Network Device Interpretation # 202107

TLS Server and Key Agreement Parameters

Status: ☒ *Active* ☐ *Inactive*

Date: *9-Aug-2021*

End of proposed Transition Period (to be updated after TR2TD process): *9-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): *NDSD v2.2*

Affected Section(s): *FCS_TLSS_EXT.1.3*

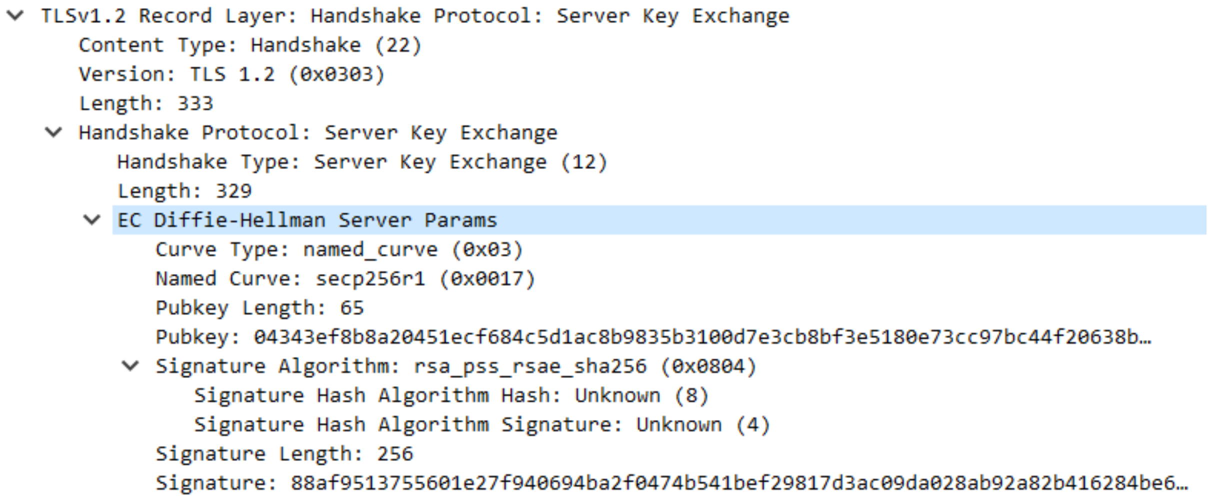
Superseded Interpretation(s): *None*

Issue:

FCS_TLSS_EXT.1.3 TSS Assurance Activity states: "If using ECDHE or DHE ciphers, the evaluator shall verify that the TSS describes the key agreement parameters of the server key exchange message."

Please clarify what is being asked to document/verify by this assurance activity in cases of ECDHE? Key agreement parameters are pre-defined for each curve and communicated in the Server Key Exchange Message as described in RFC 5246 Section 7.4.2.

Here is sample ECDHE Key Exchange Message as displayed by Wireshark:



```
v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 333
  v Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 329
    v EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: secp256r1 (0x0017)
        Pubkey Length: 65
        Pubkey: 04343ef8b8a20451ecf684c5d1ac8b9835b3100d7e3cb8bf3e5180e73cc97bc44f20638b…
      v Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
          Signature Hash Algorithm Hash: Unknown (8)
          Signature Hash Algorithm Signature: Unknown (4)
        Signature Length: 256
        Signature: 88af9513755601e27f940694ba2f0474b541bef29817d3ac09da028ab92a82b416284be6…
```

Resolution:

The SFR element in question is used to define key establishment server parameters and the intent of this TSS Assurance Activity is to declare all supported Diffie-Hellman Groups and/or Elliptic Curves that could be used in TLS key establishment.

In SDNDv2.2, FCS_TLSS_EXT.1.3 TSS Assurance Activity shall be replaced as follows:

<old>
If using ECDHE or DHE ciphers, the evaluator shall verify that the TSS describes the key agreement parameters of the server key exchange message.
</old>

<new>
If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.
</new>

Rationale:

see Resolution

Further Action:

None

Action by Network iTC:

None