Network Device Interpretation # 201834

ITT Comm UUID Reference Identifier

Status: ☒ *Active* ☒ *Inactive*

Date: *6-Jun-2019*

End of proposed Transition Period (to be updated after TR2TD process): *6-Jun-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): *NDcPP V2.0e, FWcPP V2.0e, NDcPP V2.1*

Affected Section(s): *FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2*

Superseded Interpretation(s): *None*

Issue:

The CCTL is working with a vendor of a network appliance environment intending to claim conformance to[NDCPP20E]. The appliance supports TLS communication as part of an ITT communication between two TOE devices.

The testing in the Supporting Document for FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2 requires the following:

The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a 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. (TD0257 applied)

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.

b) 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.

c) 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. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted. (TD0257 applied)

d) 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 network appliance environment consists of Management devices and network appliances. The Administrator registers the network device to the manager by providing the network address of the manager and a shared secret that the manager has also been provided. During this initial registration process both devices use a proprietary protocol to establish an encrypted TLS tunnel with each device using a local CA and end entity cert. The local CA and end entity certificates exist on each network appliance and management device. These local certs are generated automatically during their initial installation and setup. Within this TLS tunnel, as part of the vendor specific protocol, the two devices exchange their Universally Unique Identifiers (UUID) as well as shared secrets to complete the registration. If the shared secrets do not match the connection will terminate. If the shared secret matches the expected secret for the configured network address (of the network appliance), the management device will generate a new end entity cert for the network appliance and push it to the device for future use. At no point does the TOE ever use or accept a non-TOE (third party) certificate authority. The TOE environment is always in control of the certificates being generated within the ITT communication, meaning it can be assured that the CA's private key is never available to anyone but an authorized administrator.

All subsequent communication between the manager and the network appliance will be encrypted with TLS. The initial TLS tunnel (parent layer) using each device's local certs still occurs but this time the devices exchange UUIDs. If the UUIDs match an existing registration, a second embedded TLS tunnel is established. In this child layer the network device authenticates itself using the end entity cert that was provided by the manager during registration, and the manager authenticates with its end entity cert signed by the same CA. During this certificate exchange the certificates are validated and the identity of the devices are confirmed. The identity of the devices are verified by the title field in the certificate subject, which contains the devices UUID. Therefore the testing of verifying identity by only CN and SAN are not applicable to this evaluation environment.

CCTL Proposal

The CCTL proposes the following alternative testing requirements for FCS_TLSC_EXT.1.2 and FCS_TLSC_EXT.2.2 to demonstrate the successful verification of the UUID identifier.

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

a) Test 1: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier, does not contain the SAN extension and does not contain the correct UUID. The evaluator shall verify that the connection fails. (TD0257 applied)

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.

b) Test 2: The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, does not contain an identifier in the SAN that matches the reference identifier and does not contain the correct UUID. The evaluator shall verify that the connection fails.

c) Test 3 [conditional]: a) The evaluator shall present a server certificate that contains a CN that matches the reference identifier, does not contain the SAN extension and does not contain the correct UUID. The evaluator shall verify that the connection fails.

b) The evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension and does contain the correct UUID. The evaluator shall verify that the connection succeeds.

d) Test 4: a)The evaluator shall present a server certificate that contains a CN that does not match the reference identifier, does contain an identifier in the SAN that matches and does not contain the correct UUID. The evaluator shall verify that the connection fails.

Test 4: b) The evaluator shall present a server certificate that contains a CN that does not match the reference identifier, does contain an identifier in the SAN that matches and does contain the correct UUID. The evaluator shall verify that the connection succeeds.

Resolution:

NDcPP V2.0e, FWcPP V2.0e and NDcPP V2.1 do not support the use of UUIDs. In a future version UUIDs might be supported by NDcPP/FWcPP. But the support for UUIDs would need to be added through the MINT and cannot be done through the NIT.

Rationale:

See Issue and Resolution sections.

Further Action:

The iTC should consider adding support for UUIDs in a future revision of NDcPP/FWcPP.

Action by Network iTC:

None