Network Device Interpretation # 201826

FCS_CKM.2 and elliptic curve-based key establishment

Status: ☒ *Active* ☐ *Inactive*

Date: *30-Jan-2019*

End of proposed Transition Period (to be updated after TR2TD process): *30-Jan-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, NDcPP V2.1, FWcPP V2.0e*

Affected Section(s): *FCS_CKM.1, FCS_CKM.2*

Superseded Interpretation(s): *None*

Issue:

Background:

A network device acting as a TLS server supports only TLS_ECDHE_RSA_WITH_* ciphers. Here is high-level description of how it works:

1. Client sends “Client Hello” to server providing list of supported ciphers
2. Server responds with “Server Hello” selecting one of the ciphers from sensor list that server supports. This will be TLS_ECDHE_RSA_WITH_* in our case.
3. Server also sends “Server Certificate” message. This includes RSA-based certificate of the server signed by a cert authority. The message contains chain of certs up to a trust anchor. Upon receiving this message, client performs certificate validation.
4. Server generates ephemeral ECDH parameters and sends public parameter in “Server Key Exchange” message. The EC public parameter is signed by RSA private key of server.
5. Client verifies RSA signature put on ECDH public parameter by the server. This confirms that it is talking to the same server whose certificate was validated earlier in the process.
6. Client then generates ECDH parameters and sends them signed to the server. Again as before, digital signature aspect of ECDSA is not used. Client generates TLS pre-master secret using server’s public ECDH parameter and its own ECDH private parameter.
7. Client sends “Client Key Exchange” message with client’s ECDH public parameter.
8. “Finished” messages exchanged and TLS channel is established.

Issue

FCS_CKM.2 selection: “Elliptic curve-based key establishment schemes…” that would be claimed in this scenario does not allow specification of supported EC curves (see SP 800-56A Appendix D for complete list).

Resolution:

The NIT acknowledges the issue described in the Issue section. The first sentence of the application note for FCS_CKM.1 shall be modified as follows:

<old>The ST author selects all key generation schemes used for key establishment and device authentication.</old>

Shall be replaced by

<new>The ST author selects all key generation schemes used for key establishment (including generation of ephemeral keys) and device authentication.</new>

Rationale:

The modified application note clarifies that FCS_CKM.1 also applies to ephemeral keys.

Further Action:

None.

Action by Network iTC:

None.