

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

Certificate Number : ICCN0258

Date of issuance 22 Nov 2018

Expiry Date: 22 Nov 2024

Company: NXP Semiconductors Germany GmbH

Address: Beiersdorfstraße 12
Hamburg 22529 Germany

Master Component: N7121

Hardware Revision: B1

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): GlobalFoundries, Singapore (GF7) and Dresden (GF1)

Firmware name / version: Firmware v9.2.3, System Mode OS v13.2.3, Flashloader OS v1.2.5

Crypto. library name / version: v0.7.6

Other libraries name / version: Flashloader lib. v3.6.0, Comm. lib. v6.0.0, CRC lib. v1.1.8, Mem. lib. v1.2.3

Bootloader name / version: -

Security Laboratory: Brightsight (up to 2019), TÜVIT (since 2020)

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:

- NXP Secure Smart Card Controller N7121, Information on Guidance and Operation, v3.2, 28 May 2019
- N7121 Crypto Library, Information on Guidance and Operation, v3.4, 04 May 2022
- NXP Secure Smart Card Controller N7121, Overview, Product Data Sheet, v3.3, 15 Apr 2020
- NXP Secure Smart Card Controller N7121 Instruction Set Manual, v3.0, 23 Nov 2018
- NXP Secure Smart Card Controller N7121 Chip Health Mode, v3.1, 30 Jun 2020
- NXP Secure Smart Card Controller N7121 Peripheral Configuration and Use, v3.2, 18 Feb 2020
- NXP Secure Smart Card Controller N7121 Flashloader OS, v3.0, 1 Nov 2018
- NXP Secure Smart Card Controller N7121 MMU configuration & FW interface, v3.7, 10 Sep 2021
- NXP Secure Smart Card Controller N7121 Shared OS libraries, v3.2, 30 Oct 2019
- NXP Secure Smart Card Controller N7121 NXP System Mode OS, v3.6, 10 Sep 2021
- SmartMX3 family N7121 Wafer and delivery specification, v3.3, 27 Aug 2021
- N7121 Crypto Library, Symmetric Cipher Library, v1.4, 19 Sep 2018
- N7121 Crypto Library, SHA Library, v1.1, 20 Mar 2018 / Hash Library, v1.2, 20 Mar 2018
- N7121 Crypto Library, RSA Library, v1.4, 28 Mar 2019 / RSA Key Generation Library, v1.3, 11 Oct 2018
- N7121 Crypto Library, KeyStoreMgr Library, v1.1, 19 Sep 2018
- N7121 Crypto Library, ECC over GF(p) Library, v2.3, 04 May 2022
- N7121 Crypto Library, RNG Library, v1.2, 9 Nov 2018 / Utils Library, v1.1, 2 Feb 2018
- N7121 Crypto Library, UtilsAsym Library, v1.3, 13 Apr 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.