Network Device Interpretation # 201706

CA certificates - basicConstraints validation

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Jun-2017*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPP V1.0, FWcPP V1.0, NDSD V1.0, NDcPP V2.0, NDSDv2.0*

Affected Section(s): *FIA_X509_EXT.1.2*

Superseded Interpretation(s): *None*

Issue:

Inquiry has been answered, however, the below was brought to NIAP's attention with the following recommendations.

Recommendation by NIAP:

Upon review of FIA_X509_EXT.1.2 SFR and its Application Note 19, the intent of this test is for the TOE to validate a certificate path by verifying both the basicContraints extension is present and the CA flag set to TRUE on all CA certificates. It should verify these fields regardless of TOE or peer certificate - it's for any CA cert to be valid. For TOE, this includes loading a "CA" certificate - it shouldn't be recognized as a CA/root without these flags.

For peer, it shouldn't accept the peer's cert as valid because it doesn't chain properly. Currently, the NDcPP v1.0 requires TOE only, but NIAP recommends it should be TOE and peer.

Resolution:

The NIT believes that the cPP already states that the requirements of FIA_X509_EXT.1.2 apply to both TOE and peer. In particular when Application Note 19 (in cPPv1.0) states "This requirement applies to certificates that are used and processed by the TSF", this covers the peer certificate chain. Therefore no change is made to the Application Note.

However, the NIT acknowledges that the tests for FIA_X509_EXT.1.2 should be clarified and therefore makes the following modifications defined below.

Changes to SD v1.0

The Test requirements for FIA_X509_EXT.1.2 shall be modified as follows, starting at paragraph 291 in SD v1.0:

~~The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two intermediate CAs, and the self-signed Root CA.~~

The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).

For each of the following tests the evaluator shall create a chain of at least four certificates: a self-signed root CA certificate, two intermediate CA certificates, and a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).

~~a) Test 1: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.~~

a) Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~b) Test 2: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE. The validation of the certificate path fails.~~

b) Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~c) Test 3: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.~~

Changes to SD v2.0

The Test requirements for FIA_X509_EXT.1.2/ITT shall be modified as follows, starting at paragraph 231 in SD v2.0:

~~The evaluator shall create a chain of at least two certificates: the node certificate to be tested, and the self-signed Root CA.~~

The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).

For each of the following tests the evaluator shall create a chain of at least two certificates: a self-signed root CA certificate and a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).

~~a) Test 1: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.~~

a) Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~b) Test 2: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE. The validation of the certificate path fails.~~

b) Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~c) Test 3: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.~~

The Test requirements for FIA_X509_EXT.1.2/Rev shall be modified as follows, starting at paragraph 533 in SD v2.0:

~~The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an intermediate CA, and the self-signed Root CA.~~

The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).

For each of the following tests the evaluator shall create a chain of at least three certificates: a self-signed root CA certificate, an intermediate CA certificate and a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).

~~a) Test 1: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.~~

a) Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~b) Test 2: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE. The validation of the certificate path fails.~~

b) Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).

~~c) Test 3: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.~~

Rationale:

Wording changes to tests 1 & 2 clarify the intent of the test and to allow that the test can be applied either at the point of reliance or when installing a trusted certificate on the TOE to be used as a part of future certificate chains. (Because the basicConstraints CA flag is a structural property of the certificate and does not 'expire' it does not need to be checked at every point of reliance.)

Test 3 is removed as redundant: positive testing is already adequately covered by FIA_X509_EXT.1.1 Tests (in particular, FIA_X509_EXT.1.1 test 1 confirms that the evaluator can properly construct valid certificate chains).

Note that the chain length for testing is different in SD v1.0 and SD v2.0, reflecting the differences in the original text, in order to maximise the consistency in what the evaluation demonstrates in TOEs certified before and after this interpretation.

Further Action:

None

Action by Network iTC:

None