Network Device Interpretation # 202605

FCS_CKM_EXT.7 Application Note

Status: ☒ *Active* ☐ *Inactive*

Date: *17-Mar-2026*

End of proposed Transition Period (to be updated after TR2TD process): *1-Jan-2024*

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 v4.0, NDSD v4.0*

Affected Section(s): *FCS_CKM_EXT.7 App Note 14*

Superseded Interpretation(s): *None*

Issue:

Issue:

In NDcPP40, the SFR FCS_CKM_EXT.7 has a typo in application note 14. It states, “This requirement specifies key transport schemes. Key agreement schemes refer to cases in which two or more parties want to establish a single key between them, and all parties contribute to the entropy of the agreed-upon key.”

This should state, “This requirement specifies key agreement schemes.”, as key transport is covered by FCS_CKM.2.

Proposed resolution:

See above.

Resolution:

FCS_CKM_EXT.7 Application Note 14 shall be modified as follows:

{old}

This requirement specifies key transport schemes. Key agreement schemes refer to cases in which two or more parties want to establish a single key between them, and all parties contribute to the entropy of the agreed-upon key.

The ST author selects all key agreement schemes used for the selected cryptographic protocols.

The elliptic curves used for the key agreement scheme correlate with the curves specified in FCS_CKM.1.1/AKG.

The static domain parameters approved for the finite field-based key agreement scheme are specified by the key generation according to FCS_CKM.1.1/AKG.

For Key Transport, see FCS_CKM.2 in Annex A.

{/old}

{new}

This component contains methods for multi-party key agreement in which two or more parties contribute material used to derive the shared key used by each party to encrypt and decrypt incoming and outgoing messages. TOEs can use the keys as symmetric keys, keyed-hash keys, or cryptographic keys for key derivation functions.

The ST author selects all key agreement schemes used for the selected cryptographic protocols.

The elliptic curves used for the key agreement scheme correlate with the curves specified in FCS_CKM.1.1/AKG.

The static domain parameters approved for the finite field-based key agreement scheme are specified by the key generation according to FCS_CKM.1.1/AKG.

For Key Transport, see FCS_CKM.2 in Annex A.

{/new}

Rationale:

NDcPPv4 cryptographic SFRs are based on Specification of Functional Requirements for Cryptography, aka "Crypto Catalog." Application Note 14 has been updated with verbiage that matches the text contained in the Crypto Catalog.

Further Action:

None

Action by Network iTC:

None