Network Device Interpretation # 201820rev2

Manual installation of CRL (FIA_X509_EXT.2)

Status: ☒ *Active* ☐ *Inactive*

Date: *26-Nov-2018*

End of proposed Transition Period (to be updated after TR2TD process): *26-Nov-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): *ND SD v2.0e*

Affected Section(s): *FIA_X509_EXT.2*

Superseded Interpretation(s): *None*

Issue:

BACKGROUND:

The requirement [remark: 'Tests' requirements for FIA_X509_EXT.2] states that the TOE must " … communic[ate] with a non-TOE IT entity" when performing revocation list checking. This implies that the TOE must have the ability to contact a CRL distribution point, but could be read to support allowing the TOE administrator to manually load one or more CRLs into the TOE.

ISSUE:

Must the TOE be capable of initiating a connection to a CRL server (by way of the method as specified in the CDP extension of the certificate being validated) to retrieve the CRL? Or is it permissible for the TOE to require the administrator to upload the applicable CRL(s) to the TOE, which will be used for revocation checking?

CCTL PROPOSAL:

Since some TOEs will be deployed in environments that do not allow internet or CA-direct communications, the lab believes that manual CRL distribution should be allowed:

Update assurance activity wording to clarify that the TOE may either retrieve a CRL from a distribution point, or the administrator may manually install or load a CRL into the TOE.

Resolution:

The NIT believes that the current wording is appropriate and that the reference to an IT entity correctly expresses the intention to exclude reliance solely on manual update of CRLs. No change to the text is therefore proposed. The cPP does not prohibit the support for locally stored CRLs that are manually loaded into the TOE. But for a TOE to be compliant with this cPP the TOE needs to support certificate validity checking from a dynamically updated source like downloading a CRL from a CRL server or performing a lookup using OCSP.

Note: This does not require that the TOE is connected to the internet or has CA-direct communications (e.g. the dynamically updated source may be hosted on a private network).

Rationale:

The NIT believes that the current wording is appropriate and that the reference to an IT entity correctly expresses the intention to exclude reliance solely on manual update of CRLs. No change to the text is therefore proposed.

An automatic process for loading CRLs must be provided by the TOE. It may be asynchronous and populate a CRL cache.

Optionally, a manual method for uploading CRLs may be provided to supplement the automatic updating of the CRLs.

Note: This does not require that the TOE is connected to the internet or has CA-direct communications (e.g. the source(s) for the automatic update may be hosted on a private network).

As per RFI201630, use of X.509 certificates is optional for FPT_TUD_EXT.1. Use of X.509 certificates is also optional for use in FPT_TST_EXT.1.

Further Action:

None

Action by Network iTC:

None