



## EMVCo Product Approval (IC)

Please accept this document as confirmation of the EMVCo Security Evaluation process

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.

**ICCN: ICCN0280**

**Date ICCN issued: 03 Apr 2020**

**ICCN Expiry Date: 03 Apr 2022**

**Company: Infineon Technologies AG**

**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-0Dh]

Child Lot 3: IFX\_ECI\_5Eh[01h-09h]

Child Lot 4: -

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, 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

**User Guidance:**

- 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, v4.6, 13 Oct 2020
- 32-bit Security Controller – V22, Security Guidelines, v1.00-2697, 9 Nov 2020
- SLx3 (40nm) Security Controllers Production and personalization manual, v09.13, 29 Oct 2020
- 32-bit Security Controller Crypto2304T V3, User Manual, v2.0, 24 Apr 2019
- 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, 1 Jun 2021
- ACL37-Crypto2304T-C40 RSA/ECC/Toolbox (optional), v3.33.003, 18 Mar 2021
- 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

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

**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 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.