cn=pathLenConstraint0 subCA2, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 subCA2 Cert
post to certificateRevocationList

6.1.5.143 Invalid Self-Issued pathLenConstraint Test16 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=pathLenConstraint0 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued pathLenConstraint EE Certificate Test16, o=Test Certificates 2011, c=US"
signed by pathLenConstraint0 subCA2 Cert

6.1.5.144 pathLenConstraint1 CA Cert:

base: Base Intermediate Certificate
serial number: 28
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint1 CA, o=Test Certificates 2011, c=US"
basicConstraintsExtension: critical
cA: TRUE
pathLenConstraint: 1

signed by Trust Anchor Root Certificate

6.1.5.145 pathLenConstraint1 CA CRL:

base: Base CRL
issuer: "cn=pathLenConstraint1 CA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 CA Cert
post to certificateRevocationList

6.1.5.146 pathLenConstraint1 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint1 CA, o=Test Certificates 2011, c=US"

subject: "cn=pathLenConstraint1 CA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 CA Cert

6.1.5.147 pathLenConstraint1 subCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=pathLenConstraint1 CA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint1 subCA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 Self-Issued CA Cert

6.1.5.148 pathLenConstraint1 subCA CRL:

base: Base CRL
issuer: "cn=pathLenConstraint1 subCA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 subCA Cert
post to certificateRevocationList

6.1.5.149 pathLenConstraint1 Self-Issued subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=pathLenConstraint1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=pathLenConstraint1 subCA, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 subCA Cert

6.1.5.150 Valid Self-Issued pathLenConstraint Test17 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=pathLenConstraint1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued pathLenConstraint EE Certificate Test17, o=Test Certificates 2011, c=US"
signed by pathLenConstraint1 Self-Issued subCA Cert

6.1.5.151 keyUsage Critical keyCertSign False CA Cert:

base: Base Intermediate Certificate
serial number: 29
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=keyUsage Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
keyCertSign: False
signed by Trust Anchor Root Certificate

6.1.5.152 keyUsage Critical keyCertSign False CA CRL:

base: Base CRL
issuer: "cn=keyUsage Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
signed by keyUsage Critical keyCertSign False CA Cert
post to certificateRevocationList

6.1.5.153 Invalid keyUsage Critical keyCertSign False Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=keyUsage Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid keyUsage Critical keyCertSign False EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by keyUsage Critical keyCertSign False CA Cert

6.1.5.154 keyUsage Not Critical keyCertSign False CA Cert:

base: Base Intermediate Certificate
serial number: 30
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=keyUsage Not Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
keyUsageExtension: not critical
keyCertSign: False
signed by Trust Anchor Root Certificate

6.1.5.155 keyUsage Not Critical keyCertSign False CA CRL:

base: Base CRL
issuer: "cn=keyUsage Not Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical keyCertSign False CA Cert
post to certificateRevocationList

6.1.5.156 Invalid keyUsage Not Critical keyCertSign False Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=keyUsage Not Critical keyCertSign False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid keyUsage Not Critical keyCertSign False EE Cert Test2, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical keyCertSign False CA Cert

6.1.5.157 keyUsage Not Critical CA Cert:

base: Base Intermediate Certificate
serial number: 31
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=keyUsage Not Critical CA, o=Test Certificates 2011, c=US"
keyUsageExtension: not critical
keyCertSign: True
signed by Trust Anchor Root Certificate

6.1.5.158 keyUsage Not Critical CA CRL:

base: Base CRL
issuer: "cn=keyUsage Not Critical CA, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical CA Cert
post to certificateRevocationList

6.1.5.159 Valid keyUsage Not Critical Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=keyUsage Not Critical CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid keyUsage Not Critical EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical CA Cert

6.1.5.160 keyUsage Critical cRLSign False CA Cert:

base: Base Intermediate Certificate
serial number: 32
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=keyUsage Critical cRLSign False CA, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.161 keyUsage Critical cRLSign False CA CRL:

base: Base CRL
issuer: "cn=keyUsage Critical cRLSign False CA, o=Test Certificates 2011, c=US"
signed by keyUsage Critical cRLSign False CA Cert
post to certificateRevocationList

6.1.5.162 Invalid keyUsage Critical cRLSign False Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=keyUsage Critical cRLSign False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid keyUsage Critical cRLSign False EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by keyUsage Critical cRLSign False CA Cert

6.1.5.163 keyUsage Not Critical cRLSign False CA Cert:

base: Base Intermediate Certificate
serial number: 33
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=keyUsage Not Critical cRLSign False CA, o=Test Certificates 2011, c=US"
keyUsageExtension: not critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.164 keyUsage Not Critical cRLSign False CA CRL:

base: Base CRL
issuer: "cn=keyUsage Not Critical cRLSign False CA, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical cRLSign False CA Cert
post to certificateRevocationList

6.1.5.165 Invalid keyUsage Not Critical cRLSign False Test5 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=keyUsage Not Critical cRLSign False CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid keyUsage Not Critical cRLSign False EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by keyUsage Not Critical cRLSign False CA Cert

6.1.5.166 No Policies CA Cert:

base: Base Intermediate Certificate
serial number: 34
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=No Policies CA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by Trust Anchor Root Certificate

6.1.5.167 No Policies CA CRL:

base: Base CRL
issuer: "cn=No Policies CA, o=Test Certificates 2011, c=US"
signed by No Policies CA Cert
post to certificateRevocationList

6.1.5.168 All Certificates No Policies Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=No Policies CA, o=Test Certificates 2011, c=US"
subject: "cn=All Certificates No Policies EE Certificate Test2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by No Policies CA Cert

6.1.5.169 Policies P2 subCA Cert:

base: Base Intermediate Certificate
serial number: 16
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Policies P2 subCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Good CA Cert

6.1.5.170 Policies P2 subCA CRL:

base: Base CRL
issuer: "cn=Policies P2 subCA, o=Test Certificates 2011, c=US"
signed by Policies P2 subCA Cert
post to certificateRevocationList

6.1.5.171 Different Policies Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Policies P2 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test3, o=Test Certificates 2011, c=US"

certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Policies P2 subCA Cert

6.1.5.172 Good subCA Cert:

base: Base Intermediate Certificate
serial number: 17
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Good subCA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
signed by Good CA Cert

6.1.5.173 Good subCA CRL:

base: Base CRL
issuer: "cn=Good subCA, o=Test Certificates 2011, c=US"
signed by Good subCA Cert
post to certificateRevocationList

6.1.5.174 Different Policies Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Good subCA, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test4, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Good subCA Cert

6.1.5.175 Policies P2 subCA2 Cert:

base: Base Intermediate Certificate
serial number: 18
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Policies P2 subCA2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
signed by Good CA Cert

6.1.5.176 Policies P2 subCA2 CRL:

base: Base CRL
issuer: "cn=Policies P2 subCA2, o=Test Certificates 2011, c=US"
signed by Policies P2 subCA2 Cert
post to certificateRevocationList

6.1.5.177 Different Policies Test5 EE:

base: Base End Certificate
serial number: 1

issuer: "cn=Policies P2 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test5, o=Test Certificates 2011, c=US"
signed by Policies P2 subCA2 Cert

6.1.5.178 Policies P1234 CA Cert:

base: Base Intermediate Certificate
serial number: 35
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Policies P1234 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
"2.16.840.1.101.3.2.1.48.4"
signed by Trust Anchor Root Certificate

6.1.5.179 Policies P1234 CA CRL:

base: Base CRL
issuer: "cn=Policies P1234 CA, o=Test Certificates 2011, c=US"
signed by Policies P1234 CA Cert
post to certificateRevocationList

6.1.5.180 Policies P1234 subCAP123 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P1234 CA, o=Test Certificates 2011, c=US"
subject: "cn=Policies P1234 subCAP123, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
signed by Policies P1234 CA Cert

6.1.5.181 Policies P1234 subCAP123 CRL:

base: Base CRL
issuer: "cn=Policies P1234 subCAP123, o=Test Certificates 2011, c=US"
signed by Policies P1234 subCAP123 Cert
post to certificateRevocationList

6.1.5.182 Policies P1234 subsubCAP123P12 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P1234 subCAP123, o=Test Certificates 2011, c=US"
subject: "cn=Policies P1234 subsubCAP123P12, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"

"2.16.840.1.101.3.2.1.48.2"
signed by Policies P1234 subCAP123 Cert

6.1.5.183 Policies P1234 subsubCAP123P12 CRL:

base: Base CRL
issuer: "cn=Policies P1234 subsubCAP123P12, o=Test Certificates 2011, c=US"
signed by Policies P1234 subsubCAP123P12 Cert
post to certificateRevocationList

6.1.5.184 Overlapping Policies Test6 EE:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P1234 subsubCAP123P12, o=Test Certificates 2011, c=US"
subject: "cn=Overlapping Policies EE Certificate Test6, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by Policies P1234 subsubCAP123P12 Cert

6.1.5.185 Policies P123 CA Cert:

base: Base Intermediate Certificate
serial number: 36
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Policies P123 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
signed by Trust Anchor Root Certificate

6.1.5.186 Policies P123 CA CRL:

base: Base CRL
issuer: "cn=Policies P123 CA, o=Test Certificates 2011, c=US"
signed by Policies P123 CA Cert
post to certificateRevocationList

6.1.5.187 Policies P123 subCAP12 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P123 CA, o=Test Certificates 2011, c=US"
subject: "cn=Policies P123 subCAP12, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"

signed by Policies P123 CA Cert

6.1.5.188 Policies P123 subCAP12 CRL:

base: Base CRL
issuer: "cn=Policies P123 subCAP12, o=Test Certificates 2011, c=US"
signed by Policies P123 subCAP12 Cert
post to certificateRevocationList

6.1.5.189 Policies P123 subsubCAP12P1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P123 subCAP12, o=Test Certificates 2011, c=US"
subject: "cn=Policies P123 subsubCAP12P1, o=Test Certificates 2011, c=US"
signed by Policies P123 subCAP12 Cert

6.1.5.190 Policies P123 subsubCAP12P1 CRL:

base: Base CRL
issuer: "cn=Policies P123 subsubCAP12P1, o=Test Certificates 2011, c=US"
signed by Policies P123 subsubCAP12P1 Cert
post to certificateRevocationList

6.1.5.191 Different Policies Test7 EE:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P123 subsubCAP12P1, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test7, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by Policies P123 subsubCAP12P1 Cert

6.1.5.192 Policies P12 CA Cert:

base: Base Intermediate Certificate
serial number: 37
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Policies P12 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
signed by Trust Anchor Root Certificate

6.1.5.193 Policies P12 CA CRL:

base: Base CRL
issuer: "cn=Policies P12 CA, o=Test Certificates 2011, c=US"
signed by Policies P12 CA Cert
post to certificateRevocationList

6.1.5.194 Policies P12 subCAP1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P12 CA, o=Test Certificates 2011, c=US"
subject: "cn=Policies P12 subCAP1, o=Test Certificates 2011, c=US"
signed by Policies P12 CA Cert

6.1.5.195 Policies P12 subCAP1 CRL:

base: Base CRL
issuer: "cn=Policies P12 subCAP1, o=Test Certificates 2011, c=US"
signed by Policies P12 subCAP1 Cert
post to certificateRevocationList

6.1.5.196 Policies P12 subsubCAP1P2 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P12 subCAP1, o=Test Certificates 2011, c=US"
subject: "cn=Policies P12 subsubCAP1P2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Policies P12 subCAP1 Cert

6.1.5.197 Policies P12 subsubCAP1P2 CRL:

base: Base CRL
issuer: "cn=Policies P12 subsubCAP1P2, o=Test Certificates 2011, c=US"
signed by Policies P12 subsubCAP1P2 Cert
post to certificateRevocationList

6.1.5.198 Different Policies Test8 EE:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P12 subsubCAP1P2, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test8, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by Policies P12 subsubCAP1P2 Cert

6.1.5.199 Policies P123 subsubCAP12P2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Policies P123 subCAP12, o=Test Certificates 2011, c=US"
subject: "cn=Policies P123 subsubCAP12P2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Policies P123 subCAP12 Cert

6.1.5.200 Policies P123 subsubCAP2P2 CRL:

base: Base CRL
issuer: "cn=Policies P123 subsubCAP12P2, o=Test Certificates 2011, c=US"
signed by Policies P123 subsubCAP12P2 Cert
post to certificateRevocationList

6.1.5.201 Policies P123 subsubsubCAP12P2P1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Policies P123 subsubCAP12P2, o=Test Certificates 2011, c=US"
subject: "cn=Policies P123 subsubsubCAP12P2P1, o=Test Certificates 2011, c=US"
signed by Policies P123 subsubCAP12P2 Cert

6.1.5.202 Policies P123 subsubsubCAP12P2P1 CRL:

base: Base CRL
issuer: "cn=Policies P123 subsubsubCAP12P2P1, o=Test Certificates 2011, c=US"
signed by Policies P123 subsubsubCAP12P2P1 Cert
post to certificateRevocationList

6.1.5.203 Different Policies Test9 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Policies P123 subsubsubCAP12P2P1, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by Policies P123 subsubsubCAP12P2P1 Cert

6.1.5.204 All Certificates Same Policies Test10 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Policies P12 CA, o=Test Certificates 2011, c=US"
subject: "cn=All Certificates Same Policies EE Certificate Test10, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
signed by Policies P12 CA Cert

6.1.5.205 anyPolicy CA Cert:

base: Base Intermediate Certificate
serial number: 38
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=anyPolicy CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by Trust Anchor Root Certificate

6.1.5.206 anyPolicy CA CRL:

base: Base CRL
issuer: "cn=anyPolicy CA, o=Test Certificates 2011, c=US"
signed by anyPolicy CA Cert
post to certificateRevocationList

6.1.5.207 All Certificates anyPolicy Test11 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=anyPolicy CA, o=Test Certificates 2011, c=US"
subject: "cn=All Certificates anyPolicy EE Certificate Test11, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by anyPolicy CA Cert

6.1.5.208 Policies P3 CA Cert:

base: Base Intermediate Certificate
serial number: 39
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Policies P3 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
signed by Trust Anchor Root Certificate

6.1.5.209 Policies P3 CA CRL:

base: Base CRL
issuer: "cn=Policies P3 CA, o=Test Certificates 2011, c=US"
signed by Policies P3 CA Cert
post to certificateRevocationList

6.1.5.210 Different Policies Test12 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Policies P3 CA, o=Test Certificates 2011, c=US"
subject: "cn=Different Policies EE Certificate Test12, o=Test Certificates 2011, c=US"

certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.4"
signed by Policies P3 CA Cert

6.1.5.211 All Certificates Same Policies Test13 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Policies P123 CA, o=Test Certificates 2011, c=US"
subject: "cn=All Certificates Same Policies EE Certificate Test13, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
signed by Policies P123 CA Cert

6.1.5.212 AnyPolicy Test14 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=anyPolicy CA, o=Test Certificates 2011, c=US"
subject: "cn=anyPolicy EE Certificate Test14, o=Test Certificates 2011, c=US"
signed by anyPolicy CA Cert

6.1.5.213 User Notice Qualifier Test15 EE:

base: Base End Certificate
serial number: 40
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=User Notice Qualifier EE Certificate Test15, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q1: This is the user notice from qualifier 1. This certificate is for test purposes only."
signed by Trust Anchor Root Certificate

6.1.5.214 User Notice Qualifier Test16 EE:

base: Base End Certificate
serial number: 19
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=User Notice Qualifier EE Certificate Test16, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q1: This is the user notice from qualifier 1. This certificate is for test purposes only."

"2.16.840.1.101.3.2.1.48.2"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q2: This is the user notice from qualifier 2. This user notice should not be displayed."
signed by Good CA Cert

6.1.5.215 User Notice Qualifier Test17 EE:

base: Base End Certificate
serial number: 20
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=User Notice Qualifier EE Certificate Test17, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q3: This is the user notice from qualifier 3. This certificate is for test purposes only."
signed by Good CA Cert

6.1.5.216 User Notice Qualifier Test18 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Policies P12 CA, o=Test Certificates 2011, c=US"
subject: "cn=User Notice Qualifier EE Certificate Test18, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q4: This is the user notice from qualifier 4 associated with NIST-test-policy-1. This certificate is for test purposes only."
"2.5.29.32.0"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q5: This is the user notice from qualifier 5 associated with anyPolicy. This user notice should be associated with NIST-test-policy-2."
signed by Policies P12 CA Cert

6.1.5.217 User Notice Qualifier Test19 EE:

base: Base End Certificate
serial number: 41
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=User Notice Qualifier EE Certificate Test19, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical

"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q6: Section 4.2.1.5 of RFC 3280 states the maximum size of explicitText is 200 characters, but warns that some non-conforming CAs exceed this limit. Thus RFC 3280 states that certificate users SHOULD gracefully handle explicitText with more than 200 characters. This explicitText is over 200 characters long."
signed by Trust Anchor Root Certificate

6.1.5.218 CPS Pointer Qualifier Test20 EE:

base: Base End Certificate
serial number: 21
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=CPS Pointer Qualifier EE Certificate Test20, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.1
CPSuri: "http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/pki_registration.html#PKITest"
signed by Good CA Cert

6.1.5.219 requireExplicitPolicy10 CA Cert:

base: Base Intermediate Certificate
serial number: 42
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy10 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 10
signed by Trust Anchor Root Certificate

6.1.5.220 requireExplicitPolicy10 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy10 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 CA Cert
post to certificateRevocationList

6.1.5.221 requireExplicitPolicy10 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy10 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy10 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 CA Cert

6.1.5.222 requireExplicitPolicy10 subCA CRL:

base: Base CRL

issuer: "cn=requireExplicitPolicy10 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 subCA Cert
post to certificateRevocationList

6.1.5.223 requireExplicitPolicy10 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy10 subCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy10 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 subCA Cert

6.1.5.224 requireExplicitPolicy10 subsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy10 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 subsubCA Cert
post to certificateRevocationList

6.1.5.225 requireExplicitPolicy10 subsubsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy10 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy10 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 subsubCA Cert

6.1.5.226 requireExplicitPolicy10 subsubsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy10 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy10 subsubsubCA Cert
post to certificateRevocationList

6.1.5.227 Valid requireExplicitPolicy Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy10 subsubsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid requireExplicitPolicy EE Certificate Test1, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy10 subsubsubCA Cert

6.1.5.228 requireExplicitPolicy5 CA Cert:

base: Base Intermediate Certificate
serial number: 43
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy5 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 5
signed by Trust Anchor Root Certificate

6.1.5.229 requireExplicitPolicy5 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy5 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 CA Cert
post to certificateRevocationList

6.1.5.230 requireExplicitPolicy5 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy5 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy5 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 CA Cert

6.1.5.231 requireExplicitPolicy5 subCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy5 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 subCA Cert
post to certificateRevocationList

6.1.5.232 requireExplicitPolicy5 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy5 subCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy5 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 subCA Cert

6.1.5.233 requireExplicitPolicy5 subsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy5 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 subsubCA Cert
post to certificateRevocationList

6.1.5.234 requireExplicitPolicy5 subsubsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy5 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy5 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 subsubCA Cert

6.1.5.235 requireExplicitPolicy5 subsubsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy5 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy5 subsubsubCA Cert
post to certificateRevocationList

6.1.5.236 Valid requireExplicitPolicy Test2 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=requireExplicitPolicy5 subsubsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid requireExplicitPolicy EE Certificate Test2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy5 subsubsubCA Cert

6.1.5.237 requireExplicitPolicy4 CA Cert:

base: Base Intermediate Certificate
serial number: 44
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy4 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 4
signed by Trust Anchor Root Certificate

6.1.5.238 requireExplicitPolicy4 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy4 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 CA Cert
post to certificateRevocationList

6.1.5.239 requireExplicitPolicy4 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy4 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy4 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 CA Cert

6.1.5.240 requireExplicitPolicy4 subCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy4 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 subCA Cert
post to certificateRevocationList

6.1.5.241 requireExplicitPolicy4 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy4 subCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy4 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 subCA Cert

6.1.5.242 requireExplicitPolicy4 subsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy4 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 subsubCA Cert
post to certificateRevocationList

6.1.5.243 requireExplicitPolicy4 subsubsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy4 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy4 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 subsubCA Cert

6.1.5.244 requireExplicitPolicy4 subsubsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy4 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy4 subsubsubCA Cert
post to certificateRevocationList

6.1.5.245 Invalid requireExplicitPolicy Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy4 subsubsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid requireExplicitPolicy EE Certificate Test3, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy4 subsubsubCA Cert

6.1.5.246 requireExplicitPolicy0 CA Cert:

base: Base Intermediate Certificate
serial number: 45
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy0 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
signed by Trust Anchor Root Certificate

6.1.5.247 requireExplicitPolicy0 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy0 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 CA Cert
post to certificateRevocationList

6.1.5.248 requireExplicitPolicy0 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy0 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy0 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 CA Cert

6.1.5.249 requireExplicitPolicy0 subCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy0 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subCA Cert

post to certificateRevocationList

6.1.5.250 requireExplicitPolicy0 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy0 subCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy0 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subCA Cert

6.1.5.251 requireExplicitPolicy0 subsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy0 subsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subsubCA Cert
post to certificateRevocationList

6.1.5.252 requireExplicitPolicy0 subsubsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy0 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy0 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subsubCA Cert

6.1.5.253 requireExplicitPolicy0 subsubsubCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy0 subsubsubCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subsubsubCA Cert
post to certificateRevocationList

6.1.5.254 Valid requireExplicitPolicy Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy0 subsubsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid requireExplicitPolicy EE Certificate Test4, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy0 subsubsubCA Cert

6.1.5.255 requireExplicitPolicy7 CA Cert:

base: Base Intermediate Certificate
serial number: 46
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy7 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 7
signed by Trust Anchor Root Certificate

6.1.5.256 requireExplicitPolicy7 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy7 CA, o=Test Certificates 2011, c=US"

signed by requireExplicitPolicy7 CA Cert
post to certificateRevocationList

6.1.5.257 requireExplicitPolicy7 subCARE2 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy7 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy7 subCARE2, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 2
signed by requireExplicitPolicy7 CA Cert

6.1.5.258 requireExplicitPolicy7 subCARE2 CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy7 subCARE2, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy7 subCARE2 Cert
post to certificateRevocationList

6.1.5.259 requireExplicitPolicy7 subsubCARE2RE4 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy7 subCARE2, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy7 subsubCARE2RE4, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 4
signed by requireExplicitPolicy7 subCARE2 Cert

6.1.5.260 requireExplicitPolicy7 subsubCARE2RE4 CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy7 subsubCARE2RE4, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy7 subsubCARE2RE4 Cert
post to certificateRevocationList

6.1.5.261 requireExplicitPolicy7 subsubsubCARE2RE4 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy7 subsubCARE2RE4, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy7 subsubsubCARE2RE4, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy7 subsubCARE2RE4 Cert

6.1.5.262 requireExplicitPolicy7 subsubsubCARE2RE4 CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy7 subsubsubCARE2RE4, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy7 subsubsubCARE2RE4 Cert
post to certificateRevocationList

6.1.5.263 Invalid requireExplicitPolicy Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy7 subsubsubCARE2RE4, o=Test Certificates 2011, c=US"
subject: "cn=Invalid requireExplicitPolicy EE Certificate Test5, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy7 subsubsubCARE2RE4 Cert

6.1.5.264 requireExplicitPolicy2 CA Cert:

base: Base Intermediate Certificate
serial number: 47
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 2
signed by Trust Anchor Root Certificate

6.1.5.265 requireExplicitPolicy2 CA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy2 CA Cert
post to certificateRevocationList

6.1.5.266 requireExplicitPolicy2 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy2 CA Cert

6.1.5.267 Valid Self-Issued requireExplicitPolicy Test6 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued requireExplicitPolicy EE Certificate Test6, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy2 Self-Issued CA Cert

6.1.5.268 requireExplicitPolicy2 subCA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=requireExplicitPolicy2 CA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy2 Self-Issued CA Cert

6.1.5.269 requireExplicitPolicy2 subCA CRL:

base: Base CRL
issuer: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy2 subCA Cert
post to certificateRevocationList

6.1.5.270 Invalid Self-Issued requireExplicitPolicy Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued requireExplicitPolicy EE Certificate Test7, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy2 subCA Cert

6.1.5.271 requireExplicitPolicy2 Self-Issued subCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
subject: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
signed by requireExplicitPolicy2 subCA Cert

6.1.5.272 Invalid Self-Issued requireExplicitPolicy Test8 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=requireExplicitPolicy2 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued requireExplicitPolicy EE Certificate Test8, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: absent
signed by requireExplicitPolicy2 Self-Issued subCA Cert

6.1.5.273 Mapping 1to2 CA Cert:

base: Base Intermediate Certificate
serial number: 48
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Mapping 1to2 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by Trust Anchor Root Certificate

6.1.5.274 Mapping 1to2 CA CRL:

base: Base CRL
issuer: "cn=Mapping 1to2 CA, o=Test Certificates 2011, c=US"
signed by Mapping 1to2 CA Cert
post to certificateRevocationList

6.1.5.275 Valid Policy Mapping Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Mapping 1to2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test1, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Mapping 1to2 CA Cert

6.1.5.276 Invalid Policy Mapping Test2 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Mapping 1to2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Policy Mapping EE Certificate Test2, o=Test Certificates 2011, c=US"
signed by Mapping 1to2 CA Cert

