

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

**Certificate Number :** ICCN0257

**Date of issuance** 10 Aug 2018

**Expiry Date:** 10 Aug 2024

**Company:** Infineon Technologies AG

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

**Master Component:** IFX\_ECI\_22h[1h-1Eh]

**Hardware Revision:** G12

Child Lot 1: IFX\_ECI\_24h[1h-4h]

Child Lot 2: IFX\_ECI\_3Ah[1h-3h]

Child Lot 3: IFX\_ECI\_4Ch[1h-2h]

Child Lot 4: -

Child Lot 5: -

**Manufacturing site(s):** TSMC Tainan, Taiwan

**Firmware name / version:** 80.102.06.0 or 80.102.06.1

**Crypto. library name / version:** ACL v2.07.003 & v2.08.007, SCL v2.04.002 & v2.13.001, HCL v1.12.001

**Other libraries name / version:** HSL v03.11.8339 & v03.12.8812, NRG SW v02.03.3446, CIPURSE™  
v02.00.0004

**Bootloader name / version:** Included in firmware

**Security Laboratory:** TÜVIT

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

Signed by:

Alan Mushing, SEWG Chair  
EMVCo, LLC

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:

- 16-bit Security Controller Family -V05, Hardware Reference Manual (HRM), Rev 5.0, 14 Jun 2019
- Production and Personalization, 16-bit Security Controller in 65nm, Rev 3.6, 24 Jun 2019
- 16-bit Security Controller, 65-nm Technology, Programmer's Reference Manual (PRM), Rev. 9.14, 3 Dec 2019
- CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, v2.07.003, 23 Mar 2022
- CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, v2.08.007, 23 Mar 2022
- 16-bit Security Controller, Crypto@2304T V3, User Manual, Rev. 1.4.2, 14 Dec 2022
- 16-bit Security Controller - V05, Security Guidelines, v1.01-2597, 20 Aug 2020
- 16-bit Security Controller - V05, Errata Sheet, Rev. 10.0, 25 Feb 2021
- Hardware Support Library for SLCx2 (HSL), User Guidance, v03.11.8339, 12 Jul 2018
- Hardware Support Library for SLCx2 (HSL), User Guidance, v03.12.8812, 8 Jul 2019
- SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES, 16-bit Security Controller, User Interface, v2.04.002, 20 Dec 2022
- SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4, AES/DES/MAC, 16-bit Security Controller, User interface, v2.13.001, 20 Dec 2022
- HCL52-CPU-C65, Hash Crypto Library for CPU, SHA, 16-bit Security controller, User interface manual, v1.12.001, 14 Jan 2020
- CIPURSETM Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface, v1.6, 2 Feb 2018

#### 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.