

Please accept this document as confirmation of the EMVCo Security Evaluation Process.

Certificate Number : ICCN0294

Date of issuance 30 Nov 2022

Expiry Date: 30 Nov 2024

Company: Infineon Technologies AG

Address: AM Campeon 1-15
Neubiberg 85579 Germany

Master Component: IFX_ECI_75h[01h–04h, 07h–08h, 13h, 0Bh–0Fh, 10h–12h, 14h–18h, 1Ah–1Fh]

Hardware Revision: H11

Child Lot 1: IFX_ECI_6Ch[05h, 19h]

Child Lot 2: IFX_ECI_88h[01h – 0Dh]

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): TSMC Taichung (Fab 15A), Taiwan

Firmware name / version: FW 80.506.04.1

Crypto. library name / version: CS 4.02.012 & 4.06.002

Other libraries name / version: FL 9.30.001, HSL 04.05.0030, SLC26V19c, UMSLC 02.01.0040, NRGTM lib
06.03.4496 & 06.10.0003 (out of TSF)

Bootloader name / version: BOS FW 80.506.04.1

Security Laboratory: TÜVIT

Conditions of Certification: User Guidance document(s) must be followed.

Authorized by: Alan Mushing, SEWG Chair
EMVCo, LLC

Date: 20 Mar 2024

Disclaimer: Although the secure implementation of any security mechanisms and product functionalities may be evaluated, the EMVCo Security Evaluation Process does not validate the cryptographic algorithms, methods and protocols themselves nor the absence of flaws or defects in the specifications used for product development.

The ICCN number must be mentioned to all vendors or when shipping the product. The use of the ICCN number is limited to the product as detailed below. Please also reference the ICCN number in any communication with EMVCo.

The EMVCo Security Evaluation Process is intended to provide valuable and practical information relating to the general security performance characteristics and the suitability of use for smart card related products and IC chip-based tokens. The EMVCo Security Evaluation Process is designed to ensure a robust security foundation for these products at the product family and component level. The EMVCo Security Evaluation Process is an evolving process in relation to new attack techniques and technology. EMVCo therefore reserves the right to perform new/random security testing throughout the lifetime of the card which may impact certification. The full terms and conditions upon which EMVCo Compliance Certificates are issued by EMVCo are contained in the EMVCo Security Evaluation Process Document and the EMVCo Security Evaluation Certification Contract.

User Guidance Documents:

- TEGRION™ SLC26 (32-bit Security Controller – V19) Hardware Reference Manual, Rev. 3.1, 8 Aug 2023
- TEGRION™ SLC26 (32-bit Security Controller - V19) Errata Sheet, Rev. 5.0, 12 Dec 2023
- SLx2 Security Controller Family Programmer's Reference Manual, SLx2_DFP, Rev. 1.3.0, 19 Oct 2023
- SLx2 Security Controller Family, Production and Personalization Manual, Flash Loader V9, v09.30, 11 Aug 2023
- Crypto2304T V4, Rev. 2.0, 14 Jul 2023
- SLC26 32-bit Security Controller - V19, Security Guidelines, Rev. 1.00-3003, 26 Jul 2023
- CS-SLC26V19 CryptoSuite 32-bit Security Controller, User interface manual, v4.02.012, 3 Aug 2022
- CS-SLC26V19 CryptoSuite 32-bit Security Controller, User interface manual, v4.06.002, 11 Dec 2023

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.3, December 2022
- Security Guidelines for Smart Card Integrated Circuits, v2.2, December 2022

Disclaimer: Although the secure implementation of any security mechanisms and product functionalities may be evaluated, the EMVCo Security Evaluation Process does not validate the cryptographic algorithms, methods and protocols themselves nor the absence of flaws or defects in the specifications used for product development.

The ICCN number must be mentioned to all vendors or when shipping the product. The use of the ICCN number is limited to the product as detailed below. Please also reference the ICCN number in any communication with EMVCo.

The EMVCo Security Evaluation Process is intended to provide valuable and practical information relating to the general security performance characteristics and the suitability of use for smart card related products and IC chip-based tokens. The EMVCo Security Evaluation Process is designed to ensure a robust security foundation for these products at the product family and component level. The EMVCo Security Evaluation Process is an evolving process in relation to new attack techniques and technology. EMVCo therefore reserves the right to perform new/random security testing throughout the lifetime of the card which may impact certification. The full terms and conditions upon which EMVCo Compliance Certificates are issued by EMVCo are contained in the EMVCo Security Evaluation Process Document and the EMVCo Security Evaluation Certification Contract.