Network Device Interpretation # 202422

Clarification for FIA_X509_EXT.1 and FIA_X509_EXT.2

Status: ☒ *Active* □ *Inactive*

Date: *3-Mar-2025*

End of proposed Transition Period (to be updated after TR2TD process): *31-Mar-2025*

Type of Change: □ Immediate application ☒ Minor change □ Major change

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

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

Affected Document(s): *cPP_ND_v3.0e, cPP_ND_v3.0e-SD*

Affected Section(s): *TBD*

Superseded Interpretation(s): *None*

Issue:

Requesting clarification for claiming "FIA_X509_EXT.1 X.509 Certificate Validation" and "FIA_X509_EXT.2 X.509 Certificate Authentication" in case of a TOE acting as a HTTPS Server or TLS/DTLS server without mutual authentication (i.e. FCS_TLSS_EXT.1 or FCS_DTLSS_EXT.1).

Question:

When a TOE is acting as a HTTPS Server or TLS/DTLS Server without Mutual Authentication (MA) (for example web server, or web UI for administration, etc), then the TOE will be presenting its server certificate to an IT entity (TLS client). However, the TOE will not be requesting or expecting any certificate from the client. The only scenario where a TOE acting as a server without MA would be presented with a certificate is if the TOE supports Certificate Requests to an external CA and allows import/load of the signed certificate.

There seems to be few issues with NDcPP requirements in this scenario as follows:

In NDcPP v2.2e SD para 573, the testing requirement states "The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE".

This implies that all of FIA_X509_EXT.1 tests should be performed during connection time, when the TOE is validating a certificate presented to it (i.e. TOE is acting as a TLS/DTLS client or TLS/DTLS server with MA).

For a HTTPS Server or TLS/DTLS server non-MA, the only time a certificate will be presented to the TOE is if the TOE supports Certificate Request mechanisms (manually or via a formal certificate management protocol) to an external CA. In this case the Certificate Request could be validated (CSR generation and import of the external CA signed TOE certificate) when the certificate is loaded on the TOE. This scenario seems to be not allowed because the NDcPP v2.2e SD para 573, states “It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE”.

A possible conclusion is that FIA_X509_EXT.1 requirements should not be applicable for a TOE acting as a HTTPS Server or TLS/DTLS server without mutual authentication. This would be in alignment with the PP_APP_v1.4. The PP_APP_v1.4 has a note under FTP_DIT_EXT.1 that states “FIA_X509_EXT.1 and FIA_X509_EXT.2 are not applicable when the TOE acts as a HTTPS/TLS server with no mutual authentication”.

The above bold statement in 1 is not present in the NDcPP v3.0e SD para 525. Assuming that this was intentional, it implies that a TOE is allowed to perform the FIA_X509_EXT.1 tests/checks when it is loaded onto the TOE and not always during authentication step. In this case the NDcPP v3.0e SD para 525 needs to be re-worded and for NDcPP v2.2e SD para 573 the conflicting statement needs to be removed.

Application Note 115 of the NDcPP v3.0e states “If the TOE only presents its own certificate (e.g., a web server without mutual authentication), implementing the trust store is optional”.

This implies that there can be a TOE acting as a HTTPS Server or TLS/DTLS server without mutual authentication that does not have a trust store. In that case, there would never be a scenario when a certificate is ever presented to that TOE, neither during load nor connection time.

This implies that FIA_X509_EXT.1 requirements should not be applicable in this case.

Application Note 115 of the NDcPP v3.0e further states “It is expected that revocation checking is performed when a certificate is used in an authentication step. It is expected that revocation checking is performed on both leaf and intermediate CA certificates when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. Revocation checking of any CA certificate designated a trust anchor is not required.

If the TOE implements mutual authentication or acts as a server, there is no expectation of performing any checks on TOE’s own leaf certificate during authentication”.

This implies that revocation checking is not applicable for a TOE acting as a HTTPS Server or TLS/DTLS server without mutual authentication. Because here, the TOE is not expected to be presented with a certificate during authentication step.

