

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

**Certificate Number : ICCN0282**

**Date of issuance 01 Sep 2021**

**Expiry Date: 01 Sep 2024**

**Company: Samsung Electronics Co., Ltd.**

Address: 1-1, Samsungjeonja-ro  
Hwaseong-si  
Gyeonggi-Do 445-330 Republic of Korea

**Master Component: S3B512C/SC3512C**

**Hardware Revision: rev. 1**

Child Lot 1: -

Child Lot 2: -

Child Lot 3: -

Child Lot 4: -

Child Lot 5: -

Manufacturing site(s): Samsung Giheung (S1), Yongin-City, South Korea

Firmware name / version: Test ROM Code v1.0

Crypto. library name / version: ATP1 secure RSA/ECC/SHA library v1.00 & v1.02

Other libraries name / version: DTRNG FRO M library v1.3 & v1.7, Fingerprint library v0.4, v1.0 & v2.0

Bootloader name / version: Secure Boot loader Code v0.1

Security Laboratory: Leti

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:

- DTRNG FRO M Application Note, v1.3, 10 Aug 2021 (for Lib v1.7)
- DTRNG FRO M Application Note, v2.1, 10 Jul 2023 (for Lib v1.3)
- ATP1 RSA/ECC/SHA Library v1.00 API Manual, v1.033, 7 Jul 2023
- ATP1 RSA/ECC/SHA Library v1.02 API Manual, v1.11, 7 Jul 2023
- Hardware User's manual, v0.03, June 2021
- Security Application Note, v0.8, 8 Jun 2023
- Chip Delivery Specification, v0.3, February 2023
- Boot Loader Specification, v0.2, 21 Jun 2021
- SC000 Reference Manual, v0.0, 13 Oct 2016
- Fingerprint library implementation guide, v0.03, August 2021
- Fingerprint library implementation guide, v0.05, April 2022
- Fingerprint library implementation guide, v0.06, January 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.