6.1.5.277 P12 Mapping 1to3 CA Cert:

base: Base Intermediate Certificate
serial number: 49
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=P12 Mapping 1to3 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.3"
signed by Trust Anchor Root Certificate

6.1.5.278 P12 Mapping 1to3 CA CRL:

base: Base CRL
issuer: "cn=P12 Mapping 1to3 CA, o=Test Certificates 2011, c=US"
signed by P12 Mapping 1to3 CA Cert
post to certificateRevocationList

6.1.5.279 P12 Mapping 1to3 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=P12 Mapping 1to3 CA, o=Test Certificates 2011, c=US"
subject: "cn=P12 Mapping 1to3 subCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.5"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.4"
map "2.16.840.1.101.3.2.1.48.5" to "2.16.840.1.101.3.2.1.48.7"
signed by P12 Mapping 1to3 CA Cert

6.1.5.280 P12 Mapping 1to3 subCA CRL:

base: Base CRL
issuer: "cn=P12 Mapping 1to3 subCA, o=Test Certificates 2011, c=US"
signed by P12 Mapping 1to3 subCA Cert
post to certificateRevocationList

6.1.5.281 P12 Mapping 1to3 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=P12 Mapping 1to3 subCA, o=Test Certificates 2011, c=US"
subject: "cn=P12 Mapping 1to3 subsubCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
"2.16.840.1.101.3.2.1.48.4"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.4" to "2.16.840.1.101.3.2.1.48.8"
signed by P12 Mapping 1to3 subCA Cert

6.1.5.282 P12 Mapping 1to3 subsubCA CRL:

base: Base CRL
issuer: "cn=P12 Mapping 1to3 subsubCA, o=Test Certificates 2011, c=US"
signed by P12 Mapping 1to3 subsubCA Cert
post to certificateRevocationList

6.1.5.283 Valid Policy Mapping Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=P12 Mapping 1to3 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test3, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
signed by P12 Mapping 1to3 subsubCA Cert

6.1.5.284 Invalid Policy Mapping Test4 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=P12 Mapping 1to3 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Policy Mapping EE Certificate Test4, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
signed by P12 Mapping 1to3 subsubCA Cert

6.1.5.285 P1 Mapping 1to234 CA Cert:

base: Base Intermediate Certificate
serial number: 50
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=P1 Mapping 1to234 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical

requireExplicitPolicy: 0
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.3"
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.4"
signed by Trust Anchor Root Certificate

6.1.5.286 P1 Mapping 1to234 CA CRL:

base: Base CRL
issuer: "cn=P1 Mapping 1to234 CA, o=Test Certificates 2011, c=US"
signed by P1 Mapping 1to234 CA Cert
post to certificateRevocationList

6.1.5.287 P1 Mapping 1to234 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=P1 Mapping 1to234 CA, o=Test Certificates 2011, c=US"
subject: "cn=P1 Mapping 1to234 subCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.4"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.5"
map "2.16.840.1.101.3.2.1.48.4" to "2.16.840.1.101.3.2.1.48.6"
signed by P1 Mapping 1to234 CA Cert

6.1.5.288 P1 Mapping 1to234 subCA CRL:

base: Base CRL
issuer: "cn=P1 Mapping 1to234 subCA, o=Test Certificates 2011, c=US"
signed by P1 Mapping 1to234 subCA Cert
post to certificateRevocationList

6.1.5.289 Valid Policy Mapping Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=P1 Mapping 1to234 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test5, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.6"
signed by P1 Mapping 1to234 subCA Cert

6.1.5.290 Valid Policy Mapping Test6 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=P1 Mapping 1to234 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test6, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.5"

signed by P1 Mapping 1to234 subCA Cert

6.1.5.291 Mapping From anyPolicy CA Cert:

base: Base Intermediate Certificate
serial number: 51
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Mapping From anyPolicy CA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
policyMappingsExtension: critical
map "2.5.29.32.0" to "2.16.840.1.101.3.2.1.48.1"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
signed by Trust Anchor Root Certificate

6.1.5.292 Mapping From anyPolicy CA CRL:

base: Base CRL
issuer: "cn=Mapping From anyPolicy CA, o=Test Certificates 2011, c=US"
signed by Mapping From anyPolicy CA Cert
post to certificateRevocationList

6.1.5.293 Invalid Mapping From anyPolicy Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Mapping From anyPolicy CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Mapping From anyPolicy EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by Mapping From anyPolicy CA Cert

6.1.5.294 Mapping To anyPolicy CA Cert:

base: Base Intermediate Certificate
serial number: 52
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Mapping To anyPolicy CA, o=Test Certificates 2011, c=US"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.5.29.32.0"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
signed by Trust Anchor Root Certificate

6.1.5.295 Mapping To anyPolicy CA CRL:

base: Base CRL
issuer: "cn=Mapping To anyPolicy CA, o=Test Certificates 2011, c=US"
signed by Mapping To anyPolicy CA Cert
post to certificateRevocationList

6.1.5.296 Invalid Mapping To anyPolicy Test8 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=Mapping To anyPolicy CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Mapping To anyPolicy EE Certificate Test8, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by Mapping To anyPolicy CA Cert

6.1.5.297 PanyPolicy Mapping 1to2 CA Cert:

base: Base Intermediate Certificate
serial number: 53
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=PanyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.5.29.32.0"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by Trust Anchor Root Certificate

6.1.5.298 PanyPolicy Mapping 1to2 CA CRL:

base: Base CRL
issuer: "cn=PanyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
signed by PanyPolicy Mapping 1to2 CA Cert
post to certificateRevocationList

6.1.5.299 Valid Policy Mapping Test9 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=PanyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by PanyPolicy Mapping 1to2 CA Cert

6.1.5.300 Good subCA PanyPolicy Mapping 1to2 CA Cert:

base: Base Intermediate Certificate
serial number: 22
issuer: "cn=Good CA, o=Test Certificates 2011, c=US"
subject: "cn=Good subCA PanyPolicy Mapping 1to2, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.5.29.32.0"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by Good CA Cert

6.1.5.301 Good subCA PanyPolicy Mapping 1to2 CA CRL:

base: Base CRL
issuer: "cn=Good subCA PanyPolicy Mapping 1to2, o=Test Certificates 2011, c=US"
signed by Good subCA PanyPolicy Mapping 1to2 CA Cert
post to certificateRevocationList

6.1.5.302 Invalid Policy Mapping Test10 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Good subCA PanyPolicy Mapping 1to2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Policy Mapping EE Certificate Test10, o=Test Certificates 2011, c=US"
signed by Good subCA PanyPolicy Mapping 1to2 CA Cert

6.1.5.303 Valid Policy Mapping Test11 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Good subCA PanyPolicy Mapping 1to2, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test11, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by Good subCA PanyPolicy Mapping 1to2 CA Cert

6.1.5.304 Valid Policy Mapping Test12 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=P12 Mapping 1to3 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test12, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q7: This is the user notice from qualifier 7 associated with NIST-test-policy-3. This user notice should be displayed when NIST-test-policy-1 is in the user-constrained-policy-set."
"2.5.29.32.0"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q8: This is the user notice from qualifier 8 associated with anyPolicy. This user notice should be displayed when NIST-test-policy-2 is in the user-constrained-policy-set."
signed by P12 Mapping 1to3 CA Cert

6.1.5.305 P1anyPolicy Mapping 1to2 CA Cert:

base: Base Intermediate Certificate
serial number: 54
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"

subject: "cn=P1anyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q9: This is the user notice from qualifier 9 associated with NIST-test-policy-1. This user notice should be displayed for Valid Policy Mapping Test13."
"2.5.29.32.0"
policyQualifierInfo:
policyQualifierId: 1.3.6.1.5.5.7.2.2
UserNotice:
"q10: This is the user notice from qualifier 10 associated with anyPolicy. This user notice should be displayed for Valid Policy Mapping Test14."
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by Trust Anchor Root Certificate

6.1.5.306 P1anyPolicy Mapping 1to2 CA CRL:

base: Base CRL
issuer: "cn=P1anyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
signed by P1anyPolicy Mapping 1to2 CA Cert
post to certificateRevocationList

6.1.5.307 Valid Policy Mapping Test13 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=P1anyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test13, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by P1anyPolicy Mapping 1to2 CA Cert

6.1.5.308 Valid Policy Mapping Test14 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=P1anyPolicy Mapping 1to2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Policy Mapping EE Certificate Test14, o=Test Certificates 2011, c=US"
signed by P1anyPolicy Mapping 1to2 CA Cert

6.1.5.309 inhibitPolicyMapping0 CA Cert:

base: Base Intermediate Certificate
serial number: 55
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping0 CA, o=Test Certificates 2011, c=US"

policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
signed by Trust Anchor Root Certificate

6.1.5.310 inhibitPolicyMapping0 CA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping0 CA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping0 CA Cert
post to certificateRevocationList

6.1.5.311 inhibitPolicyMapping0 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping0 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping0 subCA, o=Test Certificates 2011, c=US"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping0 CA Cert

6.1.5.312 inhibitPolicyMapping0 subCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping0 subCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping0 subCA Cert
post to certificateRevocationList

6.1.5.313 Invalid inhibitPolicyMapping Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping0 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitPolicyMapping EE Certificate Test1, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping0 subCA Cert

6.1.5.314 inhibitPolicyMapping1 P12 CA Cert:

base: Base Intermediate Certificate
serial number: 56
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P12 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 1
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
signed by Trust Anchor Root Certificate

6.1.5.315 inhibitPolicyMapping1 P12 CA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P12 CA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P12 CA Cert
post to certificateRevocationList

6.1.5.316 inhibitPolicyMapping1 P12 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P12 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P12 subCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.3"
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.4"
signed by inhibitPolicyMapping1 P12 CA Cert

6.1.5.317 inhibitPolicyMapping1 P12 subCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P12 subCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P12 subCA Cert
post to certificateRevocationList

6.1.5.318 Valid inhibitPolicyMapping Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P12 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid inhibitPolicyMapping EE Certificate Test2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P12 subCA Cert

6.1.5.319 inhibitPolicyMapping1 P12 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P12 subCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P12 subsubCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
"2.16.840.1.101.3.2.1.48.4"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.3" to "2.16.840.1.101.3.2.1.48.5"
signed by inhibitPolicyMapping1 P12 subCA Cert

6.1.5.320 inhibitPolicyMapping1 P12 subsubCA CRL:

base: Base CRL

issuer: "cn=inhibitPolicyMapping1 P12 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P12 subsubCA Cert
post to certificateRevocationList

6.1.5.321 Invalid inhibitPolicyMapping Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P12 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitPolicyMapping EE Certificate Test3, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.5"
signed by inhibitPolicyMapping1 P12 subsubCA Cert

6.1.5.322 Valid inhibitPolicyMapping Test4 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P12 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid inhibitPolicyMapping EE Certificate Test4, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.4"
signed by inhibitPolicyMapping1 P12 subsubCA Cert

6.1.5.323 inhibitPolicyMapping5 CA Cert:

base: Base Intermediate Certificate
serial number: 57
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping5 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 5
signed by Trust Anchor Root Certificate

6.1.5.324 inhibitPolicyMapping5 CA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping5 CA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping5 CA Cert
post to certificateRevocationList

6.1.5.325 inhibitPolicyMapping5 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping5 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping5 subCA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
inhibitPolicyMapping: 1
signed by inhibitPolicyMapping5 CA Cert

6.1.5.326 inhibitPolicyMapping5 subCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping5 subCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping5 subCA Cert
post to certificateRevocationList

6.1.5.327 inhibitPolicyMapping5 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping5 subCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping5 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping5 subCA Cert

6.1.5.328 inhibitPolicyMapping5 subsubCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping5 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping5 subsubCA Cert
post to certificateRevocationList

6.1.5.329 inhibitPolicyMapping5 subsubsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping5 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping5 subsubsubCA, o=Test Certificates 2011, c=US"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping5 subsubCA Cert

6.1.5.330 inhibitPolicyMapping5 subsubsubCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping5 subsubsubCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping5 subsubsubCA Cert
post to certificateRevocationList

6.1.5.331 Invalid inhibitPolicyMapping Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping5 subsubsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitPolicyMapping EE Certificate Test5, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping5 subsubsubCA Cert

6.1.5.332 inhibitPolicyMapping1 P12 subCAIPM5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P12 CA, o=Test Certificates 2011, c=US"

subject: "cn=inhibitPolicyMapping1 P12 subCAIPM5, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
inhibitPolicyMapping: 5
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping1 P12 CA Cert

6.1.5.333 inhibitPolicyMapping1 P12 subCAIPM5 CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P12 subCAIPM5, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P12 subCAIPM5 Cert
post to certificateRevocationList

6.1.5.334 inhibitPolicyMapping1 P12 subsubCAIPM5 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P12 subCAIPM5, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P12 subsubCAIPM5, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P12 subCAIPM5 Cert

6.1.5.335 inhibitPolicyMapping1 P12 subsubCAIPM5 CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P12 subsubCAIPM5, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P12 subsubCAIPM5 Cert
post to certificateRevocationList

6.1.5.336 Invalid inhibitPolicyMapping Test6 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P12 subsubCAIPM5, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitPolicyMapping EE Certificate Test6, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P12 subsubCAIPM5 Cert

6.1.5.337 inhibitPolicyMapping1 P1 CA Cert:

base: Base Intermediate Certificate
serial number: 58
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P1 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: critical
requireExplicitPolicy: 0

inhibitPolicyMapping: 1
signed by Trust Anchor Root Certificate

6.1.5.338 inhibitPolicyMapping1 P1 CA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P1 CA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P1 CA Cert
post to certificateRevocationList

6.1.5.339 inhibitPolicyMapping1 P1 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P1 CA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P1 CA Cert

6.1.5.340 inhibitPolicyMapping1 P1 subCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping1 P1 Self-Issued CA Cert

6.1.5.341 inhibitPolicyMapping1 P1 subCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P1 subCA Cert
post to certificateRevocationList

6.1.5.342 Valid Self-Issued inhibitPolicyMapping Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued inhibitPolicyMapping EE Certificate Test7, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping1 P1 subCA Cert

6.1.5.343 inhibitPolicyMapping1 P1 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P1 subsubCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"

policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P1 subCA Cert

6.1.5.344 inhibitPolicyMapping1 P1 subsubCA CRL:

base: Base CRL
issuer: "cn=inhibitPolicyMapping1 P1 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitPolicyMapping1 P1 subsubCA Cert
post to certificateRevocationList

6.1.5.345 Invalid Self-Issued inhibitPolicyMapping Test8 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitPolicyMapping1 P1 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued inhibitPolicyMapping EE Certificate Test8, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P1 subsubCA Cert

6.1.5.346 Invalid Self-Issued inhibitPolicyMapping Test9 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=inhibitPolicyMapping1 P1 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued inhibitPolicyMapping EE Certificate Test9, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping1 P1 subsubCA Cert

6.1.5.347 inhibitPolicyMapping1 P1 Self-Issued subCA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: critical
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P1 subCA Cert

6.1.5.348 Invalid Self-Issued inhibitPolicyMapping Test10 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued inhibitPolicyMapping EE Certificate Test10, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical

"2.16.840.1.101.3.2.1.48.3"
signed by inhibitPolicyMapping1 P1 Self-Issued subCA Cert

6.1.5.349 Invalid Self-Issued inhibitPolicyMapping Test11 EE:

base: Base End Certificate
serial number: 5
issuer: "cn=inhibitPolicyMapping1 P1 subCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued inhibitPolicyMapping EE Certificate Test11, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
signed by inhibitPolicyMapping1 P1 Self-Issued subCA Cert

6.1.5.350 inhibitAnyPolicy0 CA Cert:

base: Base Intermediate Certificate
serial number: 59
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy0 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitAnyPolicy: critical
skipCert: 0
signed by Trust Anchor Root Certificate

6.1.5.351 inhibitAnyPolicy0 CA CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy0 CA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy0 CA Cert
post to certificateRevocationList

6.1.5.352 Invalid inhibitAnyPolicy Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy0 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitAnyPolicy EE Certificate Test1, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy0 CA Cert

6.1.5.353 Valid inhibitAnyPolicy Test2 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=inhibitAnyPolicy0 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid inhibitAnyPolicy EE Certificate Test2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
"2.16.840.1.101.3.2.1.48.1"
signed by inhibitAnyPolicy0 CA Cert

6.1.5.354 inhibitAnyPolicy1 CA Cert:

base: Base Intermediate Certificate
serial number: 60
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitAnyPolicy: critical
skipCert: 1
signed by Trust Anchor Root Certificate

6.1.5.355 inhibitAnyPolicy1 CA CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 CA Cert
post to certificateRevocationList

6.1.5.356 inhibitAnyPolicy1 subCA1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subCA1, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 CA Cert

6.1.5.357 inhibitAnyPolicy1 subCA1 CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy1 subCA1, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subCA1 Cert
post to certificateRevocationList

6.1.5.358 inhibitAnyPolicy Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy1 subCA1, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy EE Certificate Test3, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subCA1 Cert

6.1.5.359 Invalid inhibitAnyPolicy Test4 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=inhibitAnyPolicy1 subCA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitAnyPolicy EE Certificate Test4, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 subCA1 Cert

6.1.5.360 inhibitAnyPolicy5 CA Cert:

base: Base Intermediate Certificate
serial number: 61
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy5 CA, o=Test Certificates 2011, c=US"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitAnyPolicy: critical
skipCert: 5
signed by Trust Anchor Root Certificate

6.1.5.361 inhibitAnyPolicy5 CA CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy5 CA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy5 CA Cert
post to certificateRevocationList

6.1.5.362 inhibitAnyPolicy5 subCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy5 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy5 subCA, o=Test Certificates 2011, c=US"
inhibitAnyPolicy: critical
skipCert: 1
signed by inhibitAnyPolicy5 CA Cert

6.1.5.363 inhibitAnyPolicy5 subCA CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy5 subCA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy5 subCA Cert
post to certificateRevocationList

6.1.5.364 inhibitAnyPolicy5 subsubCA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy5 subCA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy5 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy5 subCA Cert

6.1.5.365 inhibitAnyPolicy5 subsubCA CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy5 subsubCA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy5 subsubCA Cert
post to certificateRevocationList

6.1.5.366 Invalid inhibitAnyPolicy Test5 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=inhibitAnyPolicy5 subsubCA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitAnyPolicy EE Certificate Test5, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy5 subsubCA Cert

6.1.5.367 inhibitAnyPolicy1 subCAIAP5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subCAIAP5, o=Test Certificates 2011, c=US"
inhibitAnyPolicy: critical
skipCert: 5
signed by inhibitAnyPolicy1 CA Cert

6.1.5.368 inhibitAnyPolicy1 subCAIAP5 CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy1 subCAIAP5, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subCAIAP5 Cert
post to certificateRevocationList

6.1.5.369 Invalid inhibitAnyPolicy Test6 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy1 subCAIAP5, o=Test Certificates 2011, c=US"
subject: "cn=Invalid inhibitAnyPolicy EE Certificate Test6, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 subCAIAP5 Cert

6.1.5.370 inhibitAnyPolicy1 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 CA Cert

6.1.5.371 inhibitAnyPolicy1 subCA2 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=inhibitAnyPolicy1 CA, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 Self-Issued CA Cert

6.1.5.372 inhibitAnyPolicy1 subCA2 CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subCA2 Cert
post to certificateRevocationList

6.1.5.373 Valid Self-Issued inhibitAnyPolicy Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued inhibitAnyPolicy EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subCA2 Cert

6.1.5.374 inhibitAnyPolicy1 subsubCA2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subsubCA2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 subCA2 Cert

6.1.5.375 inhibitAnyPolicy1 subsubCA2 CRL:

base: Base CRL
issuer: "cn=inhibitAnyPolicy1 subsubCA2, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subsubCA2 Cert
post to certificateRevocationList

6.1.5.376 Invalid Self-Issued inhibitAnyPolicy Test8 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=inhibitAnyPolicy1 subsubCA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Self-Issued inhibitAnyPolicy EE Certificate Test8, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 subsubCA2 Cert

6.1.5.377 inhibitAnyPolicy1 Self-Issued subCA2 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
signed by inhibitAnyPolicy1 subCA2 Cert

6.1.5.378 Valid Self-Issued inhibitAnyPolicy Test9 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid Self-Issued inhibitAnyPolicy EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by inhibitAnyPolicy1 Self-Issued subCA2 Cert

6.1.5.379 Invalid Self-Issued inhibitAnyPolicy Test10 EE:

base: Base Intermediate Certificate
serial number: 5
issuer: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=inhibitAnyPolicy1 subCA2, o=Test Certificates 2011, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by inhibitAnyPolicy1 subCA2 Cert

6.1.5.380 nameConstraints DN1 CA Cert:

base: Base Intermediate Certificate
serial number: 62
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=permittedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.381 nameConstraints DN1 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert
post to certificateRevocationList

6.1.5.382 Valid DN nameConstraints Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert

6.1.5.383 Invalid DN nameConstraints Test2 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test2, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert

6.1.5.384 Invalid DN nameConstraints Test3 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
directoryName: "cn=Invalid DN nameConstraints EE Certificate Test3, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert

6.1.5.385 Valid DN nameConstraints Test4 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test4, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "DNnameConstraintsTest4EE@testcertificates.gov"
signed by nameConstraints DN1 CA Cert

6.1.5.386 nameConstraints DN2 CA Cert:

base: Base Intermediate Certificate
serial number: 63
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN2 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=permittedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
permittedSubtrees:
directoryName: "ou=permittedSubtree2, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.387 nameConstraints DN2 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DN2 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN2 CA Cert
post to certificateRevocationList

6.1.5.388 Valid DN nameConstraints Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test5, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
directoryName: "cn=Valid DN nameConstraints EE Certificate Test5, ou=permittedSubtree2, o=Test Certificates 2011, c=US"
signed by nameConstraints DN2 CA Cert

6.1.5.389 nameConstraints DN3 CA Cert:

base: Base Intermediate Certificate
serial number: 64
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=excludedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.390 nameConstraints DN3 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 CA Cert
post to certificateRevocationList

6.1.5.391 Valid DN nameConstraints Test6 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test6, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 CA Cert

6.1.5.392 Invalid DN nameConstraints Test7 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"

subject: "cn=Invalid DN nameConstraints EE Certificate Test7, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 CA Cert

6.1.5.393 nameConstraints DN4 CA Cert:

base: Base Intermediate Certificate
serial number: 65
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN4 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=excludedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
excludedSubtrees:
directoryName: "ou=excludedSubtree2, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.394 nameConstraints DN4 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DN4 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN4 CA Cert
post to certificateRevocationList

6.1.5.395 Invalid DN nameConstraints Test8 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN4 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test8, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN4 CA Cert

6.1.5.396 Invalid DN nameConstraints Test9 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN4 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test9, ou=excludedSubtree2, o=Test Certificates 2011, c=US"
signed by nameConstraints DN4 CA Cert

6.1.5.397 nameConstraints DN5 CA Cert:

base: Base Intermediate Certificate
serial number: 66
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"

subject: "cn=nameConstraints DN5 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=permittedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
excludedSubtrees:
directoryName: "ou=excludedSubtree1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.398 nameConstraints DN5 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DN5 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN5 CA Cert
post to certificateRevocationList

6.1.5.399 Invalid DN nameConstraints Test10 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN5 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test10, ou=excludedSubtree1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN5 CA Cert

6.1.5.400 Valid DN nameConstraints Test11 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN5 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test11, ou=permittedSubtree2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN5 CA Cert

6.1.5.401 nameConstraints DN1 subCA1 Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 subCA1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=permittedSubtree2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by nameConstraints DN1 CA Cert

6.1.5.402 nameConstraints DN1 subCA1 CRL:

base: Base CRL
issuer: "cn=nameConstraints DN1 subCA1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA1 Cert
post to certificateRevocationList

6.1.5.403 Invalid DN nameConstraints Test12 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN1 subCA1, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test12, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA1 Cert

6.1.5.404 nameConstraints DN1 subCA2 Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 subCA2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=permittedSubtree2, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by nameConstraints DN1 CA Cert

6.1.5.405 nameConstraints DN1 subCA2 CRL:

base: Base CRL
issuer: "cn=nameConstraints DN1 subCA2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA2 Cert
post to certificateRevocationList

6.1.5.406 Invalid DN nameConstraints Test13 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN1 subCA2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test13, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA2 Cert

6.1.5.407 Valid DN nameConstraints Test14 EE:

base: Base End Certificate

serial number: 2
issuer: "cn=nameConstraints DN1 subCA2, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension: critical
rfc822Name: "ValidDNnameConstraintsTest14EE@testcertificates.gov"
signed by nameConstraints DN1 subCA2 Cert

6.1.5.408 nameConstraints DN3 subCA1 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN3 subCA1, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=excludedSubtree2, o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by nameConstraints DN3 CA Cert

6.1.5.409 nameConstraints DN3 subCA1 CRL:

base: Base CRL
issuer: "cn=nameConstraints DN3 subCA1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA1 Cert
post to certificateRevocationList

6.1.5.410 Invalid DN nameConstraints Test15 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN3 subCA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test15, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA1 Cert

