IC Security Evaluation Certificate

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

Certificate Number : ICCN0329

Date of issuance 19 Jun 2026 **Expiry Date: 19 Jun 2027**

Company: STMicroelectronics (Rousset) SAS

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

Master Component: ST31S600

Hardware Revision: Rev. A

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

Manufacturing site(s): STMicroelectronics Crolles (France)

Firmware name / version: ST31S_FWv4 v4.0.3

Crypto. library name / version: NesLib v6.12.1

Other libraries name / version: Optional RngLib v3.0.0

Bootloader name / version: included in Firmware

Security Laboratory: Thales SIX

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 12 Aug 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:

- Secure dual interface microcontroller with enhanced security and up to 608 Kbytes of flash memory - ST31S platform (ST31S600, ST31S500, ST31S400) – Datasheet, DS_ST31S, v1

- ST31S platform firmware V4 – User manual, UM_ST31S_FWv4, v1

- Security guidance of the ST31S600 secure MCU subsystem - Application note, AN_SECU_ST31S, v1

- Random number generation for ST31S - User manual, UM_ST31S_TRNG, v1

- Random number generator library RngLib 3.0.x - User manual, UM_RngLib_3.0, v1

- RngLib 3.0.0 for ST31S platform - Release note, RN_ST31S_RngLib_3.0.0, v1

- NesLib cryptographic library – NesLib 6.12 User manual, UM_NesLib_6.12, v1

- ST31S NesLib 6.12 security recommendations - Application note, AN_SECU_ST31S_NESLIB_6.12, v1

- NesLib 6.12.1 for ST31S platforms - Release note, RN_ST31S_NESLIB_6.12.1, v1

Certification Reference Documents:

- EMVCo Security Evaluation Process, v5.5, January 2026
- Security Guidelines for Smart Card Integrated Circuits, v2.2, December 2022