Network Device Interpretation # 201913rev2

RSA-based ciphers and the Server Key Exchange message

Status: ☒ *Active* □ *Inactive*

Date: *11-Dec-2019*

End of proposed Transition Period (to be updated after TR2TD process): *11-Dec-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): *ND SDv2.0e, ND SD v2.1, FW SDv2.0e*

Affected Section(s): *FCS_TLSS_EXT.*.3, FCS_DTLSS_EXT.*.4*

Superseded Interpretation(s): *RfI#201913(rev1)*

Issue:

FCS_TLSS_EXT.1.3 TSS

539 The evaluator shall verify that the TSS describes the key agreement parameters of the server Key Exchange message.

Question: As this activity is not marked as conditional, what description must be provided in cases of RSA-based ciphers?

Background information:

If RSA-based cipher is used, then the client retrieves the public key from the server certificate and encrypts the premaster secret with this key. In such cases, the Server's Certificate message is sufficient and no additional information is required to securely communicate a premaster secret to the server.

Consequently, no ServerKeyExchange message is needed and no key agreement parameters are exchanged.

Resolution:

The following text shall be modified in the ND SD:

The TSS requirements for FCS_DTLSS_EXT..4 and FCS_TLSS_EXT.*.3 shall be replaced as follows:*

<old>

The evaluator shall verify that the TSS describes the key agreement parameters of the server Key Exchange message.

</old>

shall be replaced by

<new>

If using ECDHE or DHE ciphers, the evaluator shall verify that the TSS describes the key agreement parameters of the server Key Exchange message.

</new>

Rationale:

See Issue section.

Change in rev2: Extension to ND SDv2.0e as well as FW SDv2.0e upon request.

Further Action:

None

Action by Network iTC:

None