

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

Certificate Number : ICCN0288

Date of issuance 07 Apr 2022

Expiry Date: 07 Apr 2025

Company: NXP Semiconductors Germany GmbH

Address: Beiersdorfstraße 12
Hamburg 22529 Germany

Master Component: N7122

Hardware Revision: A1

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): GlobalFoundries Singapore (Fab 7) / GlobalFoundries Dresden (Fab 1)

Firmware name / version: IC Dedicated & Support Software v11.6.5; IC Dedicated Firmware Extension v07;
Mem Lib v1.2.3.1

Crypto. library name / version: Crypto Library v1.1.2; CRC Lib v1.1.8

Other libraries name / version: FL OS v1.3.3 (COS); Comm Lib v7.10.3 (COS) v7.10.2 (NOS); FL Lib v3.10.0 (COS)

Bootloader name / version: Boot Software v11.6.5

Security Laboratory: TÜVIT

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

Authorized by: Alan Mushing, SEWG Chair
EMVCo, LLC

Date: 20 Mar 2024

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:

- N7122 - UM11590 - Information on Guidance and Operation of N7122, Rev. 1.3, 8 Feb 2022
- N7122 - Crypto Library, Information on Guidance and Operation, Rev. 1.5, 23 Nov 2023
- N7122 - Overview, Product Data Sheet, Rev. 0.1, 31 Mar 2021
- N7122 - Instruction Set Manual, Rev. 0.2, 29 Mar 2021
- N7122 - Chip Health Mode, Rev. 0.2, 29 Mar 2021
- N7122 - Peripheral Configuration and Use, Rev. 0.2, 12 Apr 2021
- N7122 - Flashloader OS, Rev. 0.4, 10 Feb 2022
- N7122 - MMU Configuration & NXP Firmware Interface Specification, Rev. 1.0, 16 Mar 2023
- N7122 - Shared OS Libraries, Rev. 0.4, 10 Feb 2022
- N7122 - Wafer and Delivery Specification, Rev. 1.2, 12 May 2023
- N7122 - Crypto Library, SymCfg User Manual, Rev. 1.1, 24 Aug 2020
- N7122 - Crypto Library, SHA User Manual, Rev. 1.1, 14 Aug 2020 / Hash User Manual, Rev. 1.1., 24 Aug 2020
- N7122 - Crypto Library, Rsa User Manual, Rev. 1.2, 24 Aug 2020
- N7122 - Crypto Library, RSA Key Generation User Manual, Rev. 1.2, 24 Aug 2020
- N7122 - Crypto Library, KeyStoreMgr User Manual, Rev. 1.1., 24 Aug 2020
- N7122 - Crypto Library, ECC over GF(p) User Manual, Rev. 1.2, 24 Aug 2020
- N7122 - Crypto Library, RNG User Manual, Rev. 1.1, 24 Aug 2020 / Utils User Manual, Rev. 1.1, 24 Aug 2020
- N7122 - Crypto Library, UtilsAsym User Manual, Rev. 1.1, 24 Aug 2020

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.