

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

Certificate Number : ICCN0254

Date of issuance: 25 May 2018

Expiry Date: 25 May 2024

Company: NXP Semiconductors Germany GmbH

Address: Troplowitzstrasse 20
Hamburg 22529 Germany

Master Component: SN100 Series

Hardware Revision: B2.1 C25, C48 & C58

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): GlobalFoundries, Singapore (GF7), Dresden (GF1, C48/C58), SMIC, Beijing (C48/C58)

Firmware name / version: Factory OS v4.2.0, Flash Driver Software v4.0.8

Crypto. library name / version: Crypto Library v1.0.0 & v2.0.0 (for C58)

Other libraries name / version: Services Software v4.13.3 (C25), v4.13.7 (C48) & v4.14.0 (C58)

Bootloader name / version: BootOS v4.2.0 PL3 v4 (C25) & PL5 V16 (C48 & C58)

Security Laboratory: SGS Brightsight

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:

- SN100_SE, Information on Guidance and Operation, User manual, Rev. 1.4, 13 Aug 2019
- SN100x Crypto Library Information on Guidance and Operation - User Guidance Manual, Rev. 1.10, 30 Jul 2019 (for C25 and C48)
- SN100x Crypto Library Information on Guidance and Operation - User Guidance Manual, Rev. 2.4, 30 Jul 2019 (for C58)
- SN100 Services User Manual, API and Operational Guidance, Rev. 4.12, 31 Aug 2018 (for C25 and C48)
- SN100 Services User Manual, API and Operational Guidance, Rev. 4.13, 5 Apr 2019 (for C58)
- SN100 Services Addendum, Additional API and Operational Guidance, Rev. 0.4, 28 Aug 2018 (for C25 and C48)
- SN100 Services Addendum, Additional API and Operational Guidance, Rev. 0.5, 5 Apr 2019 (for C58)
- SN100x_SE High-performance secure element subsystem, Objective data sheet, Rev. 1.0, 19 Oct 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.