6.1.5.411 Invalid DN nameConstraints Test16 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN3 subCA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test16, ou=excludedSubtree2, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA1 Cert

6.1.5.412 nameConstraints DN3 subCA2 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=nameConstraints DN3 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN3 subCA2, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical

permittedSubtrees:
directoryName: "o=Test Certificates 2011, c=US"
minimum: 0
maximum: absent
signed by nameConstraints DN3 CA Cert

6.1.5.413 nameConstraints DN3 subCA2 CRL:

base: Base CRL
issuer: "cn=nameConstraints DN3 subCA2, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA2 Cert
post to certificateRevocationList

6.1.5.414 Invalid DN nameConstraints Test17 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN3 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN nameConstraints EE Certificate Test17, ou=excludedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA2 Cert

6.1.5.415 Valid DN nameConstraints Test18 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN3 subCA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test18, o=Test Certificates 2011, c=US"
signed by nameConstraints DN3 subCA2 Cert

6.1.5.416 nameConstraints DN1 Self-Issued CA Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert

6.1.5.417 Valid DN nameConstraints Test19 EE:

base: Base End Certificate
serial number: 8
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN nameConstraints EE Certificate Test19, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 Self-Issued CA Cert

6.1.5.418 Invalid DN nameConstraints Test20 EE:

base: Base End Certificate
serial number: 9
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 CA Cert

6.1.5.419 nameConstraints RFC822 CA1 Cert:

base: Base Intermediate Certificate
serial number: 67
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints RFC822 CA1, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
rfc822Name: ".testcertificates.gov"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.420 nameConstraints RFC822 CA1 CRL:

base: Base CRL
issuer: "cn=nameConstraints RFC822 CA1, o=Test Certificates 2011, c=US"
signed by nameConstraints RFC822 CA1 Cert
post to certificateRevocationList

6.1.5.421 Valid RFC822 nameConstraints Test21 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints RFC822 CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid RFC822 nameConstraints EE Certificate Test21, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test21EE@mailserver.testcertificates.gov"
signed by nameConstraints RFC822 CA1 Cert

6.1.5.422 Invalid RFC822 nameConstraints Test22 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints RFC822 CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid RFC822 nameConstraints EE Certificate Test22, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test22EE@testcertificates.gov"
signed by nameConstraints RFC822 CA1 Cert

6.1.5.423 nameConstraints RFC822 CA2 Cert:

base: Base Intermediate Certificate
serial number: 68
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints RFC822 CA2, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
rfc822Name: "testcertificates.gov"
minimum: 0
maximum: absent

signed by Trust Anchor Root Certificate

6.1.5.424 nameConstraints RFC822 CA2 CRL:

base: Base CRL
issuer: "cn=nameConstraints RFC822 CA2, o=Test Certificates 2011, c=US"
signed by nameConstraints RFC822 CA2 Cert
post to certificateRevocationList

6.1.5.425 Valid RFC822 nameConstraints Test23 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints RFC822 CA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid RFC822 nameConstraints EE Certificate Test23, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test23EE@testcertificates.gov"
signed by nameConstraints RFC822 CA2 Cert

6.1.5.426 Invalid RFC822 nameConstraints Test24 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints RFC822 CA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid RFC822 nameConstraints EE Certificate Test24, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test24EE@mailserver.testcertificates.gov"
signed by nameConstraints RFC822 CA2 Cert

6.1.5.427 nameConstraints RFC822 CA3 Cert:

base: Base Intermediate Certificate
serial number: 69
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints RFC822 CA3, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
rfc822Name: "testcertificates.gov"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.428 nameConstraints RFC822 CA3 CRL:

base: Base CRL
issuer: "cn=nameConstraints RFC822 CA3, o=Test Certificates 2011, c=US"
signed by nameConstraints RFC822 CA3 Cert
post to certificateRevocationList

6.1.5.429 Valid RFC822 nameConstraints Test25 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=nameConstraints RFC822 CA3, o=Test Certificates 2011, c=US"
subject: "cn=Valid RFC822 nameConstraints EE Certificate Test25, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test25EE@mailserver.testcertificates.gov"
signed by nameConstraints RFC822 CA3 Cert

6.1.5.430 Invalid RFC822 nameConstraints Test26 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints RFC822 CA3, o=Test Certificates 2011, c=US"
subject: "cn=Invalid RFC822 nameConstraints EE Certificate Test26, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test26EE@testcertificates.gov"
signed by nameConstraints RFC822 CA3 Cert

6.1.5.431 nameConstraints DN1 subCA3 Cert:

base: Base Intermediate Certificate
serial number: 10
issuer: "cn=nameConstraints DN1 CA, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DN1 subCA3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
rfc822Name: "testcertificates.gov"
minimum: 0
maximum: absent
signed by nameConstraints DN1 CA Cert

6.1.5.432 nameConstraints DN1 subCA3 CRL:

base: Base CRL
issuer: "cn=nameConstraints DN1 subCA3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA3 Cert
post to certificateRevocationList

6.1.5.433 Valid DN and RFC822 nameConstraints Test27 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DN1 subCA3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subject: "cn=Valid DN and RFC822 nameConstraints EE Certificate Test27, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test27EE@testcertificates.gov"
signed by nameConstraints DN1 subCA3 Cert

6.1.5.434 Invalid DN and RFC822 nameConstraints Test28 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DN1 subCA3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DN and RFC822 nameConstraints EE Certificate Test28, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
rfc822Name: "Test28EE@invalidcertificates.gov"
signed by nameConstraints DN1 subCA3 Cert

6.1.5.435 Invalid DN and RFC822 nameConstraints Test29 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=nameConstraints DN1 subCA3, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
subject: "emailAddress=Test29EE@invalidcertificates.gov, cn=Invalid DN and RFC822 nameConstraints EE Certificate Test29, ou=permittedSubtree1, o=Test Certificates 2011, c=US"
signed by nameConstraints DN1 subCA3 Cert

6.1.5.436 nameConstraints DNS1 CA Cert:

base: Base Intermediate Certificate
serial number: 70
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DNS1 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
dnsName: testcertificates.gov
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.437 nameConstraints DNS1 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DNS1 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DNS1 CA Cert
post to certificateRevocationList

6.1.5.438 Valid DNS nameConstraints Test30 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DNS1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DNS nameConstraints EE Certificate Test30, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
dnsName: testserver.testcertificates.gov
signed by nameConstraints DNS1 CA Cert

6.1.5.439 Invalid DNS nameConstraints Test31 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DNS1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DNS nameConstraints EE Certificate Test31, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
dnsName: testserver.invalidcertificates.gov
signed by nameConstraints DNS1 CA Cert

6.1.5.440 nameConstraints DNS2 CA Cert:

base: Base Intermediate Certificate
serial number: 71
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints DNS2 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
dnsName: invalidcertificates.gov
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.441 nameConstraints DNS2 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints DNS2 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints DNS2 CA Cert
post to certificateRevocationList

6.1.5.442 Valid DNS nameConstraints Test32 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints DNS2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DNS nameConstraints EE Certificate Test32, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
dnsName: testserver.testcertificates.gov
signed by nameConstraints DNS2 CA Cert

6.1.5.443 Invalid DNS nameConstraints Test33 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints DNS2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DNS nameConstraints EE Certificate Test33, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
dnsName: invalidcertificates.gov
signed by nameConstraints DNS2 CA Cert

6.1.5.444 nameConstraints URI1 CA Cert:

base: Base Intermediate Certificate
serial number: 72
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints URI1 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
permittedSubtrees:
URI: ".testcertificates.gov"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.445 nameConstraints URI1 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints URI1 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints URI1 CA Cert
post to certificateRevocationList

6.1.5.446 Valid URI nameConstraints Test34 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints URI1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid URI nameConstraints EE Certificate Test34, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
URI: "http://testserver.testcertificates.gov/index.html"
signed by nameConstraints URI1 CA Cert

6.1.5.447 Invalid URI nameConstraints Test35 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints URI1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid URI nameConstraints EE Certificate Test35, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
URI: "http://testcertificates.gov/invalid.html"
signed by nameConstraints URI1 CA Cert

6.1.5.448 nameConstraints URI2 CA Cert:

base: Base Intermediate Certificate
serial number: 73
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=nameConstraints URI2 CA, o=Test Certificates 2011, c=US"
nameConstraintsExtension: critical
excludedSubtrees:
URI: "invalidcertificates.gov"
minimum: 0
maximum: absent
signed by Trust Anchor Root Certificate

6.1.5.449 nameConstraints URI2 CA CRL:

base: Base CRL
issuer: "cn=nameConstraints URI2 CA, o=Test Certificates 2011, c=US"
signed by nameConstraints URI2 CA Cert
post to certificateRevocationList

6.1.5.450 Valid URI nameConstraints Test36 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=nameConstraints URI2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid URI nameConstraints EE Certificate Test36, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
URI: "http://testserver.invalidcertificates.gov/index.html"
signed by nameConstraints URI2 CA Cert

6.1.5.451 Invalid URI nameConstraints Test37 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=nameConstraints URI2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid URI nameConstraints EE Certificate Test37, o=Test Certificates 2011, c=US"
subjectAltNameExtension:
URI: "ftp://invalidcertificates.gov:21/test37/"
signed by nameConstraints URI2 CA Cert

6.1.5.452 distributionPoint1 CA Cert:

base: Base Intermediate Certificate
serial number: 74
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.453 distributionPoint1 CA CRL:

base: Base CRL
issuer: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 of distributionPoint1 CA, ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 2
signed by distributionPoint1 CA Cert
post to certificateRevocationList at "cn=CRL1 of distributionPoint1 CA, ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
post to certificateRevocationList at "cn=CRLx of distributionPoint1 CA, ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"

6.1.5.454 Valid distributionPoint Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid distributionPoint EE Certificate Test1, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 of distributionPoint1 CA,
ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
signed by distributionPoint1 CA Cert

6.1.5.455 Invalid distributionPoint Test2 EE:

base: Base End Certificate
serial number: 2
issuer: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid distributionPoint EE Certificate Test2, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 of distributionPoint1 CA,
ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
signed by distributionPoint1 CA Cert

6.1.5.456 Invalid distributionPoint Test3 EE:

base: Base End Certificate
serial number: 3
issuer: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid distributionPoint EE Certificate Test3, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRLx of distributionPoint1 CA,
ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
signed by distributionPoint1 CA Cert

6.1.5.457 Valid distributionPoint Test4 EE:

base: Base End Certificate
serial number: 4
issuer: "ou=distributionPoint1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid distributionPoint EE Certificate Test4, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
nameRelativeToCRLIssuer: "cn=CRL1 of distributionPoint1 CA"
signed by distributionPoint1 CA Cert

6.1.5.458 distributionPoint2 CA Cert:

base: Base Intermediate Certificate

serial number: 75
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.459 distributionPoint2 CA CRL:

base: Base CRL
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
nameRelativeToCRLIssuer: "cn=CRL1 of distributionPoint2 CA"
revokedCertificates:
serialNumber: 2
signed by distributionPoint2 CA Cert
post to certificateRevocationList at "cn=CRL1 of distributionPoint2 CA, ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
post to certificateRevocationList at "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"

6.1.5.460 Valid distributionPoint Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid distributionPoint EE Certificate Test5, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
nameRelativeToCRLIssuer: "cn=CRL1 of distributionPoint2 CA"
signed by distributionPoint2 CA Cert

6.1.5.461 Invalid distributionPoint Test6 EE:

base: Base End Certificate
serial number: 2
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid distributionPoint EE Certificate Test6, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
nameRelativeToCRLIssuer: "cn=CRL1 of distributionPoint2 CA"
signed by distributionPoint2 CA Cert

6.1.5.462 Valid distributionPoint Test7 EE:

base: Base End Certificate
serial number: 3
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid distributionPoint EE Certificate Test7, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 of distributionPoint2 CA,
ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"

signed by distributionPoint2 CA Cert

6.1.5.463 Invalid distributionPoint Test8 EE:

base: Base End Certificate
serial number: 4
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid distributionPoint EE Certificate Test8, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
signed by distributionPoint2 CA Cert

6.1.5.464 Invalid distributionPoint Test9 EE:

base: Base End Certificate
serial number: 5
issuer: "ou=distributionPoint2 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid distributionPoint EE Certificate Test9, o=Test Certificates 2011, c=US"
signed by distributionPoint2 CA Cert

6.1.5.465 No issuingDistributionPoint CA Cert:

base: Base Intermediate Certificate
serial number: 76
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=No issuingDistributionPoint CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.466 No issuingDistributionPoint CA CRL:

base: Base CRL
issuer: "ou=No issuingDistributionPoint CA, o=Test Certificates 2011, c=US"
signed by No issuingDistributionPoint CA Cert
post to certificateRevocationList at "cn=CRL, ou=No issuingDistributionPoint CA, o=Test Certificates 2011, c=US"

6.1.5.467 Valid No issuingDistributionPoint Test10 EE:

base: Base End Certificate
serial number: 1
issuer: "ou=No issuingDistributionPoint CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid No issuingDistributionPoint EE Certificate Test10, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL, ou=No issuingDistributionPoint CA, o=Test Certificates 2011, c=US"
signed by No issuingDistributionPoint CA Cert

6.1.5.468 onlyContainsUserCerts CA Cert:

base: Base Intermediate Certificate
serial number: 77
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=onlyContainsUserCerts CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.469 onlyContainsUserCerts CA CRL:

base: Base CRL
issuer: "cn=onlyContainsUserCerts CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsUserCerts: TRUE
signed by onlyContainsUserCerts CA Cert
post to certificateRevocationList

6.1.5.470 Invalid onlyContainsUserCerts Test11 EE:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=onlyContainsUserCerts CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlyContainsUserCerts EE Certificate Test11, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by onlyContainsUserCerts CA Cert

6.1.5.471 onlyContainsCACerts CA Cert:

base: Base Intermediate Certificate
serial number: 78
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=onlyContainsCACerts CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.472 onlyContainsCACerts CA CRL:

base: Base CRL
issuer: "cn=onlyContainsCACerts CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsAuthorityCerts: TRUE
signed by onlyContainsCACerts CA Cert
post to authorityRevocationList
post to certificateRevocationList

6.1.5.473 Invalid onlyContainsCACerts Test12 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=onlyContainsCACerts CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlyContainsCACerts EE Certificate Test12, o=Test Certificates 2011, c=US"
signed by onlyContainsCACerts CA Cert

6.1.5.474 Valid onlyContainsCACerts Test13 EE:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=onlyContainsCACerts CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid onlyContainsCACerts EE Certificate Test13, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
digitalSignature: True
nonRepudiation: True
keyEncipherment: True
dataEncipherment: True
signed by onlyContainsCACerts CA Cert

6.1.5.475 onlyContainsAttributeCerts CA Cert:

base: Base Intermediate Certificate
serial number: 79
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=onlyContainsAttributeCerts CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.476 onlyContainsAttributeCerts CA CRL:

base: Base CRL
issuer: "cn=onlyContainsAttributeCerts CA, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsAttributeCerts: TRUE
signed by onlyContainsAttributeCerts CA Cert
post to certificateRevocationList

6.1.5.477 Invalid onlyContainsAttributeCerts Test14 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=onlyContainsAttributeCerts CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlyContainsAttirubteCerts EE Certificate Test14, o=Test Certificates 2011, c=US"
signed by onlyContainsAttributeCerts CA Cert

6.1.5.478 onlySomeReasons CA1 Cert:

base: Base Intermediate Certificate
serial number: 80
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=onlySomeReasons CA1, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.479 onlySomeReasons CA1 compromise CRL:

base: Base CRL
issuer: "cn=onlySomeReasons CA1, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlySomeReasons:
keyCompromise
cACompromise
revokedCertificates:
serialNumber: 1
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by onlySomeReasons CA1 Cert
post to certificateRevocationList

6.1.5.480 onlySomeReasons CA1 other reasons CRL:

base: Base CRL
issuer: "cn=onlySomeReasons CA1, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlySomeReasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
certificateHold
signed by onlySomeReasons CA1 Cert
post to certificateRevocationList

6.1.5.481 Invalid onlySomeReasons Test15 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=onlySomeReasons CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlySomeReasons EE Certificate Test15, o=Test Certificates 2011, c=US"
signed by onlySomeReasons CA1 Cert

6.1.5.482 Invalid onlySomeReasons Test16 EE:

base: Base End Certificate
serial number: 2

issuer: "cn=onlySomeReasons CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlySomeReasons EE Certificate Test16, o=Test Certificates 2011, c=US"
signed by onlySomeReasons CA1 Cert

6.1.5.483 onlySomeReasons CA2 Cert:

base: Base Intermediate Certificate
serial number: 81
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=onlySomeReasons CA2, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.484 onlySomeReasons CA2 CRL1:

base: Base CRL
issuer: "cn=onlySomeReasons CA2, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlySomeReasons:
affiliationChanged
superseded
signed by onlySomeReasons CA2 Cert
post to certificateRevocationList

6.1.5.485 onlySomeReasons CA2 CRL2:

base: Base CRL
issuer: "cn=onlySomeReasons CA2, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
onlySomeReasons:
cessationOfOperation
certificateHold
signed by onlySomeReasons CA2 Cert
post to certificateRevocationList

6.1.5.486 Invalid onlySomeReasons Test17 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=onlySomeReasons CA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlySomeReasons EE Certificate Test17, o=Test Certificates 2011, c=US"
signed by onlySomeReasons CA2 Cert

6.1.5.487 onlySomeReasons CA3 Cert:

base: Base Intermediate Certificate
serial number: 82
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.488 onlySomeReasons CA3 compromise CRL:

base: Base CRL
issuer: "ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL, ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
onlySomeReasons:
keyCompromise
cACompromise
signed by onlySomeReasons CA3 Cert
post to certificateRevocationList at "cn=CRL, ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"

6.1.5.489 onlySomeReasons CA3 other reasons CRL:

base: Base CRL
issuer: "ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL, ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
onlySomeReasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
signed by onlySomeReasons CA3 Cert
post to certificateRevocationList at "cn=CRL, ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"

6.1.5.490 Valid onlySomeReasons Test18 EE:

base: Base End Certificate
serial number: 1
issuer: "ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
subject: "cn=Valid onlySomeReasons EE Certificate Test18, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL, ou=onlySomeReasons CA3, o=Test Certificates 2011, c=US"
signed by onlySomeReasons CA3 Cert

6.1.5.491 onlySomeReasons CA4 Cert:

base: Base Intermediate Certificate
serial number: 83
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.492 onlySomeReasons CA4 compromise CRL:

base: Base CRL
issuer: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
onlySomeReasons:
keyCompromise
cACompromise
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by onlySomeReasons CA4 Cert
post to certificateRevocationList at "cn=CRL1, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"

6.1.5.493 onlySomeReasons CA4 other reasons CRL:

base: Base CRL
issuer: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL2, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
onlySomeReasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
revokedCertificates:
serialNumber: 3
crlEntryExtensions:

reasonCodeExtension: not critical
reasons:
affiliationChanged
signed by onlySomeReasons CA4 Cert
post to certificateRevocationList at "cn=CRL2, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"

6.1.5.494 Valid onlySomeReasons Test19 EE:

base: Base End Certificate
serial number: 1
issuer: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
subject: "cn=Valid onlySomeReasons EE Certificate Test19, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
keyCompromise
cACompromise
distributionPoint:
fullName:
directoryName: "cn=CRL2, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
signed by onlySomeReasons CA4 Cert

6.1.5.495 Invalid onlySomeReasons Test20 EE:

base: Base End Certificate
serial number: 2
issuer: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlySomeReasons EE Certificate Test20, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
keyCompromise
cACompromise
distributionPoint:
fullName:

directoryName: "cn=CRL2, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
signed by onlySomeReasons CA4 Cert

6.1.5.496 Invalid onlySomeReasons Test21 EE:

base: Base End Certificate
serial number: 3
issuer: "ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
subject: "cn=Invalid onlySomeReasons EE Certificate Test21, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
keyCompromise
cACompromise
distributionPoint:
fullName:
directoryName: "cn=CRL2, ou=onlySomeReasons CA4, o=Test Certificates 2011, c=US"
reasons:
unused
affiliationChanged
superseded
cessationOfOperation
certificateHold
privilegeWithdrawn
aACompromise
signed by onlySomeReasons CA4 Cert

6.1.5.497 indirectCRL CA1 Cert:

base: Base Intermediate Certificate
serial number: 84
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.498 indirectCRL CA1 CRL:

base: Base CRL
issuer: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"

crlExtension:
issuingDistributionPoint: critical
indirectCRL: TRUE
revokedCertificates:
serialNumber: 2
signed by indirectCRL CA1 Cert
post to certificateRevocationList at "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
post to certificateRevocationList at "cn=indirectCRL CA1x, o=Test Certificates 2011, c=US"

6.1.5.499 Valid IDP with indirectCRL Test22 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid IDP with indirectCRL EE Certificate Test22, o=Test Certificates 2011, c=US"
signed by indirectCRL CA1 Cert

6.1.5.500 Invalid IDP with indirectCRL Test23 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid IDP with indirectCRL EE Certificate Test23, o=Test Certificates 2011, c=US"
signed by indirectCRL CA1 Cert

6.1.5.501 indirectCRL CA2 Cert:

base: Base Intermediate Certificate
serial number: 85
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=indirectCRL CA2, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.502 Valid IDP with indirectCRL Test24 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=indirectCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid IDP with indirectCRL EE Certificate Test24, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
cRLIssuer: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
signed by indirectCRL CA2 Cert

6.1.5.503 Valid IDP with indirectCRL Test25 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=indirectCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid IDP with indirectCRL EE Certificate Test25, o=Test Certificates 2011, c=US"

cRLDistributionPoints: not critical
distributionPoint:
cRLIssuer: "cn=indirectCRL CA1, o=Test Certificates 2011, c=US"
signed by indirectCRL CA2 Cert

6.1.5.504 Invalid IDP with indirectCRL Test26 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=indirectCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid IDP with indirectCRL EE Certificate Test26, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
cRLIssuer: "cn=indirectCRL CA1x, o=Test Certificates 2011, c=US"
signed by indirectCRL CA2 Cert

6.1.5.505 Invalid cRLIssuer Test27 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=indirectCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cRLIssuer EE Certificate Test27, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
cRLIssuer: "cn=Good CA, o=Test Certificates 2011, c=US"
signed by indirectCRL CA2 Cert

6.1.5.506 indirectCRL CA3 Cert:

base: Base Intermediate Certificate
serial number: 86
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.507 indirectCRL CA3 CRL:

base: Base CRL
issuer: "ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
signed by indirectCRL CA3 Cert
post to certificateRevocationList at "cn=CRL1, ou=indirectCRL CA3, o=Test Certificates 2011, c=US"

6.1.5.508 indirectCRL CA3 cRLIssuer Cert:

base: Base End Certificate

serial number: 1
issuer: "ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
subject: "ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: True
digitalSignature: False
nonRepudiation: False
keyEncipherment: False
dataEncipherment: False

signed by indirectCRL CA3 Cert

6.1.5.509 indirectCRL CA3 cRLIssuer CRL:

base: Base CRL
issuer: "ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA3, ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
indirectCRL: TRUE
signed by indirectCRL CA3 cRLIssuer Cert
post to certificateRevocationList at "cn=indirect CRL for indirectCRL CA3, ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"

6.1.5.510 Valid cRLIssuer Test28 EE:

base: Base End Certificate
serial number: 2
issuer: "ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
subject: "cn=Valid cRLIssuer EE Certificate Test28, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA3, ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
signed by indirectCRL CA3 Cert

6.1.5.511 Valid cRLIssuer Test29 EE:

base: Base End Certificate
serial number: 3

issuer: "ou=indirectCRL CA3, o=Test Certificates 2011, c=US"
subject: "cn=Valid cRLIssuer EE Certificate Test29, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
nameRelativeToCRLIssuer: "cn=indirect CRL for indirectCRL CA3"
cRLIssuer: "ou=indirectCRL CA3 cRLIssuer, o=Test Certificates 2011, c=US"
signed by indirectCRL CA3 Cert

6.1.5.512 indirectCRL CA4 Cert:

base: Base Intermediate Certificate
serial number: 87
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=indirectCRL CA4, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.513 indirectCRL CA4 cRLIssuer Cert:

base: Base End Certificate
serial number: 1
issuer: "ou=indirectCRL CA4, o=Test Certificates 2011, c=US"
subject: "ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA4, ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: True
digitalSignature: False
nonRepudiation: False
keyEncipherment: False
dataEncipherment: False

signed by indirectCRL CA4 Cert

6.1.5.514 indirectCRL CA4 cRLIssuer CRL:

base: Base CRL
issuer: "ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA4, ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"

indirectCRL: TRUE
signed by indirectCRL CA4 cRLIssuer Cert
post to certificateRevocationList at "cn=indirect CRL for indirectCRL CA4, ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"

6.1.5.515 Valid cRLIssuer Test30 EE:

base: Base End Certificate
serial number: 2
issuer: "ou=indirectCRL CA4, o=Test Certificates 2011, c=US"
subject: "cn=Valid cRLIssuer EE Certificate Test30, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA4, ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA4 cRLIssuer, o=Test Certificates 2011, c=US"
signed by indirectCRL CA4 Cert

