Network Device Interpretation # 201720

TLS wildcard checking

Status: ☒ *Active* ☐ *Inactive*

Date: *9-Feb-2018*

End of proposed Transition Period (to be updated after TR2TD process): *16-Mar-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): *ND SD V1.0, ND SD V2.0*

Affected Section(s): *FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.2.2, FCS_DTLSC_EXT.1.2 (only ND SD V2.0), FCS_DTLSC_EXT.2.2(only ND SD V2.0), Test 5, 2.)*

Superseded Interpretation(s): *None*

Issue:

NDcPP's FCS_TLSC_EXT.1.2 asks TOE to check reference identifiers per RFC 6125, and the App Note states, "Finally, the 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." and the supporting document includes a number of wildcard checking tests.

However, RFC 6125 states in section "6.4.3. Checking of Wildcard Certificates

A client employing this specification's rules MAY match the reference identifier against a presented identifier whose DNS domain name portion contains the wildcard character '' as part or all of a label..."*

So because the RFC makes support for wildcards is optional ("MAY"), we believe that a TOE should have the ability to reject certificates containing wildcards. A TOE exhibiting this behavior would reject all test connections. We think this is acceptable (given the RFC) and secure behavior (albeit perhaps a bit inflexible). There are many situations where this inflexibility does not matter (e.g., TLS used for audit log export).

Resolutions:

The NIT acknowledges the issue described in the 'Issue' section.

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.

Rationale:

As stated in the 'Issue' section above.

Further Action:

To revise FCS_TLSx SFRs to clearly define supported identifiers based on RFC 6125.

Action by Network iTC:

None