Network Device Interpretation # 201822

FCS_(D)TLSC_EXT.X.2 IP addresses in reference identifiers

Status: ☒ *Active* ☐ *Inactive*

Date: *14-Aug-2019*

End of proposed Transition Period (to be updated after TR2TD process): *14-Nov-2019*

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): *NDcPPv2.1, SD NDv2.1; FWcPPv2.1, SD FWv2.1*

Affected Section(s): *FAU_GEN.1*

Superseded Interpretation(s): *None*

Issue:

FCS_TLSC_EXT.X.2 and FCS_DTLSC_EXT.X.2 require matching the presented identifier with the reference identifier per RFC 6125 section 6. RFC 6125 does not specify the use of an IP address as an expected identifier or provide rules on an IP address as a presented identifier. If matching must be performed according to the RFC, matching based on IP address is not allowed. The application notes say "…support for use of IP addresses in the Subject Name or Subject Alternative name is … may be implemented." The SFR and Application Note are inconsistent on whether IP addresses may be supported.

If IP addresses are supported, this leads to ambiguity in Test 5. Since it is supposed to apply to each supported type of reference identifier, it seems to apply to IP addresses. It does not make sense to match a certificate on *.10.10.10.

Note: FCS_DTLSC_EXT.X.2 does not include an Application Note indicating that IP addresses may be supported; however, we believe this update should apply to DTLSC as well.

<u>Proposed Resolution:</u>

-Update the SFR to read: "The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6 [selection: RFC 4513 section 3.1.3.2, no other comparison methods]."

While the RFC is specific to LDAP, this section provides a good description of IP address matching. The Application Note should provide instructions to select "RFC 4513 section 3.1.3.2" if IP addresses are supported.

-Update the test text to read, "The evaluator shall perform the following wildcard tests on the FQDN for each supported type of reference identifier that includes an FQDN."

Resolution:

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

FCS_TLSC_EXT.x.2 and FCS_DTLSC_EXT.x.2 shall be updated as follows:

<old>"The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6" </old>

shall be replaced by

<new>"The TSF shall verify that the presented identifiers of the following types: [selection: identifiers defined in RFC 6125, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN] are matched to reference identifiers."</new>

The Application Notes shall be replaced as follows:

<new>The ST author selects "identifiers defined in RFC 6125" 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. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented.

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.

Supporting Document FCS_TLSC_EXT.x.2 and FCS_DTLSC_EXT.x.2 TSS shall be updated as follows:

The following shall be appended

<new>"If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC5952 for IPv6, RFC 3986 for IPv4) is enforced.</new>

Supporting Document FCS_TLSC_EXT.x.2 and FCS_DTLSC_EXT.x.2 TSS shall be replaced as follows:

<new> The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. </new>

Supporting Document FCS_TLSC_EXT.x.2 and FCS_DTLSC_EXT.x.2 Tests shall be updated as follows:

Note that where a (D)TLS channel is being used between components of a distributed TOE for FPT_ITT.1, the requirements to have the reference identifier established by the user are relaxed and the identifier may also be established through a "Gatekeeper" discovery process. The TSS should describe the discovery process and highlight how the reference identifier is supplied to the "joining" component.

IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:

- IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.
- IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.

The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a (D)TLS connection:

a) Test 1: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN.

   Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.

a) 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.

b) Test 3: [conditional]: If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.

c) Test 4: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).

d) Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):

1) The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.

2) The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds if wildcards are supported or fails if wildcards are not supported. The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)

e) Test 6: [conditional] If URI or Service name reference identifiers are supported, the evaluator shall configure the DNS name and the service identifier. The evaluator shall present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator shall repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.

f) Test 7: [conditional] If pinned certificates are supported the evaluator shall present a certificate that does not match the pinned certificate and verify that the connection fails.

g) Test 8: [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).

Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 8.

Rationale:

See "Issue" section

Further Action:

None.

Action by Network iTC:

None.