Network Device Interpretation # 201608rev2

Compliance to RFC5759 and RFC5280 for using CRLs

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Mar-2017*

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

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

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FIA_X509_EXT.1.1*

Superseded Interpretation(s): *RfI08rev1, Feb 15th 2016.*

Issue:

NDcPP V1.0: FIA_X509_EXT.1.1 requires that any PP compliance using CRLs requires compliance to RFC 5759 (bullet #4). This RFC is specifically written around Suite B cryptography. Compliance to which requires the use of ECDSA. RFC 5280 defines the use of CRLs, their signatures, etc. This seems more "in line" with the rest of the PP. Requiring the use of Suite B cryptography any time that a vendor uses a CRL seems excessive.

The request is that the requirement be modified to allow compliance to RFC 5280 for CRLs.

Resolution:

The NIT acknowledges the issue addressed above. Therefore the paragraph:

"The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759]."

in FIA_X509_EXT.1.1 shall be modified as follows:

"The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5]."

Rationale:

N/A

Further Action:

None.

Action by Network iTC: