Network Device Interpretation # 201650

Reference identifiers for TLS certificate checking

Status: ☒ *Active* □ *Inactive*

Date: *23-Jan-2017*

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): *FCS_TLSC_EXT.1, FCS_TLSC_EXT.2*

Superseded Interpretation(s): *None*

Issue:

Reviewing the 3 instances above reveals the contradiction that occurs for FCS_TLSC_EXT.2.2 under [CPP_ND_v1.0].

• The first contradiction is in regards to the use of the Subject Alternative Name as a reference identifier. While Application Note 79 does not state it is required and the TSS activity states that it is a selection, the test activities for Subject Alternative Name or not conditional, therefore required.

• The second contradiction is in regards to the use of Common Name as a reference identifier. While the TSS states that it is a selection, Application Note 79 states that it is required and the test activities are not conditional therefore required.

• The third and final contradiction is in regards to accepting wildcards from the peer identifier. While the TSS Activity states that the use of wildcards is a selection and Application Note 79 says it should be avoided, the same Application Note 79 says it is required and the test activities are not conditional, therefore required.

CCTL Proposal

The CCTL proposes that a more distinct clarification of what the TOE is required to implement in order to satisfy FCS_TLSC_EXT.2.2 be given. Specifically, it should be made clear if both Subject Alternative Name and the Common Name are required as types of reference identifiers and if IP Addresses and Wildcards are required to be processed as acceptable peer identifiers.

<u>NIAP response</u>

NIAP requires exact compliance to the cPP so the product must be capable of doing what is required by the SFR and the lab must run all required tests. Per the SFR referenced, which does not include a *selection, the SAN, CN, and handling of wildcards are all required (as stated in the SFR and tested in the EAs). The Application Note is intended to provide clarification of what is in RFC 6125 and how that RFC will be applied to the TOE. The TRRT has determined that this Application Note does not contradict the SFR.*

Resolution:

The NIT endorses the NIAP response and gives the following additional response. Taking the three suggested contradictions in turn:

(1) Support for the SAN in reference identifiers and presented certificates is required for FCS_TLSC_EXT.1.2 & FCS_TLSC_EXT.2.2. Neither the SFR nor the TSS part of the Evaluation Activity present it as a selection, and optional support is only suggested by the TSS Evaluation Activity text in the context of support for <u>application-specific</u> SAN values.

(2) Support for the CN in reference identifiers and presented certificates is required for FCS_TLSC_EXT.1.2 & FCS_TLSC_EXT.2.2, as clarified in Application Notes 75 & 79. Neither the SFR nor the TSS part of the Evaluation Activity present it as a selection, and while the TSS Evaluation Activity includes it in a list of example types of reference identifiers this is not intended to suggest that it is optional. A wording clarification will be made as in 'Further Action' below.

(3) Application Notes 75 & 79 (for FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2) state "[T]he client should avoid constructing reference identifiers using wildcards. However, if the presented identifiers include wildcards, the client must follow the best practices regarding matching; these best practices are captured in the assurance activity." The "assurance activity" in this case is found in the Evaluation Activity in SD v1.0 sections 2.2.13 & 2.2.14.

In the TSS requirements in SD v1.0 sections 2.2.13.1 & 2.2.14.1 the text "The evaluator shall ensure that the TSS describes … whether … wildcards are supported" is interpreted as referring to the statement in Application Notes 75 & 79 that "[T]he client should avoid constructing reference identifiers using wildcards". The tests in sections 2.2.13.3 & 2.2.14.3 examine the way the client responds when presented with server certificates that contain wildcards, which refers to the other part of the statement in Application Notes 75 & 79 that "if the presented identifiers include wildcards, the client must follow the best practices regarding matching; these best practices are captured in the assurance activity". The difference is thus between use of wildcards in a reference identifier list that the TOE constructs (which is discouraged, but optional), and support for the use of wildcards in a certificate that is presented to the TOE (which is required).

Regarding IP addresses as identifiers in certificates: Application Notes 75 & 79 already state that "support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented".

Rationale:

(1) Support for SAN is consistent with the recommendations in RFC 6125.

(2) *Support for CN as a default comparison is consistent with the recommendations in RFC 6125 and the existence of substantial numbers of legacy certificates based on use of CN.*
(3) *Since the TOE cannot prevent the possibility that it will receive certificates containing wildcards, it must be able to process them, and it is reasonable to test in the Evaluation Activity that this functionality follows the RFC.*

Further Action:

Remove implication that Common Name checking is optional in the TSS Evaluation Activities for FCS_TLSC_EXT.1.2 & FCS_TLSC_EXT.2.2 by limiting the example fields in brackets to application-specific cases so that the text reads:

> *"The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported (e.g application-specific Subject Alternative Names)…"*

Action by Network iTC:

None