IC Security Evaluation Certificate

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

Certificate Number : ICCN0289

Date of issuance 22 Oct 2021 **Expiry Date: 22 Oct 2027**

Company: STMicroelectronics (Rousset) SAS

Address: ZI de Rousset
Avenue Coq
Rousset Cedex 01 13106 France

Master Component: ST31N600

Hardware Revision: rev. B & C

Child Lot 1: -
Child Lot 2: -
Child Lot 3: -
Child Lot 4: -
Child Lot 5: -

Manufacturing site(s): Samsung Giheung (South Korea)

Firmware name / version: ST31N v3.1.2 (for Rev. B) & v3.1.3 (for Rev. C)

Crypto. library name / version: NesLib 6.7.4

Other libraries name / version: -

Bootloader name / version: included in Firmware

Security Laboratory: Thales

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

Authorized by: Matheus Oliveira
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 23 Oct 2026

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:

- ST31N Platform - ST31N600 ST31N500 ST31N400 Datasheet - Secure dual interface microcontroller with enhanced security and up to 608 Kbytes of Flash memory - DS_ST31N, v6.0

- ST31N platform firmware V3 - User manual - UM_ST31N_FWv3, v10.0

- Security guidance of the ST31N secure MCU platform – Application Note – AN_SECU_ST31N, v1.0

- NesLib cryptographic library 6.7 user manual: UM_NesLib_6.7, v4

- NesLib 6.7 security recommendation for ST31N platform: AN_SECU_ST31N_NESLIB_6.7, v7

- Release note NesLib 6.7.4 for ST31N: RN_ST31N_NESLIB_6.7.4, v3

- ST31N platform random number generation - User manual - UM_ST31N_TRNG, v4.0

- NesLib - Limitation of NesLib_AES_CMAC - Technical note, v1.0

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.5, January 2026
- 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. The Product Provider, when distributing this EMVCo Compliance Certificate, shall deliver it in its entirety.