Network Device Interpretation # 201663

Use of intermediate CA certificates and certificate hierarchy depth

Status: ☒ *Active* □ *Inactive*

Date: *11-Apr-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, ND SD v1.0*

Affected Section(s): *FIA_X509_EXT.1.1, FIA_X509_EXT.1.2 and related Tests in SD*

Superseded Interpretation(s): *None*

Issue:

NDcPP FIA_X509_EXT.1 Testing

The NDcPP Supporting Document identifies one test in FIA_X509_EXT.1.1 and three tests in FIA_X509_EXT.1.2 that requires the use of intermediate CA Certificates.

FIA_X509_EXT.1.1 Test 3 requires revocation and testing of a TOE intermediate certificate.

Test 3: The evaluator shall test that the TOE can properly handle revoked certificates- conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the TOE certificate and revocation of the TOE intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.

FIA_X509_EXT.1.2 Test 1, Test 2, Test 3 requires a chain of at least four certificates: the node certificate to be tested, two intermediate CAs, and the self-signed Root CA.

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.

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.

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 TOE is its own root CA and does not support intermediate certificates. However, the TOE satisfies the SFR since the TOE certificate validation ends in a trusted root CA certificate in a root store managed by the TOE and the TOE restricts the use of certificates to a trusted CA certificate.

The use of intermediate certificates is not mandated by the NDcPP or by RFC 5280. NIAP approved TD0072 which was later implemented into the Protection Profile for Application Software v1.2. The PPAppSW modified all of the Assurance Activity testing for FIA_X509_EXT.1.1 by stating "If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created." The PPAppSW modified all of the Assurance Activity testing for FIA_X509_EXT.1.2 by stating "if the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the selfsigned Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created."

The TOE supports a depth of two. Testing with a certificate depth of two has been completed with satisfactory results for the tests identified above.

The NDcPP Supporting Document states in paragraph 6 the following:

"If any Evaluation Activity cannot be successfully completed in an evaluation then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation."

The TOE does meet "Exact Conformance" requirement as defined in the NDcPP. The "Exact Conformance" definition applies to the ST. The ST contains all of the mandatory SFRs, optional SFRs and selection based SFRS. No additional SFRs are added to the ST. No mandatory SFRs were omitted.

The above paragraph in the Supporting Document permits the modification or the removal of specific tests based upon the evaluation of each individual TOE. The CCTL is asking for the approval for the modification of the tests identified above to be tested at a certificate depth level of 2.

Rationale

- The TOE meets the exact conformance definition in the NDcPP.
- The use of an external CA is not mandated by the NDcPP.
- The use of intermediate CA certificates is not mandated by the NDcPP.
- The use of an external CA is not mandated by RFC 5280.
- The use of intermediate CA certificates is not mandated by RFC 5280.
- NIAP approved TD0072 which addressed the exact FIA_X509_EXT.1.1 and FIA_X509_EXT.1.2 test requirements. PPAppSW v1.2 was modified to include TOEs with a maximum trust depth of two, with no Intermediate CA created.
- Testing the TOE with a trust depth of two fulfills the requirement intent of each of the above NDcPP tests.

Resolution:

Network Devices and Firewalls compliant to the NDcPP or FWcPP are expected to be capable of performing X.509 certificate validation based on root certificates, intermediate CA certificates and device certificates. The tests defined in the SD for FIA_X509_EXT.1.1 and FIA_X509_EXT.1.2 are testing this expected behavior and shall therefore be applied as written.

According to Annex K of the revised CCRA the set of cPP and related SDs together define the minimum set of security requirements on the TOE. The NIT acknowledges, though, that all security requirements on the TOE should be reflected by the SFR as far as possible and it should be avoided to introduce new security requirements on the TOE through evaluation activities in the SD. The NIT therefore recommends that future versions of the NDcPP and FWcPP express the expected TOE behavior more clearly in the X.509 related SFRs.

Rationale:

See Resolution section.

Further Action:

None

Action by Network iTC:

In future versions of NDcPP and FWcPP express expected TOE behavior more clearly in the X.509 related SFRs.