

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

**Certificate Number :** ICCN0299

**Date of issuance** 22 Mar 2023

**Expiry Date:** 22 Mar 2025

**Company:** Infineon Technologies AG

**Address:** AM Campeon 1-15  
Neubiberg 85579 Germany

**Master Component:** IFX\_ECI\_6Dh[0Ch-0Eh]

**Hardware Revision:** S12

Child Lot 1: IFX\_ECI\_6Eh[02h-12h]

Child Lot 2: IFX\_ECI\_6Fh[03h-0Dh]

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

**Manufacturing site(s):** Global Foundries, Singapore

**Firmware name / version:** BOS FW 80.311.04.1 & FL 09.13.0006

**Crypto. library name / version:** SCL 2.15.000, ACL 3.34.000, HCL 1.13.002 & RCL 1.10.007

**Other libraries name / version:** NRG™ SW 05.03.4097 (not part of the TSF), HSL 3.52.9708, UMSLC 01.30.0695

**Bootloader name / version:** See FW

**Security Laboratory:** TÜVIT

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

**Authorized by:** Alan Mushing, SEWG Chair  
EMVCo, LLC

**Date:** 28 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. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.

#### User Guidance Documents:

- SLC39 32-bit Security Controller – V23, Hardware Reference Manual, v2.0, 15 Jun 2022
- SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual, v5.7, 19 Oct 2023
- SLC39 32-bit Security Controller – V23, Security Guidelines, v1.00-2942, 5 Jan 2023
- SLx3 (40nm) Security Controllers Production and Personalization Manual, v09.13, 15 May 2023
- 32-bit Security Controller Crypto2304T V3, User Manual, v2.1, 16 Dec 2022
- HSL for SLCx7 V23, Hardware Support Library, v3.52.9708, 22 Jun 2022
- UMSLC library for SLCx7V23b User Mode Security Life Control, v01.30.0695, 4 Jul 2022
- SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC, v2.15.000, 20 Jul 2023
- Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox, v3.34.000, 21 Nov 2023
- RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional), v1.10.007, 16 Jun 2020
- HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional), v1.13.002, 7 May 2020

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