6.1.5.516 indirectCRL CA5 Cert:

base: Base Intermediate Certificate
serial number: 88
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.517 indirectCRL CA5 CRL:

base: Base CRL
issuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA6, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA7, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
fullName:
directoryName: "cn=CRL1 for indirectCRL CA5, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
indirectCRL: TRUE
revokedCertificates:
serialNumber: 1
serialNumber: 2
crlEntryExtensions:
certificateIssuer: critical
directoryName: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"

serialNumber: 3
serialNumber: 4
serialNumber: 5
crlEntryExtensions:
certificateIssuer: critical
directoryName: "cn=indirectCRL CA7, o=Test Certificates 2011, c=US"
serialNumber: 6
serialNumber: 7
serialNumber: 8
crlEntryExtensions:
certificateIssuer: critical
directoryName: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"
serialNumber: 9
serialNumber: 10
crlEntryExtensions:
certificateIssuer: critical
directoryName: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
serialNumber: 11
signed by indirectCRL CA5 Cert
post to certificateRevocationList at "cn=indirect CRL for indirectCRL CA6, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
post to certificateRevocationList at "cn=indirect CRL for indirectCRL CA7, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
post to certificateRevocationList at "cn=CRL1 for indirectCRL CA5, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"

6.1.5.518 indirectCRL CA6 Cert:

base: Base Intermediate Certificate
serial number: 89
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.519 Invalid cRLIssuer Test31 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cRLIssuer EE Certificate Test31, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA6, ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
signed by indirectCRL CA6 Cert

6.1.5.520 Invalid cRLIssuer Test32 EE:

base: Base End Certificate
serial number: 9
issuer: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cRLIssuer EE Certificate Test32, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA6,
ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
signed by indirectCRL CA6 Cert

6.1.5.521 Valid cRLIssuer Test33 EE:

base: Base End Certificate
serial number: 7
issuer: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"
subject: "cn=Valid cRLIssuer EE Certificate Test33, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=indirect CRL for indirectCRL CA6,
ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
cRLIssuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
signed by indirectCRL CA6 Cert

6.1.5.522 Invalid cRLIssuer Test34 EE:

base: Base End Certificate
serial number: 11
issuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cRLIssuer EE Certificate Test34, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 for indirectCRL CA5, ou=indirectCRL
CA5, o=Test Certificates 2011, c=US"
signed by indirectCRL CA5 Cert

6.1.5.523 Invalid cRLIssuer Test35 EE:

base: Base End Certificate
serial number: 12
issuer: "ou=indirectCRL CA5, o=Test Certificates 2011, c=US"
subject: "cn=Invalid cRLIssuer EE Certificate Test35, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1 for indirectCRL CA5, ou=indirectCRL
CA5, o=Test Certificates 2011, c=US"
cRLIssuer: "cn=indirectCRL CA6, o=Test Certificates 2011, c=US"

signed by indirectCRL CA5 Cert

6.1.5.524 deltaCRLIndicator No Base CA Cert:

base: Base Intermediate Certificate
serial number: 90
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=deltaCRLIndicator No Base CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.525 deltaCRLIndicator No Base CA CRL:

base: Base CRL
crlNumber: 5
issuer: "cn=deltaCRLIndicator No Base CA, o=Test Certificates 2011, c=US"
thisUpdate: UTC: "100501083000Z"
crlExtension:
deltaCRLIndicator: critical
BaseCRLNumber: 1
signed by deltaCRLIndicator No Base CA Cert
post to certificateRevocationList

6.1.5.526 Invalid deltaCRLIndicator No Base Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=deltaCRLIndicator No Base CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRLIndicator No Base EE Certificate Test1, o=Test Certificates 2011, c=US"
signed by deltaCRLIndicator No Base CA Cert

6.1.5.527 deltaCRL CA1 Cert:

base: Base Intermediate Certificate
serial number: 91
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.528 deltaCRL CA1 CRL:

base: Base CRL
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
crlExtension:
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical

reasons:
keyCompromise
serialNumber: 4
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
certificateHold
serialNumber: 5
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
certificateHold
signed by deltaCRL CA1 Cert
post to certificateRevocationList

6.1.5.529 deltaCRL CA1 deltaCRL:

base: Base CRL
crlNumber: 5
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
thisUpdate: UTC: "110101083000Z"
crlExtension:
deltaCRLIndicator: critical
BaseCRLNumber: 1
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
serialNumber: 4
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
removeFromCRL
serialNumber: 5
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
serialNumber: 6
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
removeFromCRL
signed by deltaCRL CA1 Cert
post to deltaRevocationList

6.1.5.530 Valid deltaCRL Test2 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid deltaCRL EE Certificate Test2, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by deltaCRL CA1 Cert

6.1.5.531 Invalid deltaCRL Test3 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRL EE Certificate Test3, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by deltaCRL CA1 Cert

6.1.5.532 Invalid deltaCRL Test4 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRL EE Certificate Test4, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by deltaCRL CA1 Cert

6.1.5.533 Valid deltaCRL Test5 EE:

base: Base End Certificate
serial number: 4
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid deltaCRL EE Certificate Test5, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by deltaCRL CA1 Cert

6.1.5.534 Invalid deltaCRL Test6 EE:

base: Base End Certificate
serial number: 5
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRL EE Certificate Test6, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
signed by deltaCRL CA1 Cert

6.1.5.535 Valid deltaCRL Test7 EE:

base: Base End Certificate
serial number: 6
issuer: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid deltaCRL EE Certificate Test7, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA1, o=Test Certificates 2011, c=US"

signed by deltaCRL CA1 Cert

6.1.5.536 deltaCRL CA2 Cert:

base: Base Intermediate Certificate
serial number: 92
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.537 deltaCRL CA2 CRL:

base: Base CRL
crlNumber: 2
issuer: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
thisUpdate: "100601083000Z"
crlExtension:
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by deltaCRL CA2 Cert
post to certificateRevocationList

6.1.5.538 deltaCRL CA2 deltaCRL:

base: Base CRL
crlNumber: 3
issuer: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
thisUpdate: UTC: "110101083000Z"
crlExtension:
deltaCRLIndicator: critical
BaseCRLNumber: 1
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by deltaCRL CA2 Cert
post to deltaRevocationList

6.1.5.539 Valid deltaCRL Test8 EE:

base: Base End Certificate
serial number: 1

issuer: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Valid deltaCRL EE Certificate Test8, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
signed by deltaCRL CA2 Cert

6.1.5.540 Invalid deltaCRL Test9 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRL EE Certificate Test9, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA2, o=Test Certificates 2011, c=US"
signed by deltaCRL CA2 Cert

6.1.5.541 deltaCRL CA3 Cert:

base: Base Intermediate Certificate
serial number: 93
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.542 deltaCRL CA3 CRL:

base: Base CRL
issuer: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
nextUpdate: UTC: "100601083000Z"
crlExtension:
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
signed by deltaCRL CA3 Cert

post to certificateRevocationList

6.1.5.543 deltaCRL CA3 deltaCRL:

base: Base CRL
crlNumber: 3
issuer: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
thisUpdate: UTC: "100601083000Z"
crlExtension:
deltaCRLIndicator: critical
BaseCRLNumber: 2
signed by deltaCRL CA3 Cert
post to deltaRevocationList

6.1.5.544 Invalid deltaCRL Test10 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
subject: "cn=Invalid deltaCRL EE Certificate Test10, o=Test Certificates 2011, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
freshestCRL: not critical
distributionPoint:
fullName:
directoryName: "cn=deltaCRL CA3, o=Test Certificates 2011, c=US"
signed by deltaCRL CA3 Cert

6.1.5.545 Valid Unknown Not Critical Certificate Extension Test1 EE:

base: Base End Certificate
serial number: 94
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Valid Unknown Not Critical Certificate Extension EE Cert Test1, o=Test Certificates 2011, c=US"
privateExtension: not critical
privateNumber: 0
signed by Trust Anchor Root Certificate

6.1.5.546 Invalid Unknown Critical Certificate Extension Test2 EE:

base: Base End Certificate
serial number: 95
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Unknown Critical Certificate Extension EE Cert Test2, o=Test Certificates 2011, c=US"
privateExtension: critical
privateNumber: 0
signed by Trust Anchor Root Certificate

6.1.5.547 RFC3280 Mandatory Attribute Types CA Cert:

base: Base Intermediate Certificate
serial number: 96
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "dnQualifier=CA, serialNumber=345, st=Maryland, dc=testcertificates, dc=gov, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.548 RFC3280 Mandatory Attribute Types CA CRL:

base: Base CRL
issuer: "dnQualifier=CA, serialNumber=345, st=Maryland, dc=testcertificates, dc=gov, o=Test Certificates 2011, c=US"
signed by RFC3280 Mandatory Attribute Types CA Cert
post to certificateRevocationList

6.1.5.549 Valid RFC3280 Mandatory Attribute Types Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "dnQualifier=CA, serialNumber=345, st=Maryland, dc=testcertificates, dc=gov, o=Test Certificates 2011, c=US"
subject: "cn=Valid RFC3280 Mandatory Attribute Types EE Certificate Test7, o=Test Certificates 2011, c=US"
signed by RFC3280 Mandatory Attribute Types CA Cert

6.1.5.550 RFC3280 Optional Attribute Types CA Cert:

base: Base Intermediate Certificate
serial number: 97
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "title=M.D., generationQualifier=III, sn=CA, pseudonym=Fictitious, initials=Q, givenName=John, l=Gaithersburg, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.551 RFC3280 Optional Attribute Types CA CRL:

base: Base CRL
issuer: "title=M.D., generationQualifier=III, sn=CA, pseudonym=Fictitious, initials=Q, givenName=John, l=Gaithersburg, o=Test Certificates 2011, c=US"
signed by RFC3280 Optional Attribute Types CA Cert
post to certificateRevocationList

6.1.5.552 Valid RFC3280 Optional Attribute Types Test8 EE:

base: Base End Certificate
serial number: 1
issuer: "title=M.D., generationQualifier=III, sn=CA, pseudonym=Fictitious, initials=Q, givenName=John, l=Gaithersburg, o=Test Certificates 2011, c=US"
subject: "cn=Valid RFC3280 Optional Attribute Types EE Certificate Test8, o=Test Certificates 2011, c=US"
signed by RFC3280 Optional Attribute Types CA Cert

6.1.5.553 UTF8String Encoded Names CA Cert:

base: Base Intermediate Certificate
serial number: 98
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=#0C0D55544638537472696E67204341,
o=#0C1154657374204365727469666696361746573, c=US"
signed by Trust Anchor Root Certificate

6.1.5.554 UTF8String Encoded Names CA CRL:

base: Base CRL
issuer: "cn=#0C0D55544638537472696E67204341,
o=#0C1154657374204365727469666696361746573, c=US"
signed by UTF8String Encoded Names CA Cert
post to certificateRevocationList

6.1.5.555 Valid UTF8String Encoded Names Test9 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=#0C0D55544638537472696E67204341,
o=#0C1154657374204365727469666696361746573, c=US"
subject:
"cn=#0C3356616C6964205544638537472696E6720456E636F646564204E616D6573204545204365727469666696361746520546573743439, o=#0C1154657374204365727469666696361746573,
c=US"
signed by UTF8String Encoded Names CA Cert

6.1.5.556 Rollover from PrintableString to UTF8String CA Cert:

base: Base Intermediate Certificate
serial number: 99
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Rollover from PrintableString to UTF8String CA, o=Test Certificates 2011, c=US"
signed by Trust Anchor Root Certificate

6.1.5.557 Rollover from PrintableString to UTF8String CA CRL:

base: Base CRL
issuer:
"cn=#0C2E526F6C6C6F7665722066726F6D205072696E7461626C65537472696E6720746F20
55544638537472696E67204341, o=#0C1154657374204365727469666696361746573, c=US"
signed by Rollover from PrintableString to UTF8String CA Cert
post to certificateRevocationList

6.1.5.558 Valid Rollover from PrintableString to UTF8String Test10 EE:

base: Base End Certificate
serial number: 1
issuer:
"cn=#0C2E526F6C6C6F7665722066726F6D205072696E7461626C65537472696E6720746F20
55544638537472696E67204341, o=#0C1154657374204365727469666696361746573, c=US"
subject:

"cn=#0C3B56616C696420526F6C6C6F766572205072696E7461626C65537472696E6720746F
20555446385374726 96E67204545204365727420546573743130,
o=#0C11546573742043657274696696361746573, c=US"
signed by Rollover from PrintableString to UTF8String CA Cert

6.1.5.559 UTF8String Case Insensitive Match CA Cert:

base: Base Intermediate Certificate
serial number: 100
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject:
"cn=#0C2455544638537472696E6720436173652049 6E73656E736974697665204D6174636820
4341, o=#0C11546573742043657274696696361746573, c=US"
signed by Trust Anchor Root Certificate

6.1.5.560 UTF8String Case Insensitive Match CA CRL:

base: Base CRL
issuer:
"cn=#0C2455544638537472696E6720436173652049 6E73656E736974697665204D6174636820
4341, o=#0C11546573742043657274696696361746573, c=US"
signed by UTF8String Case Insensitive Match CA Cert
post to certificateRevocationList

6.1.5.561 Valid UTF8String Case Insensitive Match Test11 EE:

base: Base End Certificate
serial number: 1
issuer:
"cn=#0C2575746638737472696E6720636173652020696E73656E736974697665206D61746368
204341, o=#0C15202074657374206365727469666963617465732020, c=US"
subject:
"cn=#0C3D56616C6964205544638537472696E6720436173652049 6E73656E7369746976652
04D617463682045452043657274696669636174652054657374 3131,
o=#0C11546573742043657274696696361746573, c=US"
signed by UTF8String Case Insensitive Match CA Cert

6.1.5.562 Invalid DNS nameConstraints Test38 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=nameConstraints DNS1 CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DNS nameConstraints EE Certificate Test38, o=Test Certificates 2011,
c=US"
subjectAltNameExtension:
dnsName: mytestcertificates.gov
signed by nameConstraints DNS1 CA Cert

6.1.5.563 Separate Certificate and CRL Keys Certificate Signing CA Cert:

base: Base Intermediate Certificate
serial number: 101
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"

subject: "cn=Separate Certificate and CRL Keys CA1, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.564 Separate Certificate and CRL Keys CRL Signing Cert:

base: Base End Certificate
serial number: 102
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Separate Certificate and CRL Keys CA1, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: True
digitalSignature: False
nonRepudiation: False
keyEncipherment: False
dataEncipherment: False
signed by Trust Anchor Root Certificate

6.1.5.565 Separate Certificate and CRL Keys CRL:

base: Base CRL
issuer: "cn=Separate Certificate and CRL Keys CA1, o=Test Certificates 2011, c=US"
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Separate Certificate and CRL Keys CRL Signing Cert
post to certificateRevocationList

6.1.5.566 Valid Separate Certificate and CRL Keys Test19 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Separate Certificate and CRL Keys CA1, o=Test Certificates 2011, c=US"
subject: "cn=Valid Separate Certificate and CRL Keys EE Certificate Test19, o=Test Certificates 2011, c=US"
signed by Separate Certificate and CRL Keys Certificate Signing CA Cert

6.1.5.567 Invalid Separate Certificate and CRL Keys Test20 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Separate Certificate and CRL Keys CA1, o=Test Certificates 2011, c=US"
subject: "cn=Invalid Separate Certificate and CRL Keys EE Certificate Test20, o=Test Certificates 2011, c=US"
signed by Separate Certificate and CRL Keys Certificate Signing CA Cert

6.1.5.568 Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert:

base: Base Intermediate Certificate

serial number: 103
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Separate Certificate and CRL Keys CA2, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: False
signed by Trust Anchor Root Certificate

6.1.5.569 Separate Certificate and CRL Keys CA2 CRL Signing Cert:

base: Base End Certificate
serial number: 104
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=Separate Certificate and CRL Keys CA2, o=Test Certificates 2011, c=US"
keyUsageExtension: critical
cRLSign: True
digitalSignature: False
nonRepudiation: False
keyEncipherment: False
dataEncipherment: False
signed by Trust Anchor Root Certificate

6.1.5.570 Separate Certificate and CRL Keys CA2 CRL:

base: Base CRL
issuer: "cn=Separate Certificate and CRL Keys CA2, o=Test Certificates 2011, c=US"
signed by Separate Certificate and CRL Keys CA2 CRL Signing Cert
post to certificateRevocationList

6.1.5.571 Invalid Separate Certificate and CRL Keys Test21 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Separate Certificate and CRL Keys CA2, o=Test Certificates 2011, c=US "
subject: "cn=Invalid Separate Certificate and CRL Keys EE Certificate Test21, o=Test Certificates 2011, c=US"
signed by Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert

6.1.5.572 DSA CA Cert:

base: Base Intermediate Certificate
serial number: 2001
issuer: "cn=Trust Anchor, o=Test Certificates 2011, c=US"
subject: "cn=DSA CA, o=Test Certificates 2011, c=US"
subjectPublicKey: DSA key
signed by Trust Anchor Root Certificate

6.1.5.573 DSA CA CRL:

base: Base CRL
issuer: "cn=DSA CA, o=Test Certificates 2011, c=US"
signed by DSA CA Cert
post to certificateRevocationList

6.1.5.574 Valid DSA Signatures Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=DSA CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DSA Signatures EE Certificate Test4, o=Test Certificates 2011, c=US"
subjectPublicKey: DSA key
signed by DSA CA Cert

6.1.5.575 DSA Parameters Inherited CA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=DSA CA, o=Test Certificates 2011, c=US"
subject: "cn=DSA Parameters Inherited CA, o=Test Certificates 2011, c=US"
subjectPublicKey: DSA key with parameters inherited
signed by DSA CA Cert

6.1.5.576 DSA Parameters Inherited CA CRL:

base: Base CRL
issuer: "cn=DSA Parameters Inherited CA, o=Test Certificates 2011, c=US"
signed by DSA Parameters Inherited CA Cert
post to certificateRevocationList

6.1.5.577 Valid DSA Parameter Inheritance Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=DSA Parameters Inherited CA, o=Test Certificates 2011, c=US"
subject: "cn=Valid DSA Parameter Inheritance EE Certificate Test5, o=Test Certificates 2011, c=US"
subjectPublicKey: DSA key with parameters inherited
signed by DSA Parameters Inherited CA Cert

6.1.5.578 Invalid DSA Signature Test6 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=DSA CA, o=Test Certificates 2011, c=US"
subject: "cn=Invalid DSA Signature EE Certificate Test6, o=Test Certificates 2011, c=US"
subjectPublicKey: DSA key
signed by DSA CA Cert (one or more bits in the signature is modified)

6.1.6 Cross Certificate Pairs

RFC 2587 states that "[t]he forward elements of the crossCertificatePair attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the crossCertificatePair attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs." This section specifies the **crossCertificatePairs** that are to be generated for each cross-certificate specified in the previous section.

For each **crossCertificatePair** in which the **forward** [**issuedToThisCA**] element is populated, the

crossCertificatePair is placed in the directory entry identified by the subject DN of the certificate. For each **crossCertificatePair** in which the **reverse** [**issuedByThisCA**] element is populated, the **crossCertificatePair** is stored in the directory entry identified by the issuer DN of the certificate.

6.1.6.1 Good CA Cert forward crossCertificatePair:

forward: Good CA Cert
reverse: absent

6.1.6.2 Good CA Cert reverse crossCertificatePair:

forward: absent
reverse: Good CA Cert

6.1.6.3 Bad Signed CA Cert forward crossCertificatePair:

forward: Bad Signed CA Cert
reverse: absent

6.1.6.4 Bad Signed CA Cert reverse crossCertificatePair:

forward: absent
reverse: Bad Signed CA Cert

6.1.6.5 Bad notBefore Date CA Cert forward crossCertificatePair:

forward: Bad notBefore Date CA Cert
reverse: absent

6.1.6.6 Bad notBefore Date CA Cert reverse crossCertificatePair:

forward: absent
reverse: Bad notBefore Date CA Cert

6.1.6.7 Bad notAfter Date CA Cert forward crossCertificatePair:

forward: Bad notAfter Date CA Cert
reverse: absent

6.1.6.8 Bad notAfter Date CA Cert reverse crossCertificatePair:

forward: absent
reverse: Bad notAfter Date CA Cert

6.1.6.9 Name Ordering CA Cert forward crossCertificatePair:

forward: Name Ordering CA Cert
reverse: absent

6.1.6.10 Name Ordering CA Cert reverse crossCertificatePair:

forward: absent
reverse: Name Ordering CA Cert

6.1.6.11 UID CA Cert forward crossCertificatePair:

forward: UID CA Cert
reverse: absent

6.1.6.12 UID CA Cert reverse crossCertificatePair:

forward: absent
reverse: UID CA Cert

6.1.6.13 No CRL CA Cert forward crossCertificatePair:

forward: No CRL CA Cert
reverse: absent

6.1.6.14 No CRL CA Cert reverse crossCertificatePair:

forward: absent
reverse: No CRL CA Cert

6.1.6.15 Revoked subCA Cert forward crossCertificatePair:

forward: Revoked subCA Cert
reverse: absent

6.1.6.16 Revoked subCA Cert reverse crossCertificatePair:

forward: absent
reverse: Revoked subCA Cert

6.1.6.17 Bad CRL Signature CA Cert forward crossCertificatePair:

forward: Bad CRL Signature CA Cert
reverse: absent

6.1.6.18 Bad CRL Signature CA Cert reverse crossCertificatePair:

forward: absent
reverse: Bad CRL Signature CA Cert

6.1.6.19 Bad CRL Issuer Name CA Cert forward crossCertificatePair:

forward: Bad CRL Issuer Name CA Cert
reverse: absent

6.1.6.20 Bad CRL Issuer Name CA Cert reverse crossCertificatePair:

forward: absent
reverse: Bad CRL Issuer Name CA Cert

6.1.6.21 Wrong CRL CA Cert forward crossCertificatePair:

forward: Wrong CRL CA Cert
reverse: absent

6.1.6.22 Wrong CRL CA Cert reverse crossCertificatePair:

forward: absent
reverse: Wrong CRL CA Cert

6.1.6.23 Two CRLs CA Cert forward crossCertificatePair:

forward: Two CRLs CA Cert
reverse: absent

6.1.6.24 Two CRLs CA Cert reverse crossCertificatePair:

forward: absent
reverse: Two CRLs CA Cert

6.1.6.25 Unknown CRL Entry Extension CA Cert forward crossCertificatePair:

forward: Unknown CRL Entry Extension CA Cert
reverse: absent

6.1.6.26 Unknown CRL Entry Extension CA Cert reverse crossCertificatePair:

forward: absent
reverse: Unknown CRL Entry Extension CA Cert

6.1.6.27 Unknown CRL Extension CA Cert forward crossCertificatePair:

forward: Unknown CRL Extension CA Cert
reverse: absent

6.1.6.28 Unknown CRL Extension CA Cert reverse crossCertificatePair:

forward: absent
reverse: Unknown CRL Extension CA Cert

6.1.6.29 Old CRL nextUpdate CA Cert forward crossCertificatePair:

forward: Old CRL nextUpdate CA Cert
reverse: absent

6.1.6.30 Old CRL nextUpdate CA Cert reverse crossCertificatePair:

forward: absent
reverse: Old CRL nextUpdate CA Cert

6.1.6.31 pre2000 CRL nextUpdate CA Cert forward crossCertificatePair:

forward: pre2000 CRL nextUpdate CA Cert
reverse: absent

6.1.6.32 pre2000 CRL nextUpdate CA Cert reverse crossCertificatePair:

forward: absent
reverse: pre2000 CRL nextUpdate CA Cert

6.1.6.33 GeneralizedTime CRL nextUpdate CA Cert forward crossCertificatePair:

forward: GeneralizedTime CRL nextUpdate CA Cert
reverse: absent

6.1.6.34 GeneralizedTime CRL nextUpdate CA Cert reverse crossCertificatePair:

forward: absent
reverse: GeneralizedTime CRL nextUpdate CA Cert

6.1.6.35 Negative Serial Number CA Cert forward crossCertificatePair:

forward: Negative Serial Number CA Cert
reverse: absent

6.1.6.36 Negative Serial Number CA Cert reverse crossCertificatePair:

forward: absent
reverse: Negative Serial Number CA Cert

6.1.6.37 Long Serial Number CA Cert forward crossCertificatePair:

forward: Long Serial Number CA Cert
reverse: absent

6.1.6.38 Long Serial Number CA Cert reverse crossCertificatePair:

forward: absent
reverse: Long Serial Number CA Cert

6.1.6.39 Basic Self-Issued New Key CA Cert forward crossCertificatePair:

forward: Basic Self-Issued New Key CA Cert
reverse: absent

6.1.6.40 Basic Self-Issued New Key CA Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Self-Issued New Key CA Cert

6.1.6.41 Basic Self-Issued Old Key CA Cert forward crossCertificatePair:

forward: Basic Self-Issued Old Key CA Cert
reverse: absent

6.1.6.42 Basic Self-Issued Old Key CA Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Self-Issued Old Key CA Cert

6.1.6.43 Basic Self-Issued CRL Signing Key CA Cert forward crossCertificatePair:

forward: Basic Self-Issued CRL Signing Key CA Cert
reverse: absent

6.1.6.44 Basic Self-Issued CRL Signing Key CA Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Self-Issued CRL Signing Key CA Cert

