Network Device Interpretation # 29

Clarifying FIA_X509_EXT.1 test 1

Status: ☒ *Active* ☐ *Inactive*

Date: *19-Sep-2016*

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

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

Affected Document(s): *ND SD V1.0*

Affected Section(s): *2.3.5.2*

Superseded Interpretation(s): *None*

Issue:

In FIA_X509_EXT.1, the Evaluation Activity (EA) for Test 1 appears to call for three distinct tests:

1) The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing

2) The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate to be used in the function, and demonstrate that the function succeeds.

3) The evaluator shall then delete one of the certificates, and show that the function fails.

The Evaluators only presented two test cases (2 and 3) and gave the following argument for why only two are necessary:

We think you misreading a very confusingly written test. The first sentence of Test 1 is not an explicit test step, but in fact a topic sentence. The second sentence has the words "shall then", when we believe it shouldn't.

The test really is composed of two different tests. A valid control test (2nd sentence), and a broken path test (3rd sentence). There are many different ways to create an invalid chain, but in this test, it's basically just a broken path (missing CA in the chain). Test it with all CA certs in the chain, and remove one and test again.

The other aspects of an invalid chain are treated in the subsequent tests (expired cert in the chain, revoked, CRL issued by CA lacking cRLSign, three corrupted cert tests, CA missing basicConstraints, CA flag is false, valid test.

The Validators would like to know if three distinct tests are necessary or of the wording of the EA needs to be clarified.

Resolution:

The NIAP TRRT responded to this request for interpretation as follows:

"In looking at the tests, the TRRT thinks that you and the lab are correct regarding intent. There is a topic/overview sentence, Test 1 tests that everything works properly and then for a broken path. The other tests check for expiration, revocation, and other invalid certs or cert chains."

NIT supports the response provided by NIAP, and will update the test description as described below.

Rationale:

As suggested by the Issue author, the first sentence was originally intended as an overview sentence describing a two-step test. The wording should be modified to make clear the individual steps required, and to remove the suggestion of a third step.

Further Action:

Replacement of description for FIA_X509_EXT.1, Test 1:

a) Test 1a: The evaluator shall load a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the certificate to be used in the function, and shall use this chain to demonstrate that the function succeeds.

Test 1b: The evaluator shall then delete one of the certificates in the chain (i.e. the root CA certificate or other intermediate certificate, but not the end-entity certificate), and show that the function fails.

Action by Network iTC:

Update the description for FIA_X509_EXT.1, Test 1 in the ND SD according to the definition above.