

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

Certificate Number : ICCN0315

Date of issuance 04 Jul 2025

Expiry Date: 04 Jul 2026

Company: Infineon Technologies AG

Address: AM Campeon 1-15
Neubiberg 85579 Germany

Master Component: IFX_ECI_A0h[0x01] & IFX_ECI_85h[0x02, 0x04, 0x05, 0x06, 0x07]

Hardware Revision: G12

Child Lot 1: IFX_ECI_9Bh[0x03] R11

Child Lot 2: IFX_ECI_9Bh[0x06] R12

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

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

Firmware name / version: FW 80.506.04.1 (G12) & 80.511.00.0 (R11 & R12) & FL v10.01.0001

Crypto. library name / version: CS-SLC21V24 5.02.003 & HSL 04.05.0040

Other libraries name / version: UMSLC 02.01.0040 & NRG™ 06.10.0002 & 06.10.0005

Bootloader name / version: See FW

Security Laboratory: TÜVIT

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC

Date: 04 Dec 2025

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. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.

User Guidance Documents:

- TEGRION™ SLC21 (32-bit Security Controller – V24) Hardware Reference Manual, v7.0, 14 May 2025
- TEGRION™ SLx2 security controller family Programmer's Reference Manual SLx2_DFP, v1.9.0, 16 Oct 2025
- SLC21 32-bit Security Controller - V24 Security Guidelines, v1.00-3099, 4 Jun 2025
- SLC21 (32-bit Security Controller – V24) Production and personalization manual Flash Loader V10, v10.01, 28 Jun 2023
- Crypto2304T V4, User Manual, v3.0, 21 Jun 2024
- TEGRION™ SLC21 (32-bit Security Controller – V24) Errata sheet, v6.0, 23 May 2025 (for IFX_ECI_A0h[0x01] & IFX_ECI_85h[0x05, 0x06, 0x07])
- TEGRION™ SLC21 (32-bit Security Controller – V34) Errata sheet, v2.0, 23 May 2025 (for IFX_ECI_9Bh[0x03] R11 & IFX_ECI_9Bh[0x06] R12)
- CS-SLC21V24 Crypto Suite 32-bit Security Controller User interface manual, v5.02.003, 02 Oct 2025
- Ascon-128 MISE Application Note, v1.1.3, 13 Sep 2023
- SHA256 MISE Application Note, v1.1.2, 13 Sep 2023

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.4, July 2024
- 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. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.