6.1.6.45 Missing basicConstraints CA Cert forward crossCertificatePair:

forward: Missing basicConstraints CA Cert
reverse: absent

6.1.6.46 Missing basicConstraints CA Cert reverse crossCertificatePair:

forward: absent
reverse: Missing basicConstraints CA Cert

6.1.6.47 basicConstraints Critical cA False CA Cert forward crossCertificatePair:

forward: basicConstraints Critical cA False CA Cert
reverse: absent

6.1.6.48 basicConstraints Critical cA False CA Cert reverse crossCertificatePair:

forward: absent
reverse: basicConstraints Critical cA False CA Cert

6.1.6.49 basicConstraints Not Critical cA False CA Cert forward crossCertificatePair:

forward: basicConstraints Not Critical cA False CA Cert
reverse: absent

6.1.6.50 basicConstraints Not Critical cA False CA Cert reverse crossCertificatePair:

forward: absent
reverse: basicConstraints Not Critical cA False CA Cert

6.1.6.51 basicConstraints Not Critical CA Cert forward crossCertificatePair:

forward: basicConstraints Not Critical CA Cert
reverse: absent

6.1.6.52 basicConstraints Not Critical CA Cert reverse crossCertificatePair:

forward: absent
reverse: basicConstraints Not Critical CA Cert

6.1.6.53 pathLenConstraint0 CA Cert forward crossCertificatePair:

forward: pathLenConstraint0 CA Cert
reverse: absent

6.1.6.54 pathLenConstraint0 CA Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint0 CA Cert

6.1.6.55 Invalid pathLenConstraint Test6 EE forward crossCertificatePair:

forward: Invalid pathLenConstraint Test6 EE
reverse: absent

6.1.6.56 Invalid pathLenConstraint Test6 EE reverse crossCertificatePair:

forward: absent
reverse: Invalid pathLenConstraint Test6 EE

6.1.6.57 Valid pathLenConstraint Test8 EE forward crossCertificatePair:

forward: Valid pathLenConstraint Test8 EE
reverse: absent

6.1.6.58 Valid pathLenConstraint Test8 EE reverse crossCertificatePair:

forward: absent
reverse: Valid pathLenConstraint Test8 EE

6.1.6.59 pathLenConstraint0 subCA Cert forward crossCertificatePair:

forward: pathLenConstraint0 subCA Cert
reverse: absent

6.1.6.60 pathLenConstraint0 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint0 subCA Cert

6.1.6.61 pathLenConstraint6 CA Cert forward crossCertificatePair:

forward: pathLenConstraint6 CA Cert
reverse: absent

6.1.6.62 pathLenConstraint6 CA Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 CA Cert

6.1.6.63 pathLenConstraint6 subCA0 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subCA0 Cert
reverse: absent

6.1.6.64 pathLenConstraint6 subCA0 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subCA0 Cert

6.1.6.65 pathLenConstraint6 subsubCA00 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subsubCA00 Cert
reverse: absent

6.1.6.66 pathLenConstraint6 subsubCA00 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subsubCA00 Cert

6.1.6.67 Invalid pathLenConstraint Test10 EE forward crossCertificatePair:

forward: Invalid pathLenConstraint Test10 EE
reverse: absent

6.1.6.68 Invalid pathLenConstraint Test10 EE reverse crossCertificatePair:

forward: absent
reverse: Invalid pathLenConstraint Test10 EE

6.1.6.69 pathLenConstraint6 subCA1 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subCA1 Cert
reverse: absent

6.1.6.70 pathLenConstraint6 subCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subCA1 Cert

6.1.6.71 pathLenConstraint6 subsubCA11 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subsubCA11 Cert
reverse: absent

6.1.6.72 pathLenConstraint6 subsubCA11 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subsubCA11 Cert

6.1.6.73 pathLenConstraint6 subsubsubCA11X Cert forward crossCertificatePair:

forward: pathLenConstraint6 subsubsubCA11X Cert
reverse: absent

6.1.6.74 pathLenConstraint6 subsubsubCA11X Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subsubsubCA11X Cert

6.1.6.75 Invalid pathLenConstraint Test12 EE forward crossCertificatePair:

forward: Invalid pathLenConstraint Test12 EE
reverse: absent

6.1.6.76 Invalid pathLenConstraint Test12 EE reverse crossCertificatePair:

forward: absent
reverse: Invalid pathLenConstraint Test12 EE

6.1.6.77 pathLenConstraint6 subCA4 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subCA4 Cert
reverse: absent

6.1.6.78 pathLenConstraint6 subCA4 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subCA4 Cert

6.1.6.79 pathLenConstraint6 subsubCA41 Cert forward crossCertificatePair:

forward: pathLenConstraint6 subsubCA41 Cert
reverse: absent

6.1.6.80 pathLenConstraint6 subsubCA41 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subsubCA41 Cert

6.1.6.81 pathLenConstraint6 subsubsubCA41X Cert forward crossCertificatePair:

forward: pathLenConstraint6 subsubsubCA41X Cert
reverse: absent

6.1.6.82 pathLenConstraint6 subsubsubCA41X Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint6 subsubsubCA41X Cert

6.1.6.83 Valid pathLenConstraint Test14 EE forward crossCertificatePair:

forward: Valid pathLenConstraint Test14 EE
reverse: absent

6.1.6.84 Valid pathLenConstraint Test14 EE reverse crossCertificatePair:

forward: absent
reverse: Valid pathLenConstraint Test14 EE

6.1.6.85 pathLenConstraint0 subCA2 Cert forward crossCertificatePair:

forward: pathLenConstraint0 subCA2 Cert
reverse: absent

6.1.6.86 pathLenConstraint0 subCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint0 subCA2 Cert

6.1.6.87 pathLenConstraint1 CA Cert forward crossCertificatePair:

forward: pathLenConstraint1 CA Cert
reverse: absent

6.1.6.88 pathLenConstraint1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint1 CA Cert

6.1.6.89 pathLenConstraint1 subCA Cert forward crossCertificatePair:

forward: pathLenConstraint1 subCA Cert
reverse: absent

6.1.6.90 pathLenConstraint1 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: pathLenConstraint1 subCA Cert

6.1.6.91 keyUsage Critical keyCertSign False CA Cert forward crossCertificatePair:

forward: keyUsage Critical keyCertSign False CA Cert
reverse: absent

6.1.6.92 keyUsage Critical keyCertSign False CA Cert reverse crossCertificatePair:

forward: absent
reverse: keyUsage Critical keyCertSign False CA Cert

6.1.6.93 keyUsage Not Critical keyCertSign False CA Cert forward crossCertificatePair:

forward: keyUsage Not Critical keyCertSign False CA Cert
reverse: absent

6.1.6.94 keyUsage Not Critical keyCertSign False CA Cert reverse crossCertificatePair:

forward: absent
reverse: keyUsage Not Critical keyCertSign False CA Cert

6.1.6.95 keyUsage Not Critical CA Cert forward crossCertificatePair:

forward: keyUsage Not Critical CA Cert
reverse: absent

6.1.6.96 keyUsage Not Critical CA Cert reverse crossCertificatePair:

forward: absent
reverse: keyUsage Not Critical CA Cert

6.1.6.97 keyUsage Critical cRLSign False CA Cert forward crossCertificatePair:

forward: keyUsage Critical cRLSign False CA Cert
reverse: absent

6.1.6.98 keyUsage Critical cRLSign False CA Cert reverse crossCertificatePair:

forward: absent
reverse: keyUsage Critical cRLSign False CA Cert

6.1.6.99 keyUsage Not Critical cRLSign False CA Cert forward crossCertificatePair:

forward: keyUsage Not Critical cRLSign False CA Cert
reverse: absent

6.1.6.100 keyUsage Not Critical cRLSign False CA Cert reverse crossCertificatePair:

forward: absent
reverse: keyUsage Not Critical cRLSign False CA Cert

6.1.6.101 No Policies CA Cert forward crossCertificatePair:

forward: No Policies CA Cert
reverse: absent

6.1.6.102 No Policies CA Cert reverse crossCertificatePair:

forward: absent
reverse: No Policies CA Cert

6.1.6.103 Policies P2 subCA Cert forward crossCertificatePair:

forward: Policies P2 subCA Cert
reverse: absent

6.1.6.104 Policies P2 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P2 subCA Cert

6.1.6.105 Good subCA Cert forward crossCertificatePair:

forward: Good subCA Cert
reverse: absent

6.1.6.106 Good subCA Cert reverse crossCertificatePair:

forward: absent
reverse: Good subCA Cert

6.1.6.107 Policies P2 subCA2 Cert forward crossCertificatePair:

forward: Policies P2 subCA2 Cert
reverse: absent

6.1.6.108 Policies P2 subCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P2 subCA2 Cert

6.1.6.109 Policies P1234 CA Cert forward crossCertificatePair:

forward: Policies P1234 CA Cert
reverse: absent

6.1.6.110 Policies P1234 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P1234 CA Cert

6.1.6.111 Policies P1234 subCAP123 Cert forward crossCertificatePair:

forward: Policies P1234 subCAP123 Cert
reverse: absent

6.1.6.112 Policies P1234 subCAP123 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P1234 subCAP123 Cert

6.1.6.113 Policies P1234 subsubCAP123P12 Cert forward crossCertificatePair:

forward: Policies P1234 subsubCAP123P12 Cert
reverse: absent

6.1.6.114 Policies P1234 subsubCAP123P12 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P1234 subsubCAP123P12 Cert

6.1.6.115 Overlapping Policies Test6 EE forward crossCertificatePair:

forward: Overlapping Policies Test6 EE
reverse: absent

6.1.6.116 Overlapping Policies Test6 EE reverse crossCertificatePair:

forward: absent
reverse: Overlapping Policies Test6 EE

6.1.6.117 Policies P123 CA Cert forward crossCertificatePair:

forward: Policies P123 CA Cert
reverse: absent

6.1.6.118 Policies P123 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P123 CA Cert

6.1.6.119 Policies P123 subCAP12 Cert forward crossCertificatePair:

forward: Policies P123 subCAP12 Cert
reverse: absent

6.1.6.120 Policies P123 subCAP12 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P123 subCAP12 Cert

6.1.6.121 Policies P123 subsubCAP12P1 Cert forward crossCertificatePair:

forward: Policies P123 subsubCAP12P1 Cert
reverse: absent

6.1.6.122 Policies P123 subsubCAP12P1 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P123 subsubCAP12P1 Cert

6.1.6.123 Different Policies Test7 EE forward crossCertificatePair:

forward: Different Policies Test7 EE
reverse: absent

6.1.6.124 Different Policies Test7 EE reverse crossCertificatePair:

forward: absent
reverse: Different Policies Test7 EE

6.1.6.125 Policies P12 CA Cert forward crossCertificatePair:

forward: Policies P12 CA Cert
reverse: absent

6.1.6.126 Policies P12 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P12 CA Cert

6.1.6.127 Policies P12 subCAP1 Cert forward crossCertificatePair:

forward: Policies P12 subCAP1 Cert
reverse: absent

6.1.6.128 Policies P12 subCAP1 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P12 subCAP1 Cert

6.1.6.129 Policies P12 subsubCAP1P2 Cert forward crossCertificatePair:

forward: Policies P12 subsubCAP1P2 Cert
reverse: absent

6.1.6.130 Policies P12 subsubCAP1P2 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P12 subsubCAP1P2 Cert

6.1.6.131 Different Policies Test8 EE forward crossCertificatePair:

forward: Different Policies Test8 EE
reverse: absent

6.1.6.132 Different Policies Test8 EE reverse crossCertificatePair:

forward: absent
reverse: Different Policies Test8 EE

6.1.6.133 Policies P123 subsubCAP12P2 Cert forward crossCertificatePair:

forward: Policies P123 subsubCAP12P2 Cert
reverse: absent

6.1.6.134 Policies P123 subsubCAP12P2 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P123 subsubCAP12P2 Cert

6.1.6.135 Policies P123 subsubsubCAP12P2P1 Cert forward crossCertificatePair:

forward: Policies P123 subsubsubCAP12P2P1 Cert
reverse: absent

6.1.6.136 Policies P123 subsubsubCAP12P2P1 Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P123 subsubsubCAP12P2P1 Cert

6.1.6.137 anyPolicy CA Cert forward crossCertificatePair:

forward: anyPolicy CA Cert
reverse: absent

6.1.6.138 anyPolicy CA Cert reverse crossCertificatePair:

forward: absent
reverse: anyPolicy CA Cert

6.1.6.139 Policies P3 CA Cert forward crossCertificatePair:

forward: Policies P3 CA Cert
reverse: absent

6.1.6.140 Policies P3 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Policies P3 CA Cert

6.1.6.141 requireExplicitPolicy10 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy10 CA Cert
reverse: absent

6.1.6.142 requireExplicitPolicy10 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy10 CA Cert

6.1.6.143 requireExplicitPolicy10 subCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy10 subCA Cert
reverse: absent

6.1.6.144 requireExplicitPolicy10 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy10 subCA Cert

6.1.6.145 requireExplicitPolicy10 subsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy10 subsubCA Cert
reverse: absent

6.1.6.146 requireExplicitPolicy10 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy10 subsubCA Cert

6.1.6.147 requireExplicitPolicy10 subsubsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy10 subsubsubCA Cert
reverse: absent

6.1.6.148 requireExplicitPolicy10 subsubsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy10 subsubsubCA Cert

6.1.6.149 requireExplicitPolicy5 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy5 CA Cert
reverse: absent

6.1.6.150 requireExplicitPolicy5 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy5 CA Cert

6.1.6.151 requireExplicitPolicy5 subCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy5 subCA Cert
reverse: absent

6.1.6.152 requireExplicitPolicy5 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy5 subCA Cert

6.1.6.153 requireExplicitPolicy5 subsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy5 subsubCA Cert
reverse: absent

6.1.6.154 requireExplicitPolicy5 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy5 subsubCA Cert

6.1.6.155 requireExplicitPolicy5 subsubsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy5 subsubsubCA Cert
reverse: absent

6.1.6.156 requireExplicitPolicy5 subsubsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy5 subsubsubCA Cert

6.1.6.157 requireExplicitPolicy4 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy4 CA Cert
reverse: absent

6.1.6.158 requireExplicitPolicy4 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy4 CA Cert

6.1.6.159 requireExplicitPolicy4 subCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy4 subCA Cert
reverse: absent

6.1.6.160 requireExplicitPolicy4 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy4 subCA Cert

6.1.6.161 requireExplicitPolicy4 subsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy4 subsubCA Cert
reverse: absent

6.1.6.162 requireExplicitPolicy4 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy4 subsubCA Cert

6.1.6.163 requireExplicitPolicy4 subsubsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy4 subsubsubCA Cert
reverse: absent

6.1.6.164 requireExplicitPolicy4 subsubsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy4 subsubsubCA Cert

6.1.6.165 requireExplicitPolicy0 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy0 CA Cert
reverse: absent

6.1.6.166 requireExplicitPolicy0 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy0 CA Cert

6.1.6.167 requireExplicitPolicy0 subCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy0 subCA Cert
reverse: absent

6.1.6.168 requireExplicitPolicy0 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy0 subCA Cert

6.1.6.169 requireExplicitPolicy0 subsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy0 subsubCA Cert
reverse: absent

6.1.6.170 requireExplicitPolicy0 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy0 subsubCA Cert

6.1.6.171 requireExplicitPolicy0 subsubsubCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy0 subsubsubCA Cert
reverse: absent

6.1.6.172 requireExplicitPolicy0 subsubsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy0 subsubsubCA Cert

6.1.6.173 requireExplicitPolicy7 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy7 CA Cert
reverse: absent

6.1.6.174 requireExplicitPolicy7 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy7 CA Cert

6.1.6.175 requireExplicitPolicy7 subCARE2 Cert forward crossCertificatePair:

forward: requireExplicitPolicy7 subCARE2 Cert
reverse: absent

6.1.6.176 requireExplicitPolicy7 subCARE2 Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy7 subCARE2 Cert

6.1.6.177 requireExplicitPolicy7 subsubCARE2RE4 Cert forward crossCertificatePair:

forward: requireExplicitPolicy7 subsubCARE2RE4 Cert
reverse: absent

6.1.6.178 requireExplicitPolicy7 subsubCARE2RE4 Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy7 subsubCARE2RE4 Cert

6.1.6.179 requireExplicitPolicy7 subsubsubCARE2RE4 Cert forward crossCertificatePair:

forward: requireExplicitPolicy7 subsubsubCARE2RE4 Cert
reverse: absent

6.1.6.180 requireExplicitPolicy7 subsubsubCARE2RE4 Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy7 subsubsubCARE2RE4 Cert

6.1.6.181 requireExplicitPolicy2 CA Cert forward crossCertificatePair:

forward: requireExplicitPolicy2 CA Cert
reverse: absent

6.1.6.182 requireExplicitPolicy2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy2 CA Cert

6.1.6.183 requireExplicitPolicy2 subCA Cert forward crossCertificatePair:

forward: requireExplicitPolicy2 subCA Cert
reverse: absent

6.1.6.184 requireExplicitPolicy2 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: requireExplicitPolicy2 subCA Cert

6.1.6.185 Mapping 1to2 CA Cert forward crossCertificatePair:

forward: Mapping 1to2 CA Cert
reverse: absent

6.1.6.186 Mapping 1to2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Mapping 1to2 CA Cert

6.1.6.187 P12 Mapping 1to3 CA Cert forward crossCertificatePair:

forward: P12 Mapping 1to3 CA Cert
reverse: absent

6.1.6.188 P12 Mapping 1to3 CA Cert reverse crossCertificatePair:

forward: absent
reverse: P12 Mapping 1to3 CA Cert

6.1.6.189 P12 Mapping 1to3 subCA Cert forward crossCertificatePair:

forward: P12 Mapping 1to3 subCA Cert
reverse: absent

6.1.6.190 P12 Mapping 1to3 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: P12 Mapping 1to3 subCA Cert

6.1.6.191 P12 Mapping 1to3 subsubCA Cert forward crossCertificatePair:

forward: P12 Mapping 1to3 subsubCA Cert
reverse: absent

6.1.6.192 P12 Mapping 1to3 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: P12 Mapping 1to3 subsubCA Cert

6.1.6.193 P1 Mapping 1to234 CA Cert forward crossCertificatePair:

forward: P1 Mapping 1to234 CA Cert
reverse: absent

6.1.6.194 P1 Mapping 1to234 CA Cert reverse crossCertificatePair:

forward: absent
reverse: P1 Mapping 1to234 CA Cert

6.1.6.195 P1 Mapping 1to234 subCA Cert forward crossCertificatePair:

forward: P1 Mapping 1to234 subCA Cert
reverse: absent

6.1.6.196 P1 Mapping 1to234 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: P1 Mapping 1to234 subCA Cert

6.1.6.197 Mapping From anyPolicy CA Cert forward crossCertificatePair:

forward: Mapping From anyPolicy CA Cert
reverse: absent

6.1.6.198 Mapping From anyPolicy CA Cert reverse crossCertificatePair:

forward: absent
reverse: Mapping From anyPolicy CA Cert

6.1.6.199 Mapping To anyPolicy CA Cert forward crossCertificatePair:

forward: Mapping To anyPolicy CA Cert
reverse: absent

6.1.6.200 Mapping To anyPolicy CA Cert reverse crossCertificatePair:

forward: absent
reverse: Mapping To anyPolicy CA Cert

6.1.6.201 PanyPolicy Mapping 1to2 CA Cert forward crossCertificatePair:

forward: PanyPolicy Mapping 1to2 CA Cert
reverse: absent

6.1.6.202 PanyPolicy Mapping 1to2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: PanyPolicy Mapping 1to2 CA Cert

6.1.6.203 Good subCA PanyPolicy Mapping 1to2 CA Cert forward crossCertificatePair:

forward: Good subCA PanyPolicy Mapping 1to2 CA Cert
reverse: absent

6.1.6.204 Good subCA PanyPolicy Mapping 1to2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: Good subCA PanyPolicy Mapping 1to2 CA Cert

6.1.6.205 P1anyPolicy Mapping 1to2 CA Cert forward crossCertificatePair:

forward: P1anyPolicy Mapping 1to2 CA Cert
reverse: absent

6.1.6.206 P1anyPolicy Mapping 1to2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: P1anyPolicy Mapping 1to2 CA Cert

6.1.6.207 inhibitPolicyMapping0 CA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping0 CA Cert
reverse: absent

6.1.6.208 inhibitPolicyMapping0 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping0 CA Cert

6.1.6.209 inhibitPolicyMapping0 subCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping0 subCA Cert
reverse: absent

6.1.6.210 inhibitPolicyMapping0 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping0 subCA Cert

6.1.6.211 inhibitPolicyMapping1 P12 CA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P12 CA Cert
reverse: absent

6.1.6.212 inhibitPolicyMapping1 P12 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P12 CA Cert

6.1.6.213 inhibitPolicyMapping1 P12 subCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P12 subCA Cert
reverse: absent

6.1.6.214 inhibitPolicyMapping1 P12 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P12 subCA Cert

6.1.6.215 inhibitPolicyMapping1 P12 subsubCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P12 subsubCA Cert
reverse: absent

6.1.6.216 inhibitPolicyMapping1 P12 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P12 subsubCA Cert

6.1.6.217 inhibitPolicyMapping5 CA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping5 CA Cert
reverse: absent

6.1.6.218 inhibitPolicyMapping5 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping5 CA Cert

6.1.6.219 inhibitPolicyMapping5 subCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping5 subCA Cert
reverse: absent

6.1.6.220 inhibitPolicyMapping5 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping5 subCA Cert

6.1.6.221 inhibitPolicyMapping5 subsubCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping5 subsubCA Cert
reverse: absent

6.1.6.222 inhibitPolicyMapping5 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping5 subsubCA Cert

6.1.6.223 inhibitPolicyMapping5 subsubsubCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping5 subsubsubCA Cert
reverse: absent

6.1.6.224 inhibitPolicyMapping5 subsubsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping5 subsubsubCA Cert

6.1.6.225 inhibitPolicyMapping1 P12 subCAIPM5 Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P12 subCAIPM5 Cert
reverse: absent

6.1.6.226 inhibitPolicyMapping1 P12 subCAIPM5 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P12 subCAIPM5 Cert

6.1.6.227 inhibitPolicyMapping1 P12 subsubCAIPM5 Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P12 subsubCAIPM5 Cert
reverse: absent

6.1.6.228 inhibitPolicyMapping1 P12 subsubCAIPM5 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P12 subsubCAIPM5 Cert

6.1.6.229 inhibitPolicyMapping1 P1 CA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P1 CA Cert
reverse: absent

6.1.6.230 inhibitPolicyMapping1 P1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P1 CA Cert

6.1.6.231 inhibitPolicyMapping1 P1 subCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P1 subCA Cert
reverse: absent

6.1.6.232 inhibitPolicyMapping1 P1 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P1 subCA Cert

6.1.6.233 inhibitPolicyMapping1 P1 subsubCA Cert forward crossCertificatePair:

forward: inhibitPolicyMapping1 P1 subsubCA Cert
reverse: absent

6.1.6.234 inhibitPolicyMapping1 P1 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitPolicyMapping1 P1 subsubCA Cert

6.1.6.235 inhibitAnyPolicy0 CA Cert forward crossCertificatePair:

forward: inhibitAnyPolicy0 CA Cert
reverse: absent

6.1.6.236 inhibitAnyPolicy0 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy0 CA Cert

6.1.6.237 inhibitAnyPolicy1 CA Cert forward crossCertificatePair:

forward: inhibitAnyPolicy1 CA Cert
reverse: absent

6.1.6.238 inhibitAnyPolicy1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy1 CA Cert

6.1.6.239 inhibitAnyPolicy1 subCA1 Cert forward crossCertificatePair:

forward: inhibitAnyPolicy1 subCA1 Cert
reverse: absent

6.1.6.240 inhibitAnyPolicy1 subCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy1 subCA1 Cert

6.1.6.241 inhibitAnyPolicy5 CA Cert forward crossCertificatePair:

forward: inhibitAnyPolicy5 CA Cert
reverse: absent

6.1.6.242 inhibitAnyPolicy5 CA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy5 CA Cert

6.1.6.243 inhibitAnyPolicy5 subCA Cert forward crossCertificatePair:

forward: inhibitAnyPolicy5 subCA Cert
reverse: absent

6.1.6.244 inhibitAnyPolicy5 subCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy5 subCA Cert

6.1.6.245 inhibitAnyPolicy5 subsubCA Cert forward crossCertificatePair:

forward: inhibitAnyPolicy5 subsubCA Cert
reverse: absent

6.1.6.246 inhibitAnyPolicy5 subsubCA Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy5 subsubCA Cert

6.1.6.247 inhibitAnyPolicy1 subCAIAP5 Cert forward crossCertificatePair:

forward: inhibitAnyPolicy1 subCAIAP5 Cert
reverse: absent

6.1.6.248 inhibitAnyPolicy1 subCAIAP5 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy1 subCAIAP5 Cert

6.1.6.249 inhibitAnyPolicy1 subCA2 Cert forward crossCertificatePair:

forward: inhibitAnyPolicy1 subCA2 Cert
reverse: absent

6.1.6.250 inhibitAnyPolicy1 subCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy1 subCA2 Cert

