

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

Certificate Number : ICCN0293

Date of issuance 06 Sep 2019

Expiry Date: 06 Sep 2024

Company: STMicroelectronics (Rousset) SAS

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

Master Component: ST31P450

Hardware Revision: Rev. C

Child Lot 1: ST31P320

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): ST Crolles (France) & Samsung Giheung (Korea)

Firmware name / version: FW 3.1.1 and 3.1.2

Crypto. library name / version: NesLib 6.7.4

Other libraries name / version: -

Bootloader name / version: See Firmware

Security Laboratory: Thales

Conditions of Certification: User 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:

- NesLib cryptographic library 6.7 user manual, UM_NesLib_6.7, v4
- NesLib 6.7 security recommendations for the ST31P platform secure microcontrollers - Application note, AN_SECU_ST31P_NESLIB_6.7, v3.0
- NesLib 6.7.4 for ST31P platforms - Release note, RN_ST31P_NESLIB_6.7.4, v2.0
- Secure dual interface MCU with enhanced security and up to 450 Kbytes of Flash memory - ST31P450 Preliminary datasheet, DS_ST31P, v5.0
- ST31P450 firmware V3 - User manual, UM_ST31P450_FWv3, v8.0
- ST31P secure MCU platform Security guidance - Application note, AN_SECU_ST31P, v2.0
- NesLib - Limitation of NesLib AES CMAC - Release note, RN_ST31P_NESLIB_6.7.4, v1.0

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.