



EMVCo Product Approval (IC)

Please accept this document as confirmation of the EMVCo Security Evaluation process

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.

ICCN: ICCN0229

Date ICCN issued: 08 Sep 2016

ICCN Expiry Date: 08 Sep 2022

Company: STMicroelectronics (Rousset) SAS

Master Component: ST33J2M0

Hardware Revision: Rev. H & I

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): STMicroelectronics Crolles, France

Firmware name / version: Firmware Rev. 3.2.5 (Rev. H) and Rev 3.3.0 (Rev. H&I)

Crypto. library name / version: Optional crypto lib NesLib 6.3.4

Other libraries name / version: Optional MIFARE4Mobile v2.2.9 or v2.2.10

Bootloader name / version: OST rev 05.04

Security Laboratory: Serma

User Guidance: - ST33J2M0 datasheet: Secure MCU with 32-bit SecurCore SC300 CPU with SWP, ISO, SPI, I2C & Flash, DS_ST33J2M0, v9

- ST33J2M0 firmware V3 User manual, UM_ST33J2M0_FWv3, v20

- ST33J Secure MCU platforms Security Guidance, AN_SECU_ST33J, v10

- ST33J Secure MCU platform NesLib 6.3 security recommendations, AN_SECU_ST33J_NESLIB_6.3, v4

- Neslib cryptographic library Neslib 6.3 User Manual, UM_Neslib_6.3, v4

- MIFARE4Mobile library 2.2 for the ST33J platform – User manual, UM_33J_MIFARE4MOBILE-2.2, v4

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

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 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.