6.1.6.251 inhibitAnyPolicy1 subsubCA2 Cert forward crossCertificatePair:

forward: inhibitAnyPolicy1 subsubCA2 Cert
reverse: absent

6.1.6.252 inhibitAnyPolicy1 subsubCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: inhibitAnyPolicy1 subsubCA2 Cert

6.1.6.253 nameConstraints DN1 CA Cert forward crossCertificatePair:

forward: nameConstraints DN1 CA Cert
reverse: absent

6.1.6.254 nameConstraints DN1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN1 CA Cert

6.1.6.255 nameConstraints DN2 CA Cert forward crossCertificatePair:

forward: nameConstraints DN2 CA Cert
reverse: absent

6.1.6.256 nameConstraints DN2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN2 CA Cert

6.1.6.257 nameConstraints DN3 CA Cert forward crossCertificatePair:

forward: nameConstraints DN3 CA Cert
reverse: absent

6.1.6.258 nameConstraints DN3 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN3 CA Cert

6.1.6.259 nameConstraints DN4 CA Cert forward crossCertificatePair:

forward: nameConstraints DN4 CA Cert
reverse: absent

6.1.6.260 nameConstraints DN4 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN4 CA Cert

6.1.6.261 nameConstraints DN5 CA Cert forward crossCertificatePair:

forward: nameConstraints DN5 CA Cert
reverse: absent

6.1.6.262 nameConstraints DN5 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN5 CA Cert

6.1.6.263 nameConstraints DN1 subCA1 Cert forward crossCertificatePair:

forward: nameConstraints DN1 subCA1 Cert
reverse: absent

6.1.6.264 nameConstraints DN1 subCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN1 subCA1 Cert

6.1.6.265 nameConstraints DN1 subCA2 Cert forward crossCertificatePair:

forward: nameConstraints DN1 subCA2 Cert
reverse: absent

6.1.6.266 nameConstraints DN1 subCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN1 subCA2 Cert

6.1.6.267 nameConstraints DN3 subCA1 Cert forward crossCertificatePair:

forward: nameConstraints DN3 subCA1 Cert
reverse: absent

6.1.6.268 nameConstraints DN3 subCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN3 subCA1 Cert

6.1.6.269 nameConstraints DN3 subCA2 Cert forward crossCertificatePair:

forward: nameConstraints DN3 subCA2 Cert
reverse: absent

6.1.6.270 nameConstraints DN3 subCA2 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN3 subCA2 Cert

6.1.6.271 nameConstraints RFC822 CA1 Cert forward crossCertificatePair:

forward: nameConstraints RFC822 CA1 Cert
reverse: absent

6.1.6.272 nameConstraints RFC822 CA1 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints RFC822 CA1 Cert

6.1.6.273 nameConstraints RFC822 CA2 Cert forward crossCertificatePair:

forward: nameConstraints RFC822 CA2 Cert
reverse: absent

6.1.6.274 nameConstraints RFC822 CA2 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints RFC822 CA2 Cert

6.1.6.275 nameConstraints RFC822 CA3 Cert forward crossCertificatePair:

forward: nameConstraints RFC822 CA3 Cert
reverse: absent

6.1.6.276 nameConstraints RFC822 CA3 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints RFC822 CA3 Cert

6.1.6.277 nameConstraints DN1 subCA3 Cert forward crossCertificatePair:

forward: nameConstraints DN1 subCA3 Cert
reverse: absent

6.1.6.278 nameConstraints DN1 subCA3 Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DN1 subCA3 Cert

6.1.6.279 nameConstraints DNS1 CA Cert forward crossCertificatePair:

forward: nameConstraints DNS1 CA Cert
reverse: absent

6.1.6.280 nameConstraints DNS1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DNS1 CA Cert

6.1.6.281 nameConstraints DNS2 CA Cert forward crossCertificatePair:

forward: nameConstraints DNS2 CA Cert
reverse: absent

6.1.6.282 nameConstraints DNS2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints DNS2 CA Cert

6.1.6.283 nameConstraints URI1 CA Cert forward crossCertificatePair:

forward: nameConstraints URI1 CA Cert
reverse: absent

6.1.6.284 nameConstraints URI1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints URI1 CA Cert

6.1.6.285 nameConstraints URI2 CA Cert forward crossCertificatePair:

forward: nameConstraints URI2 CA Cert
reverse: absent

6.1.6.286 nameConstraints URI2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: nameConstraints URI2 CA Cert

6.1.6.287 distributionPoint1 CA Cert forward crossCertificatePair:

forward: distributionPoint1 CA Cert
reverse: absent

6.1.6.288 distributionPoint1 CA Cert reverse crossCertificatePair:

forward: absent
reverse: distributionPoint1 CA Cert

6.1.6.289 distributionPoint2 CA Cert forward crossCertificatePair:

forward: distributionPoint2 CA Cert
reverse: absent

6.1.6.290 distributionPoint2 CA Cert reverse crossCertificatePair:

forward: absent
reverse: distributionPoint2 CA Cert

6.1.6.291 No issuingDistributionPoint CA Cert forward crossCertificatePair:

forward: No issuingDistributionPoint CA Cert
reverse: absent

6.1.6.292 No issuingDistributionPoint CA Cert reverse crossCertificatePair:

forward: absent
reverse: No issuingDistributionPoint CA Cert

6.1.6.293 onlyContainsUserCerts CA Cert forward crossCertificatePair:

forward: onlyContainsUserCerts CA Cert
reverse: absent

6.1.6.294 onlyContainsUserCerts CA Cert reverse crossCertificatePair:

forward: absent
reverse: onlyContainsUserCerts CA Cert

6.1.6.295 Invalid onlyContainsUserCerts Test11 EE forward crossCertificatePair:

forward: Invalid onlyContainsUserCerts Test11 EE
reverse: absent

6.1.6.296 Invalid onlyContainsUserCerts Test11 EE reverse crossCertificatePair:

forward: absent
reverse: Invalid onlyContainsUserCerts Test11 EE

6.1.6.297 onlyContainsCACerts CA Cert forward crossCertificatePair:

forward: onlyContainsCACerts CA Cert
reverse: absent

6.1.6.298 onlyContainsCACerts CA Cert reverse crossCertificatePair:

forward: absent
reverse: onlyContainsCACerts CA Cert

6.1.6.299 Valid onlyContainsCACerts Test13 EE forward crossCertificatePair:

forward: Valid onlyContainsCACerts Test13 EE
reverse: absent

6.1.6.300 Valid onlyContainsCACerts Test13 EE reverse crossCertificatePair:

forward: absent
reverse: Valid onlyContainsCACerts Test13 EE

6.1.6.301 onlyContainsAttributeCerts CA Cert forward crossCertificatePair:

forward: onlyContainsAttributeCerts CA Cert
reverse: absent

6.1.6.302 onlyContainsAttributeCerts CA Cert reverse crossCertificatePair:

forward: absent
reverse: onlyContainsAttributeCerts CA Cert

6.1.6.303 onlySomeReasons CA1 Cert forward crossCertificatePair:

forward: onlySomeReasons CA1 Cert
reverse: absent

6.1.6.304 onlySomeReasons CA1 Cert reverse crossCertificatePair:

forward: absent
reverse: onlySomeReasons CA1 Cert

6.1.6.305 onlySomeReasons CA2 Cert forward crossCertificatePair:

forward: onlySomeReasons CA2 Cert
reverse: absent

6.1.6.306 onlySomeReasons CA2 Cert reverse crossCertificatePair:

forward: absent
reverse: onlySomeReasons CA2 Cert

6.1.6.307 onlySomeReasons CA3 Cert forward crossCertificatePair:

forward: onlySomeReasons CA3 Cert
reverse: absent

6.1.6.308 onlySomeReasons CA3 Cert reverse crossCertificatePair:

forward: absent
reverse: onlySomeReasons CA3 Cert

6.1.6.309 onlySomeReasons CA4 Cert forward crossCertificatePair:

forward: onlySomeReasons CA4 Cert
reverse: absent

6.1.6.310 onlySomeReasons CA4 Cert reverse crossCertificatePair:

forward: absent
reverse: onlySomeReasons CA4 Cert

6.1.6.311 indirectCRL CA1 Cert forward crossCertificatePair:

forward: indirectCRL CA1 Cert
reverse: absent

6.1.6.312 indirectCRL CA1 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA1 Cert

6.1.6.313 indirectCRL CA2 Cert forward crossCertificatePair:

forward: indirectCRL CA2 Cert
reverse: absent

6.1.6.314 indirectCRL CA2 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA2 Cert

6.1.6.315 indirectCRL CA3 Cert forward crossCertificatePair:

forward: indirectCRL CA3 Cert
reverse: absent

6.1.6.316 indirectCRL CA3 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA3 Cert

6.1.6.317 indirectCRL CA4 Cert forward crossCertificatePair:

forward: indirectCRL CA4 Cert
reverse: absent

6.1.6.318 indirectCRL CA4 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA4 Cert

6.1.6.319 indirectCRL CA5 Cert forward crossCertificatePair:

forward: indirectCRL CA5 Cert
reverse: absent

6.1.6.320 indirectCRL CA5 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA5 Cert

6.1.6.321 indirectCRL CA6 Cert forward crossCertificatePair:

forward: indirectCRL CA6 Cert
reverse: absent

6.1.6.322 indirectCRL CA6 Cert reverse crossCertificatePair:

forward: absent
reverse: indirectCRL CA6 Cert

6.1.6.323 deltaCRLIndicator No Base CA Cert forward crossCertificatePair:

forward: deltaCRLIndicator No Base CA Cert
reverse: absent

6.1.6.324 deltaCRLIndicator No Base CA Cert reverse crossCertificatePair:

forward: absent
reverse: deltaCRLIndicator No Base CA Cert

6.1.6.325 deltaCRL CA1 Cert forward crossCertificatePair:

forward: deltaCRL CA1 Cert
reverse: absent

6.1.6.326 deltaCRL CA1 Cert reverse crossCertificatePair:

forward: absent
reverse: deltaCRL CA1 Cert

6.1.6.327 deltaCRL CA2 Cert forward crossCertificatePair:

forward: deltaCRL CA2 Cert
reverse: absent

6.1.6.328 deltaCRL CA2 Cert reverse crossCertificatePair:

forward: absent
reverse: deltaCRL CA2 Cert

6.1.6.329 deltaCRL CA3 Cert forward crossCertificatePair:

forward: deltaCRL CA3 Cert
reverse: absent

6.1.6.330 deltaCRL CA3 Cert reverse crossCertificatePair:

forward: absent
reverse: deltaCRL CA3 Cert

6.1.6.331 RFC3280 Mandatory Attribute Types CA Cert forward crossCertificatePair:

forward: RFC3280 Mandatory Attribute Types CA Cert
reverse: absent

6.1.6.332 RFC3280 Mandatory Attribute Types CA Cert reverse crossCertificatePair:

forward: absent
reverse: RFC3280 Mandatory Attribute Types CA Cert

6.1.6.333 RFC3280 Optional Attribute Types CA Cert forward crossCertificatePair:

forward: RFC3280 Optional Attribute Types CA Cert
reverse: absent

6.1.6.334 RFC3280 Optional Attribute Types CA Cert reverse crossCertificatePair:

forward: absent
reverse: RFC3280 Optional Attribute Types CA Cert

6.1.6.335 UTF8String Encoded Names CA Cert forward crossCertificatePair:

forward: UTF8String Encoded Names CA Cert
reverse: absent

6.1.6.336 UTF8String Encoded Names CA Cert reverse crossCertificatePair:

forward: absent
reverse: UTF8String Encoded Names CA Cert

6.1.6.337 Rollover from PrintableString to UTF8String CA Cert forward crossCertificatePair:

forward: Rollover from PrintableString to UTF8String CA Cert
reverse: absent

6.1.6.338 Rollover from PrintableString to UTF8String CA Cert reverse crossCertificatePair:

forward: absent
reverse: Rollover from PrintableString to UTF8String CA Cert

6.1.6.339 UTF8String Case Insensitive Match CA Cert forward crossCertificatePair:

forward: UTF8String Case Insensitive Match CA Cert
reverse: absent

6.1.6.340 UTF8String Case Insensitive Match CA Cert reverse crossCertificatePair:

forward: absent
reverse: UTF8String Case Insensitive Match CA Cert

6.1.6.341 Separate Certificate and CRL Keys Certificate Signing CA Cert forward crossCertificatePair:

forward: Separate Certificate and CRL Keys Certificate Signing CA Cert
reverse: absent

6.1.6.342 Separate Certificate and CRL Keys Certificate Signing CA Cert reverse crossCertificatePair:

forward: absent
reverse: Separate Certificate and CRL Keys Certificate Signing CA Cert

6.1.6.343 Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert forward crossCerificatePair:

forward: Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert
reverse: absent

6.1.6.344 Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert reverse crossCerificatePair:

forward: absent
reverse: Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert

6.1.6.345 DSA CA Cert forward crossCertificatePair:

forward: DSA CA Cert
reverse: absent

6.1.6.346 DSA CA Cert reverse crossCertificatePair:

forward: absent
reverse: DSA CA Cert

6.1.6.347 DSA Parameters Inherited CA Cert forward crossCertificatePair:

forward: DSA Parameters Inherited CA Cert
reverse: absent

6.1.6.348 DSA Parameters Inherited CA Cert reverse crossCertificatePair:

forward: absent
reverse: DSA Parameters Inherited CA Cert

6.2 S/MIME Messages

6.2.1 Base Signed Message

A clear-signed message in which the hash function used for the messageDigest signedAttribute and to compute the digital signature is the same as the hash function used to sign the message signer's certificate.

6.2.2 Test Signed Messages

6.2.2.1 Signed Valid Signatures Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Signatures Test1"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid Certificate Path Test1 EE

6.2.2.2 Signed Invalid CA Signature Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid CA Signature Test2"
Certificates: Bad Signed CA Cert
CRLS: Trust Anchor Root CRL, Bad Signed CA CRL
signer: Invalid CA Signature Test2 EE

6.2.2.3 Signed Invalid EE Signature Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid EE Signature Test3"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid EE Signature Test3 EE

6.2.2.4 Signed Invalid CA notBefore Date Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid CA notBefore Date Test1"
Certificates: Bad notBefore Date CA Cert
CRLS: Trust Anchor Root CRL, Bad notBefore Date CA CRL
signer: Invalid CA notBefore Date Test1 EE

6.2.2.5 Signed Invalid EE notBefore Date Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid EE notBefore Date Test2"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid EE notBefore Date Test2 EE

6.2.2.6 Signed Valid pre2000 UTC notBefore Date Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid pre2000 UTC notBefore Date Test3"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL

signer: Valid pre2000 UTC notBefore Date Test3 EE

6.2.2.7 Signed Valid GeneralizedTime notBefore Date Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid GeneralizedTime notBefore Date Test4"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid GeneralizedTime notBefore Date Test4 EE

6.2.2.8 Signed Invalid CA notAfter Date Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid CA notAfter Date Test5"
Certificates: Bad notAfter Date CA Cert
CRLS: Trust Anchor Root CRL, Bad notAfter Date CA CRL
signer: Invalid CA notAfter Date Test5 EE

6.2.2.9 Signed Invalid EE notAfter Date Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid EE notAfter Date Test6"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid EE notAfter Date Test6 EE

6.2.2.10 Signed Invalid pre2000 UTC EE notAfter Date Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pre2000 UTC EE notAfter Date Test7"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid pre2000 UTC EE notAfter Date Test7 EE

6.2.2.11 Signed Valid GeneralizedTime notAfter Date Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid GeneralizedTime notAfter Date Test8"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid GeneralizedTime notAfter Date Test8 EE

6.2.2.12 Signed Invalid Name Chaining EE Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Name Chaining EE Test1"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL

signer: Invalid Name Chaining Test1 EE

6.2.2.13 Signed Invalid Name Chaining Order Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Name Chaining Order Test2"
Certificates: Name Ordering CA Cert
CRLS: Trust Anchor Root CRL, Name Order CA CRL
signer: Invalid Name Chaining Order Test2 EE

6.2.2.14 Signed Valid Name Chaining Whitespace Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Name Chaining Whitespace Test3"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid Name Chaining Whitespace Test3 EE

6.2.2.15 Signed Valid Name Chaining Whitespace Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Name Chaining Whitespace Test4"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid Name Chaining Whitespace Test4 EE

6.2.2.16 Signed Valid Name Chaining Capitalization Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Name Chaining Capitalization Test5"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid Name Chaining Capitalization Test5 EE

6.2.2.17 Signed Valid Name Chaining UIDs Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Name Chaining UIDs Test6"
Certificates: UID CA Cert
CRLS: Trust Anchor Root CRL, UID CA CRL
signer: Valid Name UIDs Test6 EE

6.2.2.18 Signed Missing CRL Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Missing CRL Test1"
Certificates: No CRL CA Cert
CRLS: Trust Anchor Root CRL

signer: Invalid Missing CRL Test1 EE

6.2.2.19 Signed Invalid Revoked CA Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Revoked CA Test2"
Certificates: Good CA Cert, Revoked subCA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Revoked subCA CRL
signer: Invalid Revoked CA Test2 EE

6.2.2.20 Signed Invalid Revoked EE Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Revoked EE Test3"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid Revoked EE Test3 EE

6.2.2.21 Signed Invalid Bad CRL Signature Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Bad CRL Signature Test4"
Certificates: Bad CRL Signature CA Cert,
CRLS: Trust Anchor Root CRL, Bad CRL Signature CA CRL
signer: Invalid Bad CRL Signature Test4 EE

6.2.2.22 Signed Invalid Bad CRL Issuer Name Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Bad CRL Issuer Name Test5"
Certificates: Bad CRL Issuer Name CA Cert
CRLS: Trust Anchor Root CRL, Bad CRL Issuer Name CA CRL
signer: Invalid Bad CRL Issuer Name Test5 EE

6.2.2.23 Signed Invalid Wrong CRL Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Wrong CRL Test6"
Certificates: Wrong CRL CA Cert
CRLS: Trust Anchor Root CRL, Wrong CRL CA CRL
signer: Invalid Wrong CRL Test6 EE

6.2.2.24 Signed Valid Two CRLs Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Two CRLs Test7"
Certificates: Two CRLs CA Cert
CRLS: Trust Anchor Root CRL, Two CRLs CA Good CRL, Two CRLs CA Bad CRL

signer: Valid Two CRLs Test7 EE

6.2.2.25 Signed Invalid Unknown CRL Entry Extension Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Unknown CRL Entry Extension Test8"
Certificates: Unknown CRL Entry Extension CA Cert
CRLS: Trust Anchor Root CRL, Unknown CRL Entry Extension CA CRL
signer: Invalid Unknown CRL Entry Extension Test8 EE

6.2.2.26 Signed Invalid Unknown CRL Extension Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Unknown CRL Extension Test9"
Certificates: Unknown CRL Extension CA Cert
CRLS: Trust Anchor Root CRL, Unknown CRL Extension CA CRL
signer: Invalid Unknown CRL Extension Test9 EE

6.2.2.27 Signed Invalid Unknown CRL Extension Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Unknown CRL Extension Test10"
Certificates: Unknown CRL Extension CA Cert
CRLS: Trust Anchor Root CRL, Unknown CRL Extension CA CRL
signer: Invalid Unknown CRL Extension Test10 EE

6.2.2.28 Signed Invalid Old CRL nextUpdate Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Old CRL nextUpdate Test11"
Certificates: Old CRL nextUpdate CA Cert
CRLS: Trust Anchor Root CRL, Old CRL nextUpdate CA CRL
signer: Invalid Old CRL nextUpdate Test11 EE

6.2.2.29 Signed Invalid pre2000 CRL nextUpdate Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pre2000 CRL nextUpdate Test12"
Certificates: pre2000 CRL nextUpdate CA Cert
CRLS: Trust Anchor Root CRL, pre2000 CRL nextUpdate CA CRL
signer: Invalid pre2000 CRL nextUpdate Test12 EE

6.2.2.30 Signed Valid GeneralizedTime CRL nextUpdate Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid GeneralizedTime CRL nextUpdate Test13"
Certificates: GeneralizedTime CRL nextUpdate CA Cert
CRLS: Trust Anchor Root CRL, GeneralizedTime CRL nextUpdate CA CRL

signer: Valid GeneralizedTime CRL nextUpdate Test13 EE

6.2.2.31 Signed Valid Negative Serial Number Test14:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Negative Serial Number Test14"
Certificates: Negative Serial Number CA Cert
CRLS: Trust Anchor Root CRL, Negative Serial Number CA CRL
signer: Valid Negative Serial Number Test14 EE

6.2.2.32 Signed Invalid Negative Serial Number Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Negative Serial Number Test15"
Certificates: Negative Serial Number CA Cert
CRLS: Trust Anchor Root CRL, Negative Serial Number CA CRL
signer: Invalid Negative Serial Number Test15 EE

6.2.2.33 Signed Valid Long Serial Number Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Long Serial Number Test16"
Certificates: Long Serial Number CA Cert
CRLS: Trust Anchor Root CRL, Long Serial Number CA CRL
signer: Valid Long Serial Number Test16 EE

6.2.2.34 Signed Valid Long Serial Number Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Long Serial Number Test17"
Certificates: Long Serial Number CA Cert
CRLS: Trust Anchor Root CRL, Long Serial Number CA CRL
signer: Valid Long Serial Number Test17 EE

6.2.2.35 Signed Invalid Long Serial Number Test 18:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Long Serial Number Test 18"
Certificates: Long Serial Number CA Cert
CRLS: Trust Anchor Root CRL, Long Serial Number CA CRL
signer: Invalid Long Serial Number Test18 EE

6.2.2.36 Signed Valid Basic Self-Issued Old With New Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Basic Self-Issued Old With New Test1"
Certificates: Basic Self-Issued New Key CA Cert, Basic Self-Issued New Key OldWithNew CA Cert

CRLS: Trust Anchor Root CRL, Basic Self-Issued New Key CA CRL
signer: Valid Basic Self-Issued Old With New Test1 EE

6.2.2.37 Signed Invalid Basic Self-Issued Old With New Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Basic Self-Issued Old With New Test2"
Certificates: Basic Self-Issued New Key CA Cert, Basic Self-Issued New Key OldWithNew CA Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued New Key CA CRL
signer: Invalid Basic Self-Issued Old With New Test2 EE

6.2.2.38 Signed Valid Basic Self-Issued New With Old Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Basic Self-Issued New With Old Test3"
Certificates: Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key NewWithOld CA Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued Old Key Self-Issued Cert CRL, Basic Self-Issued Old Key CA CRL
signer: Valid Basic Self-Issued New With Old Test3 EE

6.2.2.39 Signed Valid Basic Self-Issued New With Old Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Basic Self-Issued New With Old Test4"
Certificates: Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key NewWithOld CA Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued Old Key Self-Issued Cert CRL, Basic Self-Issued Old Key CA CRL
signer: Valid Basic Self-Issued New With Old Test4 EE

6.2.2.40 Signed Invalid Basic Self-Issued New With Old Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Basic Self-Issued New With Old Test5"
Certificates: Basic Self-Issued Old Key CA Cert, Basic Self-Issued Old Key NewWithOld CA Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued Old Key Self-Issued Cert CRL, Basic Self-Issued Old Key CA CRL
signer: Invalid Basic Self-Issued New With Old Test5 EE

6.2.2.41 Signed Valid Basic Self-Issued CRL Signing Key Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Basic Self-Issued CRL Signing Key Test6"
Certificates: Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert

CRLS: Trust Anchor Root CRL, Basic Self-Issued CRL Signing Key CRL Cert CRL, Basic Self-Issued CRL Signing Key CA CRL
signer: Valid Basic Self-Issued CRL Signing Key Test6 EE

6.2.2.42 Signed Invalid Basic Self-Issued CRL Signing Key Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Basic Self-Issued CRL Signing Key Test7"
Certificates: Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued CRL Signing Key CRL Cert CRL, Basic Self-Issued CRL Signing Key CA CRL
signer: Invalid Basic Self-Issued CRL Signing Key Test7 EE

6.2.2.43 Signed Invalid Basic Self-Issued CRL Signing Key Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Basic Self-Issued CRL Signing Key Test8"
Certificates: Basic Self-Issued CRL Signing Key CA Cert, Basic Self-Issued CRL Signing Key CRL Cert
CRLS: Trust Anchor Root CRL, Basic Self-Issued CRL Signing Key CRL Cert CRL, Basic Self-Issued CRL Signing Key CA CRL
signer: Invalid Basic Self-Issued CRL Signing Key Test8 EE

6.2.2.44 Signed Invalid Missing basicConstraints Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Missing basicConstraints Test1"
Certificates: Missing basicConstraints CA Cert
CRLS: Trust Anchor Root CRL, Missing basicConstraints CA CRL
signer: Invalid Missing basicConstraints Test1 EE

6.2.2.45 Signed Invalid cA False Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cA False Test2"
Certificates: basicConstraints Critical cA False CA Cert
CRLS: Trust Anchor Root CRL, basicConstraints Critical cA False CA CRL
signer: Invalid cA False Test2 EE

6.2.2.46 Signed Invalid cA False Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cA False Test3"
Certificates: basicConstraints Not Critical cA False CA Cert
CRLS: Trust Anchor Root CRL, basicConstraints Not Critical cA False CA CRL
signer: Invalid cA False Test3 EE

6.2.2.47 Signed Valid basicConstraints Not Critical Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid basicConstraints Not Critical Test4"
Certificates: basicConstraints Not Critical CA Cert
CRLS: Trust Anchor Root CRL, basicConstraints Not Critical CA CRL
signer: Valid basicConstraints Not Critical Test4 EE

