EMVCo — IC Security Evaluation Certificate

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

Certificate Number : ICCN0281

Date of issuance 15 Jul 2021	**Expiry Date:** 15 Jul 2026

Company: NXP Semiconductors Germany GmbH

Address: Beiersdorfstraße 12

Hamburg   22529   Germany

Master Component: SN220 Series

Hardware Revision: B0.1 C13 / C37

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): GLOBALFOUNDRIES, Fab1 Dresden, Germany; SMIC Beijing, PR China

Firmware name / version: Factory OS v9.0.4 (C13) / 10.0.2 (C37), Flash Driver Software v9.0.2 (C13) / 10.0.0 (C37)

Crypto. library name / version: Crypto Library v2.2.0 (C13) / v2.3.1 (C37)

Other libraries name / version: Services Software v9.17.4 (C13) / v10.17.6 (C37)

Bootloader name / version: BootOS v9.0.3 & BootOS 9.0.3_PL1_v1 (C13) / Boot OS v10.0.2 & BootOS 10.0.2_PL1_v1 (C37)

Security Laboratory: Keysight Technologies Riscure

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 15 Sep 2025

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. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.

User Guidance Documents:

- C13 configuration:

o SN220_SE Information on Guidance and Operation, Rev. 1.0, 12 Jul 2021

o SN220x Crypto Library Information on Guidance and Operation, Rev. 1.1, 12 Jul 2021

o SN220 Services User Manual - API and Operational Guidance, Rev. 1.0, 01 Oct 2020

o SN220 Services Addendum - Additional API and Operational Guidance, Rev. 1.0, 01 Oct 2020

o SN220x_SE High-performance secure element subsystem, objective data sheet, Rev. 1.2, 12 Jul 2022

- C37 configuration:

o SN220_SE Information on Guidance and Operation, Rev. 1.0, 12 Jul 2021

o SN220x Crypto Library Information on Guidance and Operation, Rev. 1.3, 31 Aug 2022

o SN220 Services User Manual - API and Operational Guidance, Rev. 1.1, 05 May 2022

o SN220 Services Addendum - Additional API and Operational Guidance, Rev. 1.1, 05 May 2022

o SN220x_SE High-performance secure element subsystem, objective data sheet, Rev. 1.2, 12 Jul 2022

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.4, July 2024
- Security Guidelines for Smart Card Integrated Circuits, v2.2, December 2022