FDE Interpretation # 202001

Status: ☒*Active* □ *Inactive*

Date: 03-10-2020

Type of Document: ☒*Technical Decision* □ *Technical Recommendation*

Approved by: ☒*FDE iTC Interpretations Team* □ *FDE iTC*

Affected Document(s): FDE AA cPP v2.0 + Errata 20190201

Affected Section(s): FCS_AFA_EXT.1.1

Superseded Interpretation(s):

Issue:

Received CSfC comment that FCS AFA EXT 1.1 does not allow ECC for smartcards. This should be allowed, would require only minor change.
The solution is updating AFA 1 to read ... protected using [selection: RSA with key size [selection: 2048 bits, 3072 bits, 4096 bits], ECC using curve [selection: P-256, P-384, P-521]]...
No changes to the SD.

Resolution:

The FIT acknowledges the issues described in the 'Issue' section above. **Bolding** and ~~strikethrough~~ indicates change. The smartcard selection within FCS_AFA_EXT.1.1 will be modified to state:

• an external Smartcard factor that is ~~at least the same bit-length as the DEK, and is~~ protecting a submask that is [selection: generated by the TOE (using the RBG as specified in FCS_RBG_EXT.1), generated by the Host Platform] protected using **[selection:** RSA with key size [selection: 2048 bits, 3072 bits, 4096 bits]**, ECC schemes using "NIST curves" of [selection: P-256, P-384, P-521]]**, with user presence proved by presentation of the smartcard and [selection: none, an OE defined PIN, a configurable PIN].

Rationale:

The FIT agrees that there was never any intent by the iTC to exclude ECC support relating to smartcards, while making this minor edit the requirement is being adjusted to be more accurate.

Further Action:

None.

Action by FDE iTC:

None.