Network Device Interpretation # 202110rev2

Clarification required for testing IPv6

Status: ☒ *Active* ☐ *Inactive*

Date: *31-Aug-2021*

End of proposed Transition Period (to be updated after TR2TD process): *30-Sep-2021*

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 v2.2*

Affected Section(s): *FCS_DTLSC_EXT.1.2, FCS_TLSC_EXT.1.2*

Superseded Interpretation(s): *RfI#202110(rev1)*

Issue:

Issue Description:

For SFR FCS_TLSC_EXT.1.2 from NDcPP 2.2e, it gives the option listed below in selection for reference identifiers:

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types].

The following are the Assurance Activities for FCS_TLSC_EXT.1.2 Test #2:

The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.

The Application Note 105 of NDcPP 2.2e states the following:

Where TLS is used for connections to/from non-TOE entities (relevant to FTP_ITC and FTP_TRP), the ST author shall select RFC 6125. For distributed TOEs (TLS connections relevant to FPT_ITT), the ST author

may select either RFC 6125 or RFC 5280. If RFC 5280 is selected, the selection is completed by listing the AttributeType (e.g. 'id-at-serialNumber') as defined in RFC 5280 Appendix A. The selection should only list those attributes that are significant (i.e. those which are used by the client for reference identifier matching), though the Subject field (DN) may contain other attribute types that are not significant for the purpose of reference identifier matching. In the TSS the ST author describes which attribute type, or combination of attributes types, are used by the client to match the presented identifier with the configured identifier. The ST author selects "the reference identifier per RFC 6125 section 6" for TOEs that support FQDN, SRV, and URI identifiers.

The ST author selects "IPv4…" and/or "IPv6…" based on the IP versions the TOE supports. The ST author selects "CN or SAN" when IP addresses are supported in the "CN" or "SAN" when the TOE mandates the presence of the SAN. When "CN or SAN" is selected, the TOE only checks the CN when the certificate does not contain the SAN extension.

The rules for verification of identity are described in Section 6 of RFC 6125. Additionally, IP address identifiers may be supported in the SAN or CN. The reference identifier is established by the Administrator (e.g. entering a URL into a web browser or clicking a link), by configuration (e.g. configuring the name of a mail server or authentication server), or by an application (e.g. a parameter of an API) depending on the application service. Based on a singular reference identifier's source domain or IP address and application service type (e.g. HTTP, SIP, LDAP), the client establishes all reference identifiers which are acceptable, such as a Common Name for the Subject Name field of the certificate and a (case-insensitive) DNS name, URI name, and Service Name for the Subject Alternative Name field. The client then compares this list of all acceptable reference identifiers to the presented identifiers in the TLS server's certificate.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name may be supported for the purposes of backwards compatibility. When the SAN extension is present in a certificate, the CN must be ignored.

Finally, the client should avoid constructing reference identifiers using wildcards. However, if the presented identifiers include wildcards and the TOE supports wildcard, the client must follow the best practices regarding matching; these best practices are captured in the evaluation activity. The exception being, the use of wildcards is not supported when using IP address as the reference identifier

---

CCTL Question/Clarification

The vendor would like to select "IPv4 address in SAN, IPv6 address in the SAN" for the product as reference identifiers. At present, the vendor is compliant to RFC 6125 section 6.

Application Note 105 and the requirements for the SFR for FCS_TLSC_EXT.1.2 allows support for IP addresses (IPv4 and IPv6 addresses) and mandates conformance to RFC 6125, Section 6. That being said, RFC 6125, Section 6 does not specify any rules for IP address (IPv4 and IPv6) verification as reference identifiers. The testing requirements do not align with the SFR selections.

CCTL Question:

The CCTL would like to understand when a product does not mandate the presence of SAN and if the vendor wants to select “IPv4 address in SAN, IPv6 address in the SAN” as a reference identifier, what would be preferred method for verification of Subject Alternative Name using the IP address?

Resolution:

The NIT came to the conclusion that Test 2 should not cause any problems in the scenario described in the RfI and therefore does not need to be updated. During the review the NIT realized, though, that FCS_DTLSC_EXT.1.2 and FCS_TLSC_EXT.1.2 Test 6 might be confusing, as it is not clear that asterisks intended to represent wild cards.

SD NDv2.2 FCS_DTLSC_EXT.1.2 and FCS_TLSC_EXT.1.2 Test 6 shall therefore be changed as follows:

<old> Test 6:[conditional] If IP addresses are supported, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with an asterisk (*) (e.g. CN=192.168.1.* when connecting to 192.168.1.20, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6).</old>

shall be replaced by

<new> Objective: The objective of this test is to ensure the TOE is able to differentiate between IP address identifiers that are not allowed to contain wildcards and other types of identifiers that may contain wildcards.

Test 6: [conditional] If IP address identifiers supported in the SAN or CN, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with a wildcard asterisk (*) (e.g. CN=*.168.0.1 when connecting to 192.168.0.1, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6).</new>

This negative test corresponds to the following section of the Application Note 64/105: "The exception being, the use of wildcards is not supported when using IP address as the reference identifier."

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

None