Network Device Interpretation # 201724

Handling of the basicConstraints extension in CA and leaf certificates

Status: ☒ *Active* ☐ *Inactive*

Date: *8-Mar-2018*

End of proposed Transition Period (to be updated after TR2TD process): *11-Apr-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Superseded Interpretation(s): *None*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:

It has been brought to our attention that there is a potential misinterpretation of the following bullet within FIA_X509_EXT.1.1 in both NDcPP v1.0 and NDcPP v2.0

"The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates."

*NIAP understands that the entirety of this bullet applies only to **CA** certificates.*

However, some vendors and labs are interpreting the requirement differently and breaking the requirement into two parts as follows:

The TSF shall ensure the presence of the basicConstraints extension. (for any/all certificates in the path)

The TSF shall ensure the CA flag is set to TRUE for all CA certificates.

As a result, they are operating under the assumption that "ensuring the presence of the basicConstraints extension" also applies to end entity certificates.

The following requirements are affected in each PP:

NDcPP v2.0 - FIA_X509_EXT.1.1, FIA_X509_EXT.1/ITT and FIA_X509_EXT.1.1/Rev

NDcPP v1.0 – FIA_X509_EXT.1.1

Would the iTC or NIT be able to verify our interpretation?

If you agree, we propose two options to resolve this.

- *Remove the bullet in FIA_X509_EXT.1.1 since it could be covered by FIA_X509_EXT.1.2, or*
- *Clarify the bullet in FIA_X509_EXT.1.1. Suggest: "The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE."*

Resolution:

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

FIA_X509_EXT.1.1 (NDcPP V1.0, FWcPP V1.0) FIA_X509_EXT.1.1/Rev, item 3 (NDcPP V2.0, FWcPP V2.0) and FIA_X509_EXT.1.1/ITT, item 3 (NDcPP V2.0, FWcPP V2.0) shall be modified as follows:

"The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE."

Rationale:

According to RFC 5280 the presence of the basicConstraints extension is mandated only for CA certificates. Therefore the focus of the FIA_X509_EXT.1.1 SFRs has been restricted to CA certificates. This has been ambiguous in the original SFRs.

Further Action:

None.

Action by Network iTC:

The Network iTC should consider specifying requirements and evaluation activities for handling of the basicConstraints extension in leaf certificates/end entity certificates since this could help to enhance security for some use cases.