

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

Certificate Number : ICCN0287

Date of issuance 20 Sep 2021

Expiry Date: 20 Sep 2024

Company: STMicroelectronics (Rousset) SAS

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

Master Component: ST33K1M5C & ST33K1M5T

Hardware Revision: rev. B, C & D

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): STMicro CROLLES (France) for Rev. B/C/D / Samsung Giheung (Korea) for Rev. D

Firmware name / version: Firmware v3.1.3 for HW rev B
Firmware v3.1.4 for HW rev C

Crypto. library name / version: NesLib 6.7.4

Other libraries name / version: -

Bootloader name / version: included in Firmware

Security Laboratory: SGS Brightsight

Conditions of Certification: 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:

- Security Guidance of the ST33K Secure MCU platform – Application note, AN_SECU_ST33K v1, September 2021
- ST33K1M5C Datasheet, DS_ST33K1M5C v6, May 2023
- ST33K1M5T Datasheet, DS_ST33K1M5T v5, May 2023
- ST33K platform firmware V3 – User manual, UM_ST33K_FW v7, March 2023
- NesLib cryptographic library 6.7 user manual, UM_NesLib_6.7, rev. 4.0, 2 Dec 2021
- NesLib 6.7 security recommendation for ST33K platform, AN_SECU_ST33K_NESLIB_6.7 rev. 4.0, 22 Feb 2022
- Release Note NesLib 6.7.4 for ST33K platforms, RN_ST33K_NESLIB_6.7.4, rev. 2.0, February 2023
- Random number generation V1.4 User manual, v7, April 2023
- Limitation of NesLib_AES_CMAC , Technical Note V1, February 2023

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.