FIA_X509_EXT.1.1/Rev Test 3, FIA_X509_EXT.1.1/Rev Test 4, and FIA_X509_EXT.2 Test 1 should be Not Applicable, because they all are related to revocation checking. The test description for these test states “The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate”. Again, the expectation seems to be for the TOE to validate a peer IT Entity’s certificate during authentication step and not TOE’s own certificate.

In conclusion, FIA_X509_EXT.2 requirements and revocation checking requirements from FIA_X509_EXT.1 should not be applicable for a TOE acting as a HTTPS Server or TLS/DTLS server without mutual authentication.

Therefore, it seems that a TOE acting as a server without MA should not be required to claim FIA_X509_EXT.1 or FIA_X509_EXT.2 because the testing for these SFRs seems to be focused on a TOE that is validating the certificates presented during connection time (i.e. when a TOE is acting as a client or a server with MA).

Alternatively, FIA_X509_EXT.1 can be made applicable by making some changes.

Potential Resolution:

Option 1:

A TD should be issued for NDcPP clarifying that "FIA_X509_EXT.1 and FIA_X509_EXT.2 are not applicable when the TOE acts as a HTTPS/TLS server with no mutual authentication".

FIA_X509_EXT.3 is required to be claimed but it is no longer dependent on FIA_X509_EXT.1 and FIA_X509_EXT.2.

Option 2:

A TD should be issued for NDcPP clarifying that "FIA_X509_EXT.2 is not applicable when the TOE acts as a HTTPS/TLS server with no mutual authentication".

FIA_X509_EXT.1 and FIA_X509_EXT.3 are required to be claimed but it is no longer dependent on FIA_X509_EXT.2.

FIA_X509_EXT.1 needs following modifications:

- Update NDcPP v3.0e SD para 525 t state "The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step, when a certificate is loaded onto the TOE, or when performing trusted updates (if FPT_TUD_EXT.2 is selected)."
- Update NDcPP v2.2e SD para 573 based on above bullet point and remove the sentence "It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE".
- Clarify for testing to be performed during certificate load/import when TOE is acting as a server. There are two scenarios here depending on is there an expectation for a TOE to perform revocation checking of its own certificate during the time of load/import:
    - Update FIA_X509_EXT.1.1/Rev Test 3 and FIA_X509_EXT.1.1/Rev Test 4 to allow revocation checking during certificate load/import when TOE is acting as a server. OR
    - Update FIA_X509_EXT.1.1/Rev Test 3 and FIA_X509_EXT.1.1/Rev Test 4 to make them conditional. i.e. applicable only when a TOE is expected to be presented with a certificate during authentication/connection.
- For the SFR definition of FIA_X509_EXT.1.1/Rev, the following bullet point may or may-not need change depending on the direction taken in bullet point above:
    - The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List

(CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].

Resolution:

The NIT acknowledges the issue. The intent was that a TOE should only be required to revocation check certificates presented to it for validation. A TOE was not intended to revocation check X.509 certificates a TOE uses to identify itself to other entities.

The following change shall be applied:

cPP_ND_v3.0e Section B.4.1

{old}

Support for X.509 certificate-based authentication is required if IPsec, TLS or DTLS communications are claimed for FPT_ITT.1, FTP_ITC.1 or FTP_TRP.1/Admin. Claiming functionality in FIA_X509_EXT.1/Rev is mandatory when using certificate-based authentication as part of establishing secure channel with a remote endpoint where the TOE performs certificate validation. These SFRs are also required if FPT_TUD_EXT.2 is claimed.

Although the functionality in FIA_X509_EXT.1/Rev and FIA_X509_EXT.2 is always required when using X.509 certificate-based authentication, the TOE only needs to be able to generate a Certification Request if the TOE needs to present an X.509 certificate to another endpoint via the TSF for authentication (e.g. if at least one of the following SFRs is included in the ST: FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_IPSEC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2). Therefore FIA_X509_EXT.3 only needs to be added to the ST in this case. If the TOE does not need to present an X.509 certificate to another endpoint via the TSF for authentication (e.g. a client not supporting mutual authentication) the use of FIA_X509_EXT.3 is optional.

