



## 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:** ICCN0224

**Date ICCN issued:** 07 Apr 2016

**ICCN Expiry Date:** 07 Apr 2022

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

**Master Component:** S3FV9RR

**Hardware Revision:** Rev. 0 & 1

Child Lot 1: S3FV9RR

Child Lot 2: S3FV9RQ

Child Lot 3: S3FV9RP

Child Lot 4: S3FV9RK

Child Lot 5: -

**Manufacturing site(s):** Samsung Giheung plant, Line S1, South Korea

**Firmware name / version:** Test ROM Code v1.0 (out of the TOE)

**Crypto. library name / version:** AE1 Secure RSA/SHA Lib v2.02, RSA/SHA/ECC Lib v2.03/v3.00/v3.001

**Other libraries name / version:** DTRNG FRO M library v2.0, v2.1, v3.2, v3.61, v4.0 & vC4.0

**Bootloader name / version:** Secure Boot loader & System API Code, v1.4

**Security Laboratory:** Leti

**User Guidance:**

- DTRNG FRO M Application Note, v1.13, 9 Mar 2021 (DTRNG FRO M Lib. v2.0)
- DTRNG FRO M Application Note, v1.3, 9 Mar 2021 (DTRNG FRO M Lib. v2.1)
- DTRNG FRO M Application Note, v2.1, 9 Mar 2021 (DTRNG FRO M Lib. v3.2 & v3.61)
- DTRNG FRO M Application Note, v3.0, 9 Mar 2021 (DTRNG FRO M Lib. v4.0 & vC4.0)
- AE1 RSA Library API Manual for AE1 Secure RSA/SHA, v0.11, 29 Jun 2020 (RSA/SHA Lib. v2.02)
- Tornado-E RSA/ECC Library API Manual, v1.02, 01 Jul 2020 (RSA/ECC/SHA Lib. v2.03)
- Tornado-E RSA/ECC Library API Manual, v1.04, 09 Nov 2020 (RSA/ECC/SHA Lib. v3.00 & v3.001)
- S3FV9RR User's manual, 2.01, 10 Apr 2017
- Security Application Note for S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK/S3NSN4V, v1.0, 21 Oct 2020
- S3FV9RR Chip Delivery Specification, v1.0, Feb 2016
- Bootloader User's Manual for S3FV9RR, v1.15, 23 Mar 2016
- S3FV9RR System API Application Note, v1.2, 12 Feb 2016
- SC300 Reference Manual, v0.0, 12 May 2014

**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.