Network Device Interpretation # 201904rev3

Identification of usage of cryptographic schemes

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, FW SDv2.0e, ND SD v2.1*

Affected Section(s): *FCS_CKM.2*

Superseded Interpretation(s): *RfI#201903, RfI#201904rev2*

Issue:

ND Supporting Document, FCS_CKM.2 Cryptographic Key Establishment, Section 2.2.2.1 TSS states:

"If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme (including whether the TOE acts as a sender, a recipient, or both)."

Please clarify if "including whether the TOE acts as a sender, a recipient, or both" is normative or informative statement. If normative, please clarify necessary level of detail that must be present in the TSS. For example, is it sufficient to list supported protocols and corresponding key establishment methods?

Alternatively, clarify this requirement in the following way:

"If the ST specifies support for both finite field and elliptic-curve cryptography and more than one cryptographic protocol, the evaluator shall examine the TSS to verify that it identifies supported key establishment methods for each protocol."

Resolution:

The TSS guidance shall be modified as the following.

<old>

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme (including whether the TOE *acts as a sender, a recipient, or both). If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall describe how the implementation meets RFC 3526 Section 3.*

</old>

to

<new>

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.

If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall affirm that the TOE implements RFC 3526 Section 3.

The intent of this activity is to be able to identify the scheme being used by each service. This would mean, for example, one way to document scheme usage could be:

Scheme	*SFR*	*Service*
RSA	*FCS_TLSS_EXT.1*	*Administration*
ECDH	*FCS_SSHC_EXT.1*	*Audit Server*
Diffie-Hellman (Group 14)	*FCS_SSHC_EXT.1*	*Backup Server*
ECDH	*FCS_IPSEC_EXT.1*	*Authentication Server*

The information provided in the example above does not necessarily have to be included as a table but can be presented in other ways as long as the necessary data is available.

</new>

Rationale:

See Issue section.

Change in rev2: The resolution in RfI#201904rev2 resolves the conflict regarding the concurrent wording changes in RfI#201903 and RfI#201904(rev1).

Change in rev3: Extension to ND SDv2.0e as well as FW SDv2.0e upon request.

Further Action:

None

Action by Network iTC:

None