Network Device Interpretation # 56

Timing of verification of revocation status for X.509 certificates

Status: ☒ *Active* ☐ *Inactive*

Date: *11-Oct-2016*

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

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

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

Affected Section(s): *FIA_X509_EXT.1.1*

Superseded Interpretation(s): *Supersedes RfI#9 due to the need to clarify follow-up questions*

Issue:

Under what conditions does revocation checking in FIA_X509_EXT.1.1 apply? It sounds like it applies whenever a certificate is being used; however, it is not feasible for the TOE to validate a certificate if it is using the certificate as part of a POST. Also, most servers will verify a certificate when it is loaded into the server, but do not check it's revocation status prior to presenting the certificate to a client. We believe that revocation checking should be performed when a certificate is presented for authentication purposes or loaded onto the TOE for it to use. Revocation checking should not have to be performed during power-up self-tests, loading a certificate for use, or when performing trusted update.

Please also clarify if FIA_X509_EXT.1.1 mandates revocation checking for TOE's own certificates during protocol negotiation.

Resolution:

NIT fully supports the response provided by NIAP on that request.

"Agree, the revocation should not have to be performed during power-up self-tests. Disagree, if when loading a certificate for use and if certificates are being used to verify trusted updates."

When establishing a trusted channel, the TOE is not expected to verify the validity of its own X.509 certificate. The related FTP requirements refer to ‘peer certificate’ only. So the TOE only needs to verify the peer certificate in this case.

Rationale:

None

Further Action:

Application Note for FIA_X509_EXT.1.1 (NDcPP):

The TSS shall describe when revocation checking is performed. It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not sufficient to verify the status of a X.509 certificate only when it's loaded onto the device.

It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).

Addition to SD, chap. Section 2.3.5.1 - TSS FIA_X509_EXT.1:

“The evaluator shall ensure the TSS describes when the check of validity of the certificates takes place. It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not sufficient to verify the status of a X.509 certificate only when it's loaded onto the device.

It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).”

Addition to SD, chap. Section 2.3.5.2 – Tests FIA_X509_EXT.1 – general, before the description of tests:

“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's loaded onto the device.

It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).”

Addition to SD, chap. Section 2.5.4.1 – Tests FPT_TST_EXT.2:

“It is not necessary to verify the revocation status of X.509 certificates during power-up.”

Addition to SD, chap. Section 2.5.6.1 – TSS FPT_TUD_EXT.2:

„The TSS shall describe when revocation checking is performed. It is expected that revocation checking is performed when a certificate is used when performing trusted updates. It is not sufficient to verify the status of a X.509 certificate only when it's loaded onto the device.”

Addition to SD, chap. Section 2.5.6.3 – Tests FPT_TUD_EXT.2:

“The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used when performing trusted updates. It is not sufficient to verify the status of a X.509 certificate only when it's loaded onto the device.”

Action by Network iTC:

Click here to enter text.