6.2.2.48 Signed Invalid pathLenConstraint Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test5"
Certificates: pathLenConstraint0 CA Cert, pathLenConstraint0 subCA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL, pathLenConstraint0 subCA CRL
signer: Invalid pathLenConstraint Test5 EE

6.2.2.49 Signed Invalid pathLenConstraint Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test6"
Certificates: pathLenConstraint0 CA Cert, pathLenConstraint0 subCA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL, pathLenConstraint0 subCA CRL
signer: Invalid pathLenConstraint Test6 EE

6.2.2.50 Signed Valid pathLenConstraint Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid pathLenConstraint Test7"
Certificates: pathLenConstraint0 CA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL
signer: Valid pathLenConstraint Test7 EE

6.2.2.51 Signed Valid pathLenConstraint Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid pathLenConstraint Test8"
Certificates: pathLenConstraint0 CA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL
signer: Valid pathLenConstraint Test8 EE

6.2.2.52 Signed Invalid pathLenConstraint Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test9"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA0 Cert, pathLenConstraint6 subsubCA00 Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA0 CRL, pathLenConstraint6 subsubCA00 CRL

signer: Invalid pathLenConstraint Test9 EE

6.2.2.53 Signed Invalid pathLenConstraint Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test10"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA0 Cert, pathLenConstraint6 subsubCA00 Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA0 CRL, pathLenConstraint6 subsubCA00 CRL
signer: Invalid pathLenConstraint Test10 EE

6.2.2.54 Signed Invalid pathLenConstraint Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test11"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA1 Cert, pathLenConstraint6 subsubCA11 Cert, pathLenConstraint6 subsubsubCA11X Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA1 CRL, pathLenConstraint6 subsubCA11 CRL, pathLenConstraint6 subsubsubCA11X CRL
signer: Invalid pathLenConstraint Test11 EE

6.2.2.55 Signed Invalid pathLenConstraint Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid pathLenConstraint Test12"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA1 Cert, pathLenConstraint6 subsubCA11 Cert, pathLenConstraint6 subsubsubCA11X Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA1 CRL, pathLenConstraint6 subsubCA11 CRL, pathLenConstraint6 subsubsubCA11X CRL
signer: Invalid pathLenConstraint Test12 EE

6.2.2.56 Signed Valid pathLenConstraint Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid pathLenConstraint Test13"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA4 Cert, pathLenConstraint6 subsubCA41 Cert, pathLenConstraint6 subsubsubCA41X Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA4 CRL, pathLenConstraint6 subsubCA41 CRL, pathLenConstraint6 subsubsubCA41X CRL
signer: Valid pathLenConstraint Test13 EE

6.2.2.57 Signed Valid pathLenConstraint Test14:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid pathLenConstraint Test14"
Certificates: pathLenConstraint6 CA Cert, pathLenConstraint6 subCA4 Cert, pathLenConstraint6 subsubCA41 Cert, pathLenConstraint6 subsubsubCA41X Cert

CRLS: Trust Anchor Root CRL, pathLenConstraint6 CA CRL, pathLenConstraint6 subCA4 CRL, pathLenConstraint6 subsubCA41 CRL, pathLenConstraint6 subsubsubCA41X CRL
signer: Valid pathLenConstraint Test14 EE

6.2.2.58 Signed Valid Self-Issued pathLenConstraint Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued pathLenConstraint Test15"
Certificates: pathLenConstraint0 CA Cert, pathLenConstraint0 Self-Issued CA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL
signer: Valid Self-Issued pathLenConstraint Test15 EE

6.2.2.59 Signed Invalid Self-Issued pathLenConstraint Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued pathLenConstraint Test16"
Certificates: pathLenConstraint0 CA Cert, pathLenConstraint0 Self-Issued CA Cert, pathLenConstraint0 subCA2 Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint0 CA CRL, pathLenConstraint0 subCA2 CRL
signer: Invalid Self-Issued pathLenConstraint Test16 EE

6.2.2.60 Signed Valid Self-Issued pathLenConstraint Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued pathLenConstraint Test17"
Certificates: pathLenConstraint1 CA Cert, pathLenConstraint1 Self-Issued CA Cert, pathLenConstraint1 subCA Cert, pathLenConstraint1 Self-Issued subCA Cert
CRLS: Trust Anchor Root CRL, pathLenConstraint1 CA CRL, pathLenConstraint1 subCA CRL
signer: Valid Self-Issued pathLenConstraint Test17 EE

6.2.2.61 Signed Invalid keyUsage Critical keyCertSign False Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid keyUsage Critical keyCertSign False Test1"
Certificates: keyUsage Critical keyCertSign False CA Cert
CRLS: Trust Anchor Root CRL, keyUsage Critical keyCertSign False CA CRL
signer: Invalid keyUsage Critical keyCertSign False Test1 EE

6.2.2.62 Signed Invalid keyUsage Not Critical keyCertSign False Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid keyUsage Not Critical keyCertSign False Test2"
Certificates: keyUsage Not Critical keyCertSign False CA Cert
CRLS: Trust Anchor Root CRL, keyUsage Not Critical keyCertSign False CA CRL
signer: Invalid keyUsage Not Critical keyCertSign False Test2 EE

6.2.2.63 Signed Valid keyUsage Not Critical Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid keyUsage Not Critical Test3"
Certificates: keyUsage Not Critical CA Cert
CRLS: Trust Anchor Root CRL, keyUsage Not Critical CA CRL
signer: Valid keyUsage Not Critical Test3 EE

6.2.2.64 Signed Invalid keyUsage Critical cRLSign False Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid keyUsage Critical cRLSign False Test4"
Certificates: keyUsage Critical cRLSign False CA Cert
CRLS: Trust Anchor Root CRL, keyUsage Critical cRLSign False CA CRL
signer: Invalid keyUsage Critical cRLSign False Test4 EE

6.2.2.65 Signed Invalid keyUsage Not Critical cRLSign False Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid keyUsage Not Critical cRLSign False Test5"
Certificates: keyUsage Not Critical cRLSign False CA Cert
CRLS: Trust Anchor Root CRL, keyUsage Not Critical cRLSign False CA CRL
signer: Invalid keyUsage Not Critical cRLSign False Test5 EE

6.2.2.66 Signed All Certificates Same Policy Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "All Certificates Same Policy Test1"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Valid Certificate Path Test1 EE

6.2.2.67 Signed All Certificates No Policies Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "All Certificates No Policies Test2"
Certificates: No Policies CA Cert
CRLS: Trust Anchor Root CRL, No Policies CA CRL
signer: All Certificates No Policies Test2 EE

6.2.2.68 Signed Different Policies Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test3"
Certificates: Good CA Cert, Policies P2 subCA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Policies P2 subCA CRL
signer: Different Policies Test3 EE

6.2.2.69 Signed Different Policies Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test4"
Certificates: Good CA Cert, Good subCA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Good subCA CRL
signer: Different Policies Test4 EE

6.2.2.70 Signed Different Policies Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test5"
Certificates: Good CA Cert, Policies P2 subCA2 Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Policies P2 subCA2 CRL
signer: Different Policies Test5 EE

6.2.2.71 Signed Overlapping Policies Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Overlapping Policies Test6"
Certificates: Policies P1234 CA Cert, Policies P1234 subCAP123 Cert, Policies P1234 subsubCAP123P12 Cert
CRLS: Trust Anchor Root CRL, Policies P1234 CA CRL, Policies P1234 subCAP123 CRL, Policies P1234 subsubCAP123P12 CRL
signer: Overlapping Policies Test6 EE

6.2.2.72 Signed Different Policies Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test7"
Certificates: Policies P123 CA Cert, Policies P123 subCAP12 Cert, Policies P123 subsubCAP12P1 Cert
CRLS: Trust Anchor Root CRL, Policies P123 CA CRL, Policies P123 subCAP12 CRL, Policies P123 subsubCAP12P1 CRL
signer: Different Policies Test7 EE

6.2.2.73 Signed Different Policies Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test8"
Certificates: Policies P12 CA Cert, Policies P12 subCAP1 Cert, Policies P12 subsubCAP1P2 Cert
CRLS: Trust Anchor Root CRL, Policies P12 CA CRL, Policies P12 subCAP1 CRL, Policies P12 subsubCAP1P2 CRL
signer: Different Policies Test8 EE

6.2.2.74 Signed Different Policies Test9:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Different Policies Test9"
Certificates: Policies P123 CA Cert, Policies P123 subCAP12 Cert, Policies P123 subsubCAP12P2 Cert, Policies P123 subsubsubCAP12P2P1 Cert
CRLS: Trust Anchor Root CRL, Policies P123 CA CRL, Policies P123 subCAP12 CRL, Policies P123 subsubCAP2P2 CRL, Policies P123 subsubsubCAP12P2P1 CRL
signer: Different Policies Test9 EE

6.2.2.75 Signed All Certificates Same Policies Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "All Certificates Same Policies Test10"
Certificates: Policies P12 CA Cert
CRLS: Trust Anchor Root CRL, Policies P12 CA CRL
signer: All Certificates Same Policies Test10 EE

6.2.2.76 Signed All Certificates AnyPolicy Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "All Certificates AnyPolicy Test11"
Certificates: anyPolicy CA Cert
CRLS: Trust Anchor Root CRL, anyPolicy CA CRL
signer: All Certificates anyPolicy Test11 EE

6.2.2.77 Signed Different Policies Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Different Policies Test12"
Certificates: Policies P3 CA Cert
CRLS: Trust Anchor Root CRL, Policies P3 CA CRL
signer: Different Policies Test12 EE

6.2.2.78 Signed All Certificates Same Policies Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "All Certificates Same Policies Test13"
Certificates: Policies P123 CA Cert
CRLS: Trust Anchor Root CRL, Policies P123 CA CRL
signer: All Certificates Same Policies Test13 EE

6.2.2.79 Signed AnyPolicy Test14:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "AnyPolicy Test14"
Certificates: anyPolicy CA Cert
CRLS: Trust Anchor Root CRL, anyPolicy CA CRL
signer: AnyPolicy Test14 EE

6.2.2.80 Signed User Notice Qualifier Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "User Notice Qualifier Test15"
CRLS: Trust Anchor Root CRL
signer: User Notice Qualifier Test15 EE

6.2.2.81 Signed User Notice Qualifier Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "User Notice Qualifier Test16"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: User Notice Qualifier Test16 EE

6.2.2.82 Signed User Notice Qualifier Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "User Notice Qualifier Test17"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: User Notice Qualifier Test17 EE

6.2.2.83 Signed User Notice Qualifier Test18:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "User Notice Qualifier Test18"
Certificates: Policies P12 CA Cert
CRLS: Trust Anchor Root CRL, Policies P12 CA CRL
signer: User Notice Qualifier Test18 EE

6.2.2.84 Signed User Notice Qualifier Test19:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "User Notice Qualifier Test19"
CRLS: Trust Anchor Root CRL
signer: User Notice Qualifier Test19 EE

6.2.2.85 Signed CPS Pointer Qualifier Test20:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "CPS Pointer Qualifier Test20"
Certificates: Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: CPS Pointer Qualifier Test20 EE

6.2.2.86 Signed Valid RequireExplicitPolicy Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid RequireExplicitPolicy Test1"
Certificates: requireExplicitPolicy10 CA Cert, requireExplicitPolicy10 subCA Cert, requireExplicitPolicy10 subsubCA Cert, requireExplicitPolicy10 subsubsubCA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy10 CA CRL, requireExplicitPolicy10 subCA CRL, requireExplicitPolicy10 subsubCA CRL, requireExplicitPolicy10 subsubsubCA CRL
signer: Valid requireExplicitPolicy Test1 EE

6.2.2.87 Signed Valid RequireExplicitPolicy Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid RequireExplicitPolicy Test2"
Certificates: requireExplicitPolicy5 CA Cert, requireExplicitPolicy5 subCA Cert, requireExplicitPolicy5 subsubCA Cert, requireExplicitPolicy5 subsubsubCA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy5 CA CRL, requireExplicitPolicy5 subCA CRL, requireExplicitPolicy5 subsubCA CRL, requireExplicitPolicy5 subsubsubCA CRL
signer: Valid requireExplicitPolicy Test2 EE

6.2.2.88 Signed Invalid RequireExplicitPolicy Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid RequireExplicitPolicy Test3"
Certificates: requireExplicitPolicy4 CA Cert, requireExplicitPolicy4 subCA Cert, requireExplicitPolicy4 subsubCA Cert, requireExplicitPolicy4 subsubsubCA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy4 CA CRL, requireExplicitPolicy4 subCA CRL, requireExplicitPolicy4 subsubCA CRL, requireExplicitPolicy4 subsubsubCA CRL
signer: Invalid requireExplicitPolicy Test3 EE

6.2.2.89 Signed Valid RequireExplicitPolicy Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid RequireExplicitPolicy Test4"
Certificates: requireExplicitPolicy0 CA Cert, requireExplicitPolicy0 subCA Cert, requireExplicitPolicy0 subsubCA Cert, requireExplicitPolicy0 subsubsubCA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy0 CA CRL, requireExplicitPolicy0 subCA CRL, requireExplicitPolicy0 subsubCA CRL, requireExplicitPolicy0 subsubsubCA CRL
signer: Valid requireExplicitPolicy Test4 EE

6.2.2.90 Signed Invalid RequireExplicitPolicy Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid RequireExplicitPolicy Test5"
Certificates: requireExplicitPolicy7 CA Cert, requireExplicitPolicy7 subCARE2 Cert, requireExplicitPolicy7 subsubCARE2RE4 Cert, requireExplicitPolicy7 subsubsubCARE2RE4 Cert

CRLS: Trust Anchor Root CRL, requireExplicitPolicy7 CA CRL, requireExplicitPolicy7 subCARE2 CRL, requireExplicitPolicy7 subsubCARE2RE4 CRL, requireExplicitPolicy7 subsubsubCARE2RE4 CRL
signer: Invalid requireExplicitPolicy Test5 EE

6.2.2.91 Signed Valid Self-Issued requireExplicitPolicy Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued requireExplicitPolicy Test6"
Certificates: requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 Self-Issued CA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy2 CA CRL
signer: Valid Self-Issued requireExplicitPolicy Test6 EE

6.2.2.92 Signed Invalid Self-Issued requireExplicitPolicy Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued requireExplicitPolicy Test7"
Certificates: requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 Self-Issued CA Cert, requireExplicitPolicy2 subCA Cert,
CRLS: Trust Anchor Root CRL, requireExplicitPolicy2 CA CRL, requireExplicitPolicy2 subCA CRL
signer: Invalid Self-Issued requireExplicitPolicy Test7 EE

6.2.2.93 Signed Invalid Self-Issued requireExplicitPolicy Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued requireExplicitPolicy Test8"
Certificates: requireExplicitPolicy2 CA Cert, requireExplicitPolicy2 Self-Issued CA Cert, requireExplicitPolicy2 subCA Cert, requireExplicitPolicy2 Self-Issued subCA Cert
CRLS: Trust Anchor Root CRL, requireExplicitPolicy2 CA CRL, requireExplicitPolicy2 subCA CRL
signer: Invalid Self-Issued requireExplicitPolicy Test8 EE

6.2.2.94 Signed Valid Policy Mapping Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test1"
Certificates: Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, Mapping 1to2 CA CRL
signer: Valid Policy Mapping Test1 EE

6.2.2.95 Signed Invalid Policy Mapping Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Policy Mapping Test2"
Certificates: Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, Mapping 1to2 CA CRL
signer: Invalid Policy Mapping Test2 EE

6.2.2.96 Signed Valid Policy Mapping Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test3"
Certificates: P12 Mapping 1to3 CA Cert, P12 Mapping 1to3 subCA Cert, P12 Mapping 1to3 subsubCA Cert
CRLS: Trust Anchor Root CRL, P12 Mapping 1to3 CA CRL, P12 Mapping 1to3 subCA CRL, P12 Mapping 1to3 subsubCA CRL
signer: Valid Policy Mapping Test3 EE

6.2.2.97 Signed Invalid Policy Mapping Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Policy Mapping Test4"
Certificates: P12 Mapping 1to3 CA Cert, P12 Mapping 1to3 subCA Cert, P12 Mapping 1to3 subsubCA Cert
CRLS: Trust Anchor Root CRL, P12 Mapping 1to3 CA CRL, P12 Mapping 1to3 subCA CRL, P12 Mapping 1to3 subsubCA CRL
signer: Invalid Policy Mapping Test4 EE

6.2.2.98 Signed Valid Policy Mapping Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test5"
Certificates: P1 Mapping 1to234 CA Cert, P1 Mapping 1to234 subCA Cert
CRLS: Trust Anchor Root CRL, P1 Mapping 1to234 CA CRL, P1 Mapping 1to234 subCA CRL
signer: Valid Policy Mapping Test5 EE

6.2.2.99 Signed Valid Policy Mapping Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test6"
Certificates: P1 Mapping 1to234 CA Cert, P1 Mapping 1to234 subCA Cert
CRLS: Trust Anchor Root CRL, P1 Mapping 1to234 CA CRL, P1 Mapping 1to234 subCA CRL
signer: Valid Policy Mapping Test6 EE

6.2.2.100 Signed Invalid Mapping From anyPolicy Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Mapping From anyPolicy Test7"
Certificates: Mapping From anyPolicy CA Cert
CRLS: Trust Anchor Root CRL, Mapping From anyPolicy CA CRL
signer: Invalid Mapping From anyPolicy Test7 EE

6.2.2.101 Signed Invalid Mapping To anyPolicy Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Mapping To anyPolicy Test8"

Certificates: Mapping To anyPolicy CA Cert
CRLS: Trust Anchor Root CRL, Mapping To anyPolicy CA CRL
signer: Invalid Mapping To anyPolicy Test8 EE

6.2.2.102 Signed Valid Policy Mapping Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test9"
Certificates: PanyPolicy Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, PanyPolicy Mapping 1to2 CA CRL
signer: Valid Policy Mapping Test9 EE

6.2.2.103 Signed Invalid Policy Mapping Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Policy Mapping Test10"
Certificates: Good CA Cert, Good subCA PanyPolicy Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Good subCA PanyPolicy Mapping 1to2 CA CRL
signer: Invalid Policy Mapping Test10 EE

6.2.2.104 Signed Valid Policy Mapping Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test11"
Certificates: Good CA Cert, Good subCA PanyPolicy Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL, Good subCA PanyPolicy Mapping 1to2 CA CRL
signer: Valid Policy Mapping Test11 EE

6.2.2.105 Signed Valid Policy Mapping Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test12"
Certificates: P12 Mapping 1to3 CA Cert
CRLS: Trust Anchor Root CRL, P12 Mapping 1to3 CA CRL
signer: Valid Policy Mapping Test12 EE

6.2.2.106 Signed Valid Policy Mapping Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test13"
Certificates: P1anyPolicy Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, P1anyPolicy Mapping 1to2 CA CRL
signer: Valid Policy Mapping Test13 EE

6.2.2.107 Signed Valid Policy Mapping Test14:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Valid Policy Mapping Test14"
Certificates: P1anyPolicy Mapping 1to2 CA Cert
CRLS: Trust Anchor Root CRL, P1anyPolicy Mapping 1to2 CA CRL
signer: Valid Policy Mapping Test14 EE

6.2.2.108 Signed Invalid inhibitPolicyMapping Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitPolicyMapping Test1"
Certificates: inhibitPolicyMapping0 CA Cert, inhibitPolicyMapping0 subCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping0 CA CRL, inhibitPolicyMapping0 subCA CRL
signer: Invalid inhibitPolicyMapping Test1 EE

6.2.2.109 Signed Valid inhibitPolicyMapping Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid inhibitPolicyMapping Test2"
Certificates: inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 subCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P12 CA CRL, inhibitPolicyMapping1 P12 subCA CRL
signer: Valid inhibitPolicyMapping Test2 EE

6.2.2.110 Signed Invalid inhibitPolicyMapping Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitPolicyMapping Test3"
Certificates: inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 subCA Cert, inhibitPolicyMapping1 P12 subsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P12 CA CRL, inhibitPolicyMapping1 P12 subCA CRL, inhibitPolicyMapping1 P12 subsubCA CRL
signer: Invalid inhibitPolicyMapping Test3 EE

6.2.2.111 Signed Valid inhibitPolicyMapping Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid inhibitPolicyMapping Test4"
Certificates: inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 subCA Cert, inhibitPolicyMapping1 P12 subsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P12 CA CRL, inhibitPolicyMapping1 P12 subCA CRL, inhibitPolicyMapping1 P12 subsubCA CRL
signer: Valid inhibitPolicyMapping Test4 EE

6.2.2.112 Signed Invalid inhibitPolicyMapping Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitPolicyMapping Test5"

Certificates: inhibitPolicyMapping5 CA Cert, inhibitPolicyMapping5 subCA Cert, inhibitPolicyMapping5 subsubCA Cert, inhibitPolicyMapping5 subsubsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping5 CA CRL, inhibitPolicyMapping5 subCA CRL, inhibitPolicyMapping5 subsubCA CRL, inhibitPolicyMapping5 subsubsubCA CRL
signer: Invalid inhibitPolicyMapping Test5 EE

6.2.2.113 Signed Invalid inhibitPolicyMapping Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitPolicyMapping Test6"
Certificates: inhibitPolicyMapping1 P12 CA Cert, inhibitPolicyMapping1 P12 subCAIPM5 Cert, inhibitPolicyMapping1 P12 subsubCAIPM5 Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P12 CA CRL, inhibitPolicyMapping1 P12 subCAIPM5 CRL, inhibitPolicyMapping1 P12 subsubCAIPM5 CRL
signer: Invalid inhibitPolicyMapping Test6 EE

6.2.2.114 Signed Valid Self-Issued inhibitPolicyMapping Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued inhibitPolicyMapping Test7"
Certificates: inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 Self-Issued CA Cert, inhibitPolicyMapping1 P1 subCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P1 CA CRL, inhibitPolicyMapping1 P1 subCA CRL
signer: Valid Self-Issued inhibitPolicyMapping Test7 EE

6.2.2.115 Signed Invalid Self-Issued inhibitPolicyMapping Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitPolicyMapping Test8"
Certificates: inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 Self-Issued CA Cert, inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P1 CA CRL, inhibitPolicyMapping1 P1 subCA CRL, inhibitPolicyMapping1 P1 subsubCA CRL
signer: Invalid Self-Issued inhibitPolicyMapping Test8 EE

6.2.2.116 Signed Invalid Self-Issued inhibitPolicyMapping Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitPolicyMapping Test9"
Certificates: inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 Self-Issued CA Cert, inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 subsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P1 CA CRL, inhibitPolicyMapping1 P1 subCA CRL, inhibitPolicyMapping1 P1 subsubCA CRL
signer: Invalid Self-Issued inhibitPolicyMapping Test9 EE

6.2.2.117 Signed Invalid Self-Issued inhibitPolicyMapping Test10:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitPolicyMapping Test10"
Certificates: inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 Self-Issued CA Cert, inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 Self-Issued subCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P1 CA CRL, inhibitPolicyMapping1 P1 subCA CRL
signer: Invalid Self-Issued inhibitPolicyMapping Test10 EE

6.2.2.118 Signed Invalid Self-Issued inhibitPolicyMapping Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitPolicyMapping Test11"
Certificates: inhibitPolicyMapping1 P1 CA Cert, inhibitPolicyMapping1 P1 Self-Issued CA Cert, inhibitPolicyMapping1 P1 subCA Cert, inhibitPolicyMapping1 P1 Self-Issued subCA Cert
CRLS: Trust Anchor Root CRL, inhibitPolicyMapping1 P1 CA CRL, inhibitPolicyMapping1 P1 subCA CRL
signer: Invalid Self-Issued inhibitPolicyMapping Test11 EE

6.2.2.119 Signed Invalid inhibitAnyPolicy Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitAnyPolicy Test1"
Certificates: inhibitAnyPolicy0 CA Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy0 CA CRL
signer: Invalid inhibitAnyPolicy Test1 EE

6.2.2.120 Signed Valid inhibitAnyPolicy Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid inhibitAnyPolicy Test2"
Certificates: inhibitAnyPolicy0 CA Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy0 CA CRL
signer: Valid inhibitAnyPolicy Test2 EE

6.2.2.121 Signed inhibitAnyPolicy Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "inhibitAnyPolicy Test3"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 subCA1 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA1 CRL
signer: inhibitAnyPolicy Test3 EE

6.2.2.122 Signed Invalid inhibitAnyPolicy Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitAnyPolicy Test4"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 subCA1 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA1 CRL

signer: Invalid inhibitAnyPolicy Test4 EE

6.2.2.123 Signed Invalid inhibitAnyPolicy Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitAnyPolicy Test5"
Certificates: inhibitAnyPolicy5 CA Cert, inhibitAnyPolicy5 subCA Cert, inhibitAnyPolicy5 subsubCA Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy5 CA CRL, inhibitAnyPolicy5 subCA CRL, inhibitAnyPolicy5 subsubCA CRL
signer: Invalid inhibitAnyPolicy Test5 EE

6.2.2.124 Signed Invalid inhibitAnyPolicy Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid inhibitAnyPolicy Test6"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 subCAIAP5 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCAIAP5 CRL
signer: Invalid inhibitAnyPolicy Test6 EE

