

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

Certificate Number : ICCN0255

Date of issuance 26 Apr 2018

Expiry Date: 26 Apr 2024

Company: Infineon Technologies AG

Address: AM Campeon 1-15
Neubiberg 85579 Germany

Master Component: IFX_ECI_29h[1h,2h,3h,5h]

Hardware Revision: G12

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): TSMC Tainan (Taiwan)

Firmware name / version: 80.201.04.1 & 80.201.04.2

Crypto. library name / version: ACLv2.08.006,v3.03.003,v3.04.001,SCLv2.13.001,CIPURSE™CL
v02.00.0005

Other libraries name / version: HSL v2.01.6198, NRG Software lib v04.03.3431

Bootloader name / version: BOS 80.201.04.1 & 80.201.04.2

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:

- 32-bit Security Controller - V07 Hardware Reference Manual, Revision 6.0, 13 Jun 2019
- ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, 12 Feb 2010, ARM Limited
- SLC37 (65 nm) Security Controllers, Programmers Reference Manual, Revision 5.3, 8 Jul 2022
- Production and personalization 32-bit ARM based security controller User's Manual, Revision 3.5, 17 Dec 2021
- 32-bit Security Controller- V07 Errata Sheet, Revision 7.2, 24 Jan 2022
- 32-bit Security Controller – V07 Security Guidelines, Version 1.01-2761, 19 Jul 2021
- SLC37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User Interface, Version 2.13.001, 16 Jun 2021
- 32-bit Security Controller Crypto@2304T V3 User Manual, Revision 2.1, 16 Dec 2022
- CIPURSE™ Crypto Library CCL37xCIP v02.00.0005 CIPURSE™ V2 User Interface, Revision 1.4, 13 Mar 2018
- SLxx7-C65 Hardware Support Library, Revision 1.3, 05 Jul 2019
- ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface (v2.08.006), 20 Jun 2022
- ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface (v3.03.003), 20 Jun 2022
- ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface (v3.04.001), 20 Jun 2022

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.