{/old}

{new}

Support for X.509 certificate-based authentication (FIA_X509_EXT.2) is required if IPsec, FCS_TLSC_EXT.1, FCS_TLSS_EXT.2, FCS_DTLSC_EXT.1, FCS_DTLSS_EXT.2, x509v3- in FCS_SSH_EXT.1.2 as an SSH server, or x509v3-* in FCS_SSHC_EXT.1.1 are claimed. Support for X.509 certificate-based authentication is also required if FPT_TUD_EXT.1.3 selects “X.509 certificate.” If the certificate-based authentication is used for Intra-TSF communication (i.e., FTP_ITT.1) either FIA_X509_EXT.1/Rev or FIA_X509_EXT.1/ITT is required. For all other X.509 certificate-based authentication, FIA_X509_EXT.1/Rev is required.*

Support for generating Certification Requests (FIA_X509_EXT.3) is required if the TOE (or distributed TOE component) authenticates itself to an external IT entity, administrators, or distributed TOE components using X.509 certificates (i.e., at least one of the following SFRs is included in the ST: FCS_IPSEC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_SSH_EXT.1.2 with x509v3- as an SSH client, or FCS_SSHS_EXT.1.1 with x509v3-*).*

{/new}

cPP_ND_v3.0e Section B.4.1.1 Application Note 115 last paragraph

{old}

The ST author must include FIA_X509_EXT.1/Rev in all instances except when only SSH is selected within FTP_ITC.1, FTP_TRP.1 or FPT_ITT.1, and implementation is limited to public-key authentication that does not rely on X.509 certificates. Additionally, FIA_X509_EXT.1/Rev must also be included if FPT_TUD_EXT is included in the ST.

{/old}

{new}

Please see section B.4.1 for a description of when FIA_X509_EXT.1/Rev must be included.

{/new}

cPP_ND_v3.0e Section B.4.1.3

{delete}

Although the functionality in FIA_X509_EXT.1/Rev and FIA_X509_EXT.2 is always required when using X.509 certificate-based authentication, the TOE only needs to be able to generate a Certification Request if the TOE needs to present an X.509 certificate to another endpoint via the TSF for authentication (i.e. if at least one of the following SFRs is included in the ST: FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_IPSEC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2). Therefore FIA_X509_EXT.3 only needs to be added to the ST in this case. If the TOE does not need to present an X.509 certificate to another endpoint via the TSF for authentication (e.g. a client not supporting mutual authentication) the use of FIA_X509_EXT.3 is optional. This element must be included in the ST if X.509 certificates are used as part of FTP_ITC.1, FTP_TRP.1/Admin, or FPT_ITT.1 where the TOE authenticating itself to external IT entities, administrators, or distributed components.

{/delete}

cPP_ND_v3.0e Section C.3.3.3

{old}

Dependencies:

- *FCS_CKM.1 Cryptographic Key Generation*

- *FIA_X509_EXT.1 X.509 Certificate Validation*

{/old}

{new}

Dependencies:

- *FCS_CKM.1 Cryptographic Key Generation*

{/new}

cPP_ND_v3.0e-SD Section 4.3.1.3 paragraph 525

{old}

The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is expected that either OCSP or CRL revocation checking is performed when a certificate is presented to the TOE (e.g. during authentication). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:

{/old}

{new}

The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is expected that either OCSP or CRL revocation checking is performed when a certificate is presented to the TOE (e.g. during authentication). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates to authenticate remote endpoints or entities. These tests do not apply to certificates the TOE presents to remote endpoints to identify itself. For example, if the TOE implements certificate-based authentication with IPsec and as a TLS client, then it shall be tested with each of these protocols:

{/new}

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

None