

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 **inhibitPolicyMapping** 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 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 **directoryNames** and **rfc822Names** 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 **DistributionPoints**, 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 **DistributionPoints**, 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 **DistributionPoints**, 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 **certificatelissuer** 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 **certificatelissuer** 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 **certificatelissuer** 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.

<i>1.07</i>	<i>PKITS</i>
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

<i>1.07</i>	<i>PKITS</i>
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

<i>1.07</i>	<i>PKITS</i>
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

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