IC Security Evaluation Certificate

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

Certificate Number : ICCN0280

Date of issuance 03 Apr 2020 **Expiry Date: 03 Apr 2026**

Company: Infineon Technologies AG

Address: AM Campeon 1-15
Neubiberg 85579 Germany

Master Component: IFX_ECI_46h[01h-03h]

Hardware Revision: S11

Child Lot 1: IFX_ECI_50h[01h-34h]
Child Lot 2: IFX_ECI_5Ch[01h-13h]
Child Lot 3: IFX_ECI_5Eh[01h-09h]
Child Lot 4: IFX_ECI_74h[01h-04h]
Child Lot 5: -

Manufacturing site(s): Global Foundries, Singapore

Firmware name / version: BOS&POWS 80.309.05.0

Crypto. library name / version: SCL 2.15.000, ACL 3.33.003, 3.34.000 & 3.35.001, HCL 1.13.002

Other libraries name / version: FL 09.13.0004, HSL 3.52.9708, UMSLC 01.30.0564, NRG™ 05.03.4097, RCL 1.10.007

Bootloader name / version: BOS&POWS 80.309.05.0

Security Laboratory: TÜVIT

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 22 Apr 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:

- 32-bit Security Controller – V22, Hardware Reference Manual, v2.3, 23 Oct 2020
- 32-bit Security Controllers, SLx1/SLx3 Controller Family, Programmer's Reference Manual, v5.7, 19 Oct 2023
- 32-bit Security Controller – V22, Security Guidelines, v1.00-2697, 9 Nov 2020
- SLx3 (40nm) Security Controllers Production and personalization manual, v09.13, 15 May 2023
- 32-bit Security Controller Crypto2304T V3, User Manual, v3.0, 21 Jun 2024
- HSL SLCx V22 Hardware Support Library (optional), v3.52.9708, 25 Jan 2021
- UMSLC library for SLCx7 V22a in 40nm, v01.30.0564, 23 Mar 2020
- SCL37-SCP-v440-C40 AES/DES/MAC (optional), v2.15.000, 20 Jul 2023
- ACL37-Crypto2304T-C40 Asymmetric Crypto Library RSA/ECC/Toolbox (optional), v3.33.003, 16 Aug 2024
- ACL37-Crypto2304T-C40 Asymmetric Crypto Library RSA/ECC/Toolbox (optional), v3.34.000, 16 Aug 2024
- ACL37-Crypto2304T-C40 Asymmetric Crypto Library RSA/ECC/Toolbox (optional), v3.35.001, 15 Nov 2024
- HCL37-CPU-C40 Hash Crypto Library (optional), v1.13.002, 7 May 2020
- RCL37-X-C40 Random Crypto Library (optional), v1.10.007, 16 Jun 2020

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.4, July 2024
- Security Guidelines for Smart Card Integrated Circuits, v2.2, December 2022