HCD0006 - Technical issue in TSS assurace activity for FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)

Version: 1, Published: 2024-02-02

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)

Issue Description

The TSS assurance activity does not cover the selection of section 6.3 of NIST SP 800-133 Rev.2 in the FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys) SFR.

Resolution

Update the TSS assurance activity to cover the generation of symmetric keys by combining one or more keys and other data in accordance with section 6.3 of NIST SP 800-133 Rev.2.

CPP_HCD_V1.0_supporting_doc

The SD is updated as follows (yellow highlights for additions, strikethrough for deletions) per section that is being updated:

2.2.1.1. TSS

The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked and how the TOE obtains a symmetric key through direct generation from a random bit generator as specified in FCS_RBG_EXT.1 or by combining one or more symmetric keys and other data.

Tracking

Issue #18