IC Security Evaluation Certificate

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

Certificate Number : ICCN0303

Date of issuance 11 Aug 2023 **Expiry Date: 11 Aug 2027**

Company: Samsung Electronics Co., Ltd.

Address: 1-1, Samsungjeonja-ro
Hwaseong-si
Gyeonggi-Do 18448 Republic of Korea

Master Component: S3D384E

Hardware Revision: Rev. 2

Child Lot 1: S3D352E
Child Lot 2: S3D300E
Child Lot 3: S3D264E
Child Lot 4: S3D232E
Child Lot 5: S3K384E

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

Firmware name / version: Test ROM Code v1.0

Crypto. library name / version: ATP1 secure RSA/ECC/SHA Library v2.00, v2.01, v2.04 & v2.10

Other libraries name / version: DTRNG FRO M library v1.3, v1.4 & v1.5

Bootloader name / version: Secure Boot loader & System API Code v0.2

Security Laboratory: Leti

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

Authorized by: Alan Mushing
Security Evaluation Working Group Chair
EMVCo, LLC
Date: 05 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:

- DTRNG FRO M Library v1.3 Application Note, v1.21, 16 Jun 2026
- DTRNG FRO M Library v1.4 Application Note, v1.32, 16 Jun 2026
- DTRNG FRO M Library v1.5 Application Note, v1.01, 16 Jun 2026
- ATP1 RSA/ECC/SHA Library v2.00 API Manual, v2.032, 19 Jun 2026
- ATP1 RSA/ECC/SHA Library v2.01 API Manual, v2.014, 19 Jun 2026
- ATP1 RSA/ECC/SHA Library v2.04 API Manual, v2.071, 19 Jun 2026
- ATP1 RSA/ECC/SHA Library v2.10 API Manual, v2.14, 21 Jul 2026
- Hardware User's manual, v0.6, 15 Jul 2026
- Security Application Note, v0.6, 29 Jul 2025
- Chip Delivery Specification, v0.3, May 2023
- Boot Loader Specification, v0.3, 29 Jul 2025
- SC000 Reference Manual, v0.0, 13 Oct 2016

Certification Reference Documents:

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