6.2.2.125 Signed Valid Self-Issued inhibitAnyPolicy Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued inhibitAnyPolicy Test7"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 Self-Issued CA Cert, inhibitAnyPolicy1 subCA2 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA2 CRL
signer: Valid Self-Issued inhibitAnyPolicy Test7 EE

6.2.2.126 Signed Invalid Self-Issued inhibitAnyPolicy Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitAnyPolicy Test8"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 Self-Issued CA Cert, inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 subsubCA2 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA2 CRL, inhibitAnyPolicy1 subsubCA2 CRL
signer: Invalid Self-Issued inhibitAnyPolicy Test8 EE

6.2.2.127 Signed Valid Self-Issued inhibitAnyPolicy Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued inhibitAnyPolicy Test9"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 Self-Issued CA Cert, inhibitAnyPolicy1 subCA2 Cert, inhibitAnyPolicy1 Self-Issued subCA2 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA2 CRL
signer: Valid Self-Issued inhibitAnyPolicy Test9 EE

6.2.2.128 Signed Invalid Self-Issued inhibitAnyPolicy Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued inhibitAnyPolicy Test10"
Certificates: inhibitAnyPolicy1 CA Cert, inhibitAnyPolicy1 Self-Issued CA Cert, inhibitAnyPolicy1 subCA2 Cert
CRLS: Trust Anchor Root CRL, inhibitAnyPolicy1 CA CRL, inhibitAnyPolicy1 subCA2 CRL
signer: Invalid Self-Issued inhibitAnyPolicy Test10 EE

6.2.2.129 Signed Valid DN nameConstraints Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test1"
Certificates: nameConstraints DN1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Valid DN nameConstraints Test1 EE

6.2.2.130 Signed Invalid DN nameConstraints Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test2"
Certificates: nameConstraints DN1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Invalid DN nameConstraints Test2 EE

6.2.2.131 Signed Invalid DN nameConstraints Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test3"
Certificates: nameConstraints DN1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Invalid DN nameConstraints Test3 EE

6.2.2.132 Signed Valid DN nameConstraints Test4:

Base: Base Signed Message
from: "DNnameConstraintsTest4EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test4"
Certificates: nameConstraints DN1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Valid DN nameConstraints Test4 EE

6.2.2.133 Signed Valid DN nameConstraints Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test5"
Certificates: nameConstraints DN2 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN2 CA CRL

signer: Valid DN nameConstraints Test5 EE

6.2.2.134 Signed Valid DN nameConstraints Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test6"
Certificates: nameConstraints DN3 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL
signer: Valid DN nameConstraints Test6 EE

6.2.2.135 Signed Invalid DN nameConstraints Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test7"
Certificates: nameConstraints DN3 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL
signer: Invalid DN nameConstraints Test7 EE

6.2.2.136 Signed Invalid DN nameConstraints Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test8"
Certificates: nameConstraints DN4 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN4 CA CRL
signer: Invalid DN nameConstraints Test8 EE

6.2.2.137 Signed Invalid DN nameConstraints Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test9"
Certificates: nameConstraints DN4 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN4 CA CRL
signer: Invalid DN nameConstraints Test9 EE

6.2.2.138 Signed Invalid DN nameConstraints Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test10"
Certificates: nameConstraints DN5 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN5 CA CRL
signer: Invalid DN nameConstraints Test10 EE

6.2.2.139 Signed Valid DN nameConstraints Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test11"
Certificates: nameConstraints DN5 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN5 CA CRL

signer: Valid DN nameConstraints Test11 EE

6.2.2.140 Signed Invalid DN nameConstraints Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test12"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA1 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA1 CRL
signer: Invalid DN nameConstraints Test12 EE

6.2.2.141 Signed Invalid DN nameConstraints Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test13"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA2 CRL
signer: Invalid DN nameConstraints Test13 EE

6.2.2.142 Signed Valid DN nameConstraints Test14:

Base: Base Signed Message
from: "ValidDNnameConstraintsTest14EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test14"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA2 CRL
signer: Valid DN nameConstraints Test14 EE

6.2.2.143 Signed Invalid DN nameConstraints Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test15"
Certificates: nameConstraints DN3 CA Cert, nameConstraints DN3 subCA1 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL, nameConstraints DN3 subCA1 CRL
signer: Invalid DN nameConstraints Test15 EE

6.2.2.144 Signed Invalid DN nameConstraints Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test16"
Certificates: nameConstraints DN3 CA Cert, nameConstraints DN3 subCA1 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL, nameConstraints DN3 subCA1 CRL
signer: Invalid DN nameConstraints Test16 EE

6.2.2.145 Signed Invalid DN nameConstraints Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DN nameConstraints Test17"
Certificates: nameConstraints DN3 CA Cert, nameConstraints DN3 subCA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL, nameConstraints DN3 subCA2 CRL
signer: Invalid DN nameConstraints Test17 EE

6.2.2.146 Signed Valid DN nameConstraints Test18:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DN nameConstraints Test18"
Certificates: nameConstraints DN3 CA Cert, nameConstraints DN3 subCA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN3 CA CRL, nameConstraints DN3 subCA2 CRL
signer: Valid DN nameConstraints Test18 EE

6.2.2.147 Signed Valid Self-Issued DN nameConstraints Test19:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Self-Issued DN nameConstraints Test19"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 Self-Issued CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Valid DN nameConstraints Test19 EE

6.2.2.148 Signed Invalid Self-Issued DN nameConstraints Test20:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Self-Issued DN nameConstraints Test20"
Certificates: nameConstraints DN1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL
signer: Invalid DN nameConstraints Test20 EE

6.2.2.149 Signed Valid RFC822 nameConstraints Test21:

Base: Base Signed Message
from: "Test21EE@mailserver.testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid RFC822 nameConstraints Test21"
Certificates: nameConstraints RFC822 CA1 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA1 CRL
signer: Valid RFC822 nameConstraints Test21 EE

6.2.2.150 Signed Invalid RFC822 nameConstraints Test22:

Base: Base Signed Message
from: "Test22EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Invalid RFC822 nameConstraints Test22"

Certificates: nameConstraints RFC822 CA1 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA1 CRL
signer: Invalid RFC822 nameConstraints Test22 EE

6.2.2.151 Signed Valid RFC822 nameConstraints Test23:

Base: Base Signed Message
from: "Test23EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid RFC822 nameConstraints Test23"
Certificates: nameConstraints RFC822 CA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA2 CRL
signer: Valid RFC822 nameConstraints Test23 EE

6.2.2.152 Signed Invalid RFC822 nameConstraints Test24:

Base: Base Signed Message
from: "Test24EE@mailserver.testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Invalid RFC822 nameConstraints Test24"
Certificates: nameConstraints RFC822 CA2 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA2 CRL
signer: Invalid RFC822 nameConstraints Test24 EE

6.2.2.153 Signed Valid RFC822 nameConstraints Test25:

Base: Base Signed Message
from: "Test25EE@mailserver.testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid RFC822 nameConstraints Test25"
Certificates: nameConstraints RFC822 CA3 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA3 CRL
signer: Valid RFC822 nameConstraints Test25 EE

6.2.2.154 Signed Invalid RFC822 nameConstraints Test26:

Base: Base Signed Message
from: "Test26EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Invalid RFC822 nameConstraints Test26"
Certificates: nameConstraints RFC822 CA3 Cert
CRLS: Trust Anchor Root CRL, nameConstraints RFC822 CA3 CRL
signer: Invalid RFC822 nameConstraints Test26 EE

6.2.2.155 Signed Valid DN and RFC822 nameConstraints Test27:

Base: Base Signed Message
from: "Test27EE@testcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Valid DN and RFC822 nameConstraints Test27"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA3 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA3 CRL

signer: Valid DN and RFC822 nameConstraints Test27 EE

6.2.2.156 Signed Invalid DN and RFC822 nameConstraints Test28:

Base: Base Signed Message
from: "Test28EE@invalidcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Invalid DN and RFC822 nameConstraints Test28"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA3 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA3 CRL
signer: Invalid DN and RFC822 nameConstraints Test28 EE

6.2.2.157 Signed Invalid DN and RFC822 nameConstraints Test29:

Base: Base Signed Message
from: "Test29EE@invalidcertificates.gov"
to: "recipient@testcertificates.gov"
subject: "Invalid DN and RFC822 nameConstraints Test29"
Certificates: nameConstraints DN1 CA Cert, nameConstraints DN1 subCA3 Cert
CRLS: Trust Anchor Root CRL, nameConstraints DN1 CA CRL, nameConstraints DN1 subCA3 CRL
signer: Invalid DN and RFC822 nameConstraints Test29 EE

6.2.2.158 Signed Valid DNS nameConstraints Test30:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DNS nameConstraints Test30"
Certificates: nameConstraints DNS1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DNS1 CA CRL
signer: Valid DNS nameConstraints Test30 EE

6.2.2.159 Signed Invalid DNS nameConstraints Test31:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DNS nameConstraints Test31"
Certificates: nameConstraints DNS1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DNS1 CA CRL
signer: Invalid DNS nameConstraints Test31 EE

6.2.2.160 Signed Valid DNS nameConstraints Test32:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DNS nameConstraints Test32"
Certificates: nameConstraints DNS2 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DNS2 CA CRL
signer: Valid DNS nameConstraints Test32 EE

6.2.2.161 Signed Invalid DNS nameConstraints Test33:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Invalid DNS nameConstraints Test33"
Certificates: nameConstraints DNS2 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DNS2 CA CRL
signer: Invalid DNS nameConstraints Test33 EE

6.2.2.162 Signed Valid URI nameConstraints Test34:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid URI nameConstraints Test34"
Certificates: nameConstraints URI1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints URI1 CA CRL
signer: Valid URI nameConstraints Test34 EE

6.2.2.163 Signed Invalid URI nameConstraints Test35:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid URI nameConstraints Test35"
Certificates: nameConstraints URI1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints URI1 CA CRL
signer: Invalid URI nameConstraints Test35 EE

6.2.2.164 Signed Valid URI nameConstraints Test36:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid URI nameConstraints Test36"
Certificates: nameConstraints URI2 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints URI2 CA CRL
signer: Valid URI nameConstraints Test36 EE

6.2.2.165 Signed Invalid URI nameConstraints Test37:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid URI nameConstraints Test37"
Certificates: nameConstraints URI2 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints URI2 CA CRL
signer: Invalid URI nameConstraints Test37 EE

6.2.2.166 Signed Valid distributionPoint Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid distributionPoint Test1"
Certificates: distributionPoint1 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint1 CA CRL
signer: Valid distributionPoint Test1 EE

6.2.2.167 Signed Invalid distributionPoint Test2:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Invalid distributionPoint Test2"
Certificates: distributionPoint1 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint1 CA CRL
signer: Invalid distributionPoint Test2 EE

6.2.2.168 Signed Invalid distributionPoint Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid distributionPoint Test3"
Certificates: distributionPoint1 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint1 CA CRL
signer: Invalid distributionPoint Test3 EE

6.2.2.169 Signed Valid distributionPoint Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid distributionPoint Test4"
Certificates: distributionPoint1 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint1 CA CRL
signer: Valid distributionPoint Test4 EE

6.2.2.170 Signed Valid distributionPoint Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid distributionPoint Test5"
Certificates: distributionPoint2 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint2 CA CRL
signer: Valid distributionPoint Test5 EE

6.2.2.171 Signed Invalid distributionPoint Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid distributionPoint Test6"
Certificates: distributionPoint2 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint2 CA CRL
signer: Invalid distributionPoint Test6 EE

6.2.2.172 Signed Valid distributionPoint Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid distributionPoint Test7"
Certificates: distributionPoint2 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint2 CA CRL
signer: Valid distributionPoint Test7 EE

6.2.2.173 Signed Invalid distributionPoint Test8:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Invalid distributionPoint Test8"
Certificates: distributionPoint2 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint2 CA CRL
signer: Invalid distributionPoint Test8 EE

6.2.2.174 Signed Invalid distributionPoint Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid distributionPoint Test9"
Certificates: distributionPoint2 CA Cert
CRLS: Trust Anchor Root CRL, distributionPoint2 CA CRL
signer: Invalid distributionPoint Test9 EE

6.2.2.175 Signed Valid No issuingDistributionPoint Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid No issuingDistributionPoint Test10"
Certificates: No issuingDistributionPoint CA Cert
CRLS: Trust Anchor Root CRL, No issuingDistributionPoint CA CRL
signer: Valid No issuingDistributionPoint Test10 EE

6.2.2.176 Signed Invalid onlyContainsUserCerts CRL Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlyContainsUserCerts CRL Test11"
Certificates: onlyContainsUserCerts CA Cert
CRLS: Trust Anchor Root CRL, onlyContainsUserCerts CA CRL
signer: Invalid onlyContainsUserCerts Test11 EE

6.2.2.177 Signed Invalid onlyContainsCACerts CRL Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlyContainsCACerts CRL Test12"
Certificates: onlyContainsCACerts CA Cert
CRLS: Trust Anchor Root CRL, onlyContainsCACerts CA CRL
signer: Invalid onlyContainsCACerts Test12 EE

6.2.2.178 Signed Valid onlyContainsCACerts CRL Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid onlyContainsCACerts CRL Test13"
Certificates: onlyContainsCACerts CA Cert
CRLS: Trust Anchor Root CRL, onlyContainsCACerts CA CRL
signer: Valid onlyContainsCACerts Test13 EE

6.2.2.179 Signed Invalid onlyContainsAttributeCerts Test14:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Invalid onlyContainsAttributeCerts Test14"
Certificates: onlyContainsAttributeCerts CA Cert
CRLS: Trust Anchor Root CRL, onlyContainsAttributeCerts CA CRL
signer: Invalid onlyContainsAttributeCerts Test14 EE

6.2.2.180 Signed Invalid onlySomeReasons Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlySomeReasons Test15"
Certificates: onlySomeReasons CA1 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA1 compromise CRL, onlySomeReasons CA1 other reasons CRL
signer: Invalid onlySomeReasons Test15 EE

6.2.2.181 Signed Invalid onlySomeReasons Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlySomeReasons Test16"
Certificates: onlySomeReasons CA1 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA1 compromise CRL, onlySomeReasons CA1 other reasons CRL
signer: Invalid onlySomeReasons Test16 EE

6.2.2.182 Signed Invalid onlySomeReasons Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlySomeReasons Test17"
Certificates: onlySomeReasons CA2 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA2 CRL1, onlySomeReasons CA2 CRL2
signer: Invalid onlySomeReasons Test17 EE

6.2.2.183 Signed Valid onlySomeReasons Test18:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid onlySomeReasons Test18"
Certificates: onlySomeReasons CA4 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
signer: Valid onlySomeReasons Test19 EE

6.2.2.184 Signed Valid onlySomeReasons Test19:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid onlySomeReasons Test19"
Certificates: onlySomeReasons CA4 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL

signer: Valid onlySomeReasons Test19 EE

6.2.2.185 Signed Invalid onlySomeReasons Test20:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlySomeReasons Test20"
Certificates: onlySomeReasons CA4 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
signer: Invalid onlySomeReasons Test20 EE

6.2.2.186 Signed Invalid onlySomeReasons Test21:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid onlySomeReasons Test21"
Certificates: onlySomeReasons CA4 Cert
CRLS: Trust Anchor Root CRL, onlySomeReasons CA4 compromise CRL, onlySomeReasons CA4 other reasons CRL
signer: Invalid onlySomeReasons Test21 EE

6.2.2.187 Signed Valid IDP with indirectCRL Test22:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid IDP with indirectCRL Test22"
Certificates: indirectCRL CA1 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA1 CRL
signer: Valid IDP with indirectCRL Test22 EE

6.2.2.188 Signed Invalid IDP with indirectCRL Test23:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid IDP with indirectCRL Test23"
Certificates: indirectCRL CA1 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA1 CRL
signer: Invalid IDP with indirectCRL Test23 EE

6.2.2.189 Signed Valid IDP with indirectCRL Test24:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid IDP with indirectCRL Test24"
Certificates: indirectCRL CA2 Cert, indirectCRL CA1 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA1 CRL
signer: Valid IDP with indirectCRL Test24 EE

6.2.2.190 Signed Valid IDP with indirectCRL Test25:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid IDP with indirectCRL Test25"

Certificates: indirectCRL CA2 Cert, indirectCRL CA1 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA1 CRL
signer: Valid IDP with indirectCRL Test25 EE

6.2.2.191 Signed Invalid IDP with indirectCRL Test26:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid IDP with indirectCRL Test26"
Certificates: indirectCRL CA2 Cert, indirectCRL CA1 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA1 CRL
signer: Invalid IDP with indirectCRL Test26 EE

6.2.2.192 Signed Invalid cRLIssuer Test27:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cRLIssuer Test27"
Certificates: indirectCRL CA2 Cert, Good CA Cert
CRLS: Trust Anchor Root CRL, Good CA CRL
signer: Invalid cRLIssuer Test27 EE

6.2.2.193 Signed Valid cRLIssuer Test28:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid cRLIssuer Test28"
Certificates: indirectCRL CA3 Cert, indirectCRL CA3 cRLIssuer Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA3 CRL, indirectCRL CA3 cRLIssuer CRL
signer: Valid cRLIssuer Test28 EE

6.2.2.194 Signed Valid cRLIssuer Test29:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid cRLIssuer Test29"
Certificates: indirectCRL CA3 Cert, indirectCRL CA3 cRLIssuer Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA3 CRL, indirectCRL CA3 cRLIssuer CRL
signer: Valid cRLIssuer Test29 EE

6.2.2.195 Signed Valid cRLIssuer Test30:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid cRLIssuer Test30"
Certificates: indirectCRL CA4 Cert, indirectCRL CA4 cRLIssuer Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA4 cRLIssuer CRL
signer: Valid cRLIssuer Test30 EE

6.2.2.196 Signed Invalid cRLIssuer Test31:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cRLIssuer Test31"

Certificates: indirectCRL CA5 Cert, indirectCRL CA6 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA5 CRL
signer: Invalid cRLIssuer Test31 EE

6.2.2.197 Signed Invalid cRLIssuer Test32:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cRLIssuer Test32"
Certificates: indirectCRL CA5 Cert, indirectCRL CA6 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA5 CRL
signer: Invalid cRLIssuer Test32 EE

6.2.2.198 Signed Valid cRLIssuer Test33:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid cRLIssuer Test33"
Certificates: indirectCRL CA5 Cert, indirectCRL CA6 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA5 CRL
signer: Valid cRLIssuer Test33 EE

6.2.2.199 Signed Invalid cRLIssuer Test34:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cRLIssuer Test34"
Certificates: indirectCRL CA5 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA5 CRL
signer: Invalid cRLIssuer Test34 EE

6.2.2.200 Signed Invalid cRLIssuer Test35:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid cRLIssuer Test35"
Certificates: indirectCRL CA5 Cert
CRLS: Trust Anchor Root CRL, indirectCRL CA5 CRL
signer: Invalid cRLIssuer Test35 EE

6.2.2.201 Signed Invalid deltaCRLIndicator No Base Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid deltaCRLIndicator No Base Test1"
Certificates: deltaCRLIndicator No Base CA Cert
CRLS: Trust Anchor Root CRL, deltaCRLIndicator No Base CA CRL
signer: Invalid deltaCRLIndicator No Base Test1 EE

6.2.2.202 Signed Valid delta-CRL Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid delta-CRL Test2"

Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Valid deltaCRL Test2 EE

6.2.2.203 Signed Invalid delta-CRL Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid delta-CRL Test3"
Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Invalid deltaCRL Test3 EE

6.2.2.204 Signed Invalid delta-CRL Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid delta-CRL Test4"
Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Invalid deltaCRL Test4 EE

6.2.2.205 Signed Valid delta-CRL Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid delta-CRL Test5"
Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Valid deltaCRL Test5 EE

6.2.2.206 Signed Invalid delta-CRL Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid delta-CRL Test6"
Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Invalid deltaCRL Test6 EE

6.2.2.207 Signed Valid delta-CRL Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid delta-CRL Test7"
Certificates: deltaCRL CA1 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA1 CRL, deltaCRL CA1 deltaCRL
signer: Valid deltaCRL Test7 EE

6.2.2.208 Signed Valid delta-CRL Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid delta-CRL Test8"

Certificates: deltaCRL CA2 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA2 CRL, deltaCRL CA2 deltaCRL
signer: Valid deltaCRL Test8 EE

6.2.2.209 Signed Invalid delta-CRL Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid delta-CRL Test9"
Certificates: deltaCRL CA2 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA2 CRL, deltaCRL CA2 deltaCRL
signer: Invalid deltaCRL Test9 EE

6.2.2.210 Signed Invalid delta-CRL Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid delta-CRL Test10"
Certificates: deltaCRL CA3 Cert
CRLS: Trust Anchor Root CRL, deltaCRL CA3 CRL, deltaCRL CA3 deltaCRL
signer: Invalid deltaCRL Test10 EE

6.2.2.211 Signed Valid Unknown Not Critical Certificate Extension Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Unknown Not Critical Certificate Extension Test1"
CRLS: Trust Anchor Root CRL
signer: Valid Unknown Not Critical Certificate Extension Test1 EE

6.2.2.212 Signed Invalid Unknown Critical Certificate Extension Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Unknown Critical Certificate Extension Test2"
CRLS: Trust Anchor Root CRL
signer: Invalid Unknown Critical Certificate Extension Test2 EE

6.2.2.213 Signed Valid RFC3280 Mandatory Attribute Types Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid RFC3280 Mandatory Attribute Types Test7"
Certificates: RFC3280 Mandatory Attribute Types CA Cert
CRLS: Trust Anchor Root CRL, RFC3280 Mandatory Attribute Types CA CRL
signer: Valid RFC3280 Mandatory Attribute Types Test7 EE

6.2.2.214 Signed Valid RFC3280 Optional Attribute Types Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid RFC3280 Optional Attribute Types Test8"
Certificates: RFC3280 Optional Attribute Types CA Cert
CRLS: Trust Anchor Root CRL, RFC3280 Optional Attribute Types CA CRL

signer: Valid RFC3280 Optional Attribute Types Test8 EE

6.2.2.215 Signed Valid UTF8String Encoded Names Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid UTF8String Encoded Names Test9"
Certificates: UTF8String Encoded Names CA Cert
CRLS: Trust Anchor Root CRL, UTF8String Encoded Names CA CRL
signer: Valid UTF8String Encoded Names Test9 EE

6.2.2.216 Signed Valid Rollover from PrintableString to UTF8String Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Rollover from PrintableString to UTF8String Test10"
Certificates: Rollover from PrintableString to UTF8String CA Cert
CRLS: Trust Anchor Root CRL, Rollover from PrintableString to UTF8String CA CRL
signer: Valid Rollover from PrintableString to UTF8String Test10 EE

6.2.2.217 Signed Valid UTF8String Case Insensitive Match Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid UTF8String Case Insensitive Match Test11"
Certificates: UTF8String Case Insensitive Match CA Cert
CRLS: Trust Anchor Root CRL, UTF8String Case Insensitive Match CA CRL
signer: Valid UTF8String Case Insensitive Match Test11 EE

6.2.2.218 Signed Invalid DNS nameConstraints Test38:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DNS nameConstraints Test38"
Certificates: nameConstraints DNS1 CA Cert
CRLS: Trust Anchor Root CRL, nameConstraints DNS1 CA CRL
signer: Invalid DNS nameConstraints Test38 EE

6.2.2.219 Signed Valid Separate Certificate and CRL Keys Test19:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid Separate Certificate and CRL Keys Test19"
Certificates: Separate Certificate and CRL Keys Certificate Signing CA Cert, Separate Certificate and CRL Keys CRL Signing Cert
CRLS: Trust Anchor Root CRL, Separate Certificate and CRL Keys CRL
signer: Valid Separate Certificate and CRL Keys Test19 EE

6.2.2.220 Signed Invalid Separate Certificate and CRL Keys Test20:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Separate Certificate and CRL Keys Test20"
Certificates: Separate Certificate and CRL Keys Certificate Signing CA Cert, Separate Certificate

and CRL Keys CRL Signing Cert
CRLS: Trust Anchor Root CRL, Separate Certificate and CRL Keys CRL
signer: Invalid Separate Certificate and CRL Keys Test20 EE

6.2.2.221 Signed Invalid Separate Certificate and CRL Keys Test21:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid Separate Certificate and CRL Keys Test21"
Certificates: Separate Certificate and CRL Keys CA2 Certificate Signing CA Cert, Separate Certificate and CRL Keys CA2 CRL Signing Cert
CRLS: Trust Anchor Root CRL, Separate Certificate and CRL Keys CA2 CRL
signer: Invalid Separate Certificate and CRL Keys Test21 EE

6.2.2.222 Signed Valid DSA Signatures Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DSA Signatures Test4"
Certificates: DSA CA Cert
CRLS: Trust Anchor Root CRL, DSA CA CRL
signer: Valid DSA Signatures Test4 EE

6.2.2.223 Signed Valid DSA Parameter Inheritance Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Valid DSA Parameter Inheritance Test5"
Certificates: DSA CA Cert, DSA Parameters Inherited CA Cert
CRLS: Trust Anchor Root CRL, DSA CA CRL, DSA Parameters Inherited CA CRL
signer: Valid DSA Parameter Inheritance Test5 EE

6.2.2.224 Signed Invalid DSA Signature Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Invalid DSA Signature Test6"
Certificates: DSA CA Cert
CRLS: Trust Anchor Root CRL, DSA CA CRL
signer: Invalid DSA Signature Test6 EE