Network Device Interpretation # 201726rev2

Applicability of FIA_X509_EXT.3

Status: ☒ *Active* ☐ *Inactive*

Date: *15-May-2018*

End of proposed Transition Period (to be updated after TR2TD process): *24-Jun-2018*

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): *NDcPP V1.0, NDcPP V2.0, FWcPP V1.0, FWcPP V2.0*

Affected Section(s): *FIA_X509_EXT.1.1*

Superseded Interpretation(s): *None*

Issue:

TD0182 and TD0184 as well as the subsequent revisions in NDcPP 2.0 make it clear that the FIA_X509_EXT SFRs should be optional based on whether the TSF uses X.509 certificates. TD0168 says that FIA_X509_EXT.3 remains applicable in all cases, except for the case where the only trusted communications use ssh-rsa and updates do not rely on certificates.

All of the FIA_X509_EXT SFRs (.1/Rev, .2, and .3) are always discussed as a group in the NDcPP (i.e. section B.3.1 does not differentiate between them in terms of when they are applicable), which suggests that if one of them applies, then all of them do.

However, in the case of a TOE that uses FCS_SSHS_EXT.1 for remote administration with ssh-rsa as its only authentication method, and that uses FCS_TLSC_EXT.1 for its only remote trusted channel, the only certificates the TSF is responsible for handling are server certificates presented to it; it would never need to present its own certificate so support for the generation of a Certificate Request message is not necessary.

Is it acceptable to define a TOE that claims FIA_X509_EXT.1/Rev and FIA_X509_EXT.2 for the purpose of establishing a TLS trusted channel but omitting the optional FIA_X509_EXT.3 SFR because there is no security function for which the TOE will ever present its own certificate to a remote entity? And if FIA_X509_EXT.3 is required in this case, what is the specific TSF usage that it is intended to capture?

Resolution:

The NIT acknowledges the issue described in the 'Issue' section. The following changes shall be applied.

The following text shall be added to the existing text in chap. B.3.1 (Authentication using X.509 certificates (Extended – FIA_X509_EXT)) and chap. B.3.1.3 (FIA_X509_EXT.1 X.509 Certificate Validation) of the cPP:

"Although the functionality in FIA_X509_EXT.1 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_SSHC_EXT.1.5 (applicable only if at least one of the x509v3- ciphers is selected), FCS_SSHS_EXT.1.5 (applicable only if at least one of the x509v3-* ciphers is selected), 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".*

FIA_X509_EXT.3.1 shall be modified as follows:

"The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country]."

The dependencies for the FIA_X509_EXT.x requirements as specified in chap C.3.4 shall be modified as follows:

FIA_X509_EXT.1

Dependencies: FIA_X509_EXT.2 X.509 Certificate Authentication

~~FIA_X509_EXT.3 X.509 Certificate Requests~~

FIA_X509_EXT.2

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

~~FIA_X509_EXT.3 X.509 Certificate Requests~~

FIA_X509_EXT.3

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FIA_X509_EXT.1 X.509 Certificate Validation

~~FIA_X509_EXT.2 X.509 Certificate Requests~~

The dependency rationale in Table 7 shall be updated as follows for FIA_X509_EXT.1/ITT:

SFR	Dependencies	Rationale Statement

FIA_X509_EXT.1/ITT	FIA_X509_EXT.2	

The dependency rationale in Table 8 shall be updated as follows for FIA_X509_EXT.1/Rev, FIA_X509_EXT.2 and FIA_X509_EXT.3:

SFR	Dependencies	Rationale Statement
FIA_X509_EXT.1/Rev	FIA_X509_EXT.2	
FIA_X509_EXT.2	FIA_X509_EXT.1	
FIA_X509_EXT.3	FCS_CKM.1 FIA_X509_EXT.1	

In the Supporting Document the following changes shall be performed to the FIA_X509_EXT.3 section:

The Guidance Documentation section shall be replaced by the following text:

"The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certification Requests. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request."

Test 1 of the Test section shall be replaced by the following text:

"Test 1: The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated request and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information."

Test 2 of the Test section shall be replaced by the following text:

"Test 2: The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the response message, and demonstrate that the function succeeds."

Rationale:

If a TOE does not need to present an X.509 certificate to another endpoint via the TSF, there is no need for the TOE to request an X.509 certificate in the first place.

Further Action:

None.

Action by Network iTC:

None.