Certification Report

STRONGV3P00_In04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0

Sponsor and developer: *SAMSUNG Electronics Co. Ltd.*
Security & Power product development team DSR,
Samsungjeonja-ro 1-1
Hwaseong-si, Gyeonggi-Do
South Korea

Evaluation facility: *SGS Brightsight B.V.*
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0354165-CR**
Report version:	**1**
Project number:	**0354165**
Author(s):	**Jordi Mujal**
Date:	**06 December 2023**
Number of pages:	**12**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0. The developer of the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0 is SAMSUNG Electronics Co. Ltd. located in Hwaseong-si, South Korea and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Secure Sub-System (3S) with defined physical boundaries, implemented in a SoC that is designed and packaged specifically for mobile applications. The TOE is a complete solution, implementing a secure integrated circuit (secure IC) as defined in the Protection Profile *[PP]*, and designed and packaged specifically for mobile applications.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 06 December 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0 from SAMSUNG Electronics Co. Ltd. located in Hwaseong-si, South Korea.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	STRONGV3P00_ln04lpe Secure Sub-System on the S5E9935 SoC	0.0
	SoC S5E9935, embedding the TOE	0.0
	SoC Package	1462-FOWLP-14.0x15.3
Software	Secure Boot loader	1.2
	AH3 Secure RSA/ECC/SHA Library (optional)	1.06
	DTRNG library	1.1
	DRBG library	1.04
	SMK library	0.1

To ensure secure usage a set of guidance documents is provided, together with the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.2.4.

2.2 *Security Policy*

- Security sensors or detectors including High and Low Temperature detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detector and Laser detectors
- Active Shields against physical intrusive attacks
- Life time detector for protection of detector signals
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks, such as Random Branch Insertion and ROM and RAM encryption mechanisms
- Dedicated hardware mechanisms against Fault Injection attacks, such as redundancy
- Secure TDES and AES Symmetric Cryptography support
- TORNADOTM-H cryptographic coprocessor
- Key Manager: KDF (block KEYMGR in the Security Controller)
- ECC/ Parity/ CRC-32 calculators
- One Hardware Digital True Random Number Generator (DTRNG) that meets PTG.2 class of BSI-AIS-20/31 (German scheme)

- SHA-2/ SHA-3/ HMAC hardware engines
- Direct Memory Access (SC_DMA)
- Secure AXI Bridge
- Memory Management Unit (MMU)
- The IC Dedicated Software includes:
    - The modular arithmetic AH3 Secure RSA/ECC/SHA library for the support of RSA and ECC cryptographic operations (optional)
    - DTRNG library built around a hardware DTRNG, together with corresponding DTRNG application notes. This library meets PTG.2 class of BSI-AIS-20/31 (German scheme)
    - DRBG library is for deterministic random bit generator as specified in [NIST SP 800-90A] using a seed from the DTRNG. This library meets DRG.3 class of BSI-AIS-20/31 (German scheme)
    - Secure Boot Loader is a loader for copying the firmware from an external FLASH storage into the internal SRAM
    - SMK Library for the OS developer. Supports the encryption keys that are used to encrypt application’s encryption keys.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.3 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The following functionality is also present without specific security claims:

• SHA2 in the CRYPTO block

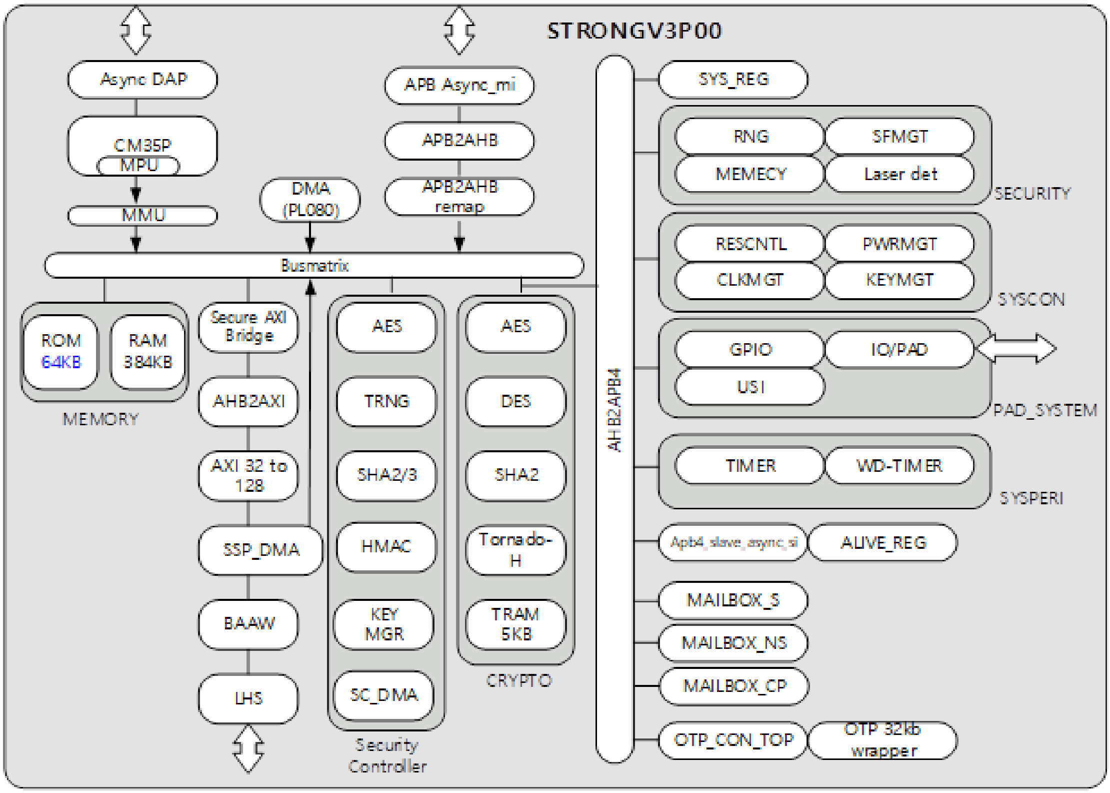
• DMA (PL080)

• Key manager KEYMGT in SYSCON

• Code execution through the Secure AXI bridge (eXecute In Place, XIP)

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
STRONGV3P00_ln04lpe HW DTRNG FRO M and DTRNG FRO M Library Application Note	1.3
STRONGV3P00_ln04lpe DRBG library Application Note	1.2
AH3 Secure RSA /ECC/SHA Library API Manual	1.06
STRONGV3P00_ln04lpe SMK Library Application Note	0.1
STRONGV3P00 of S5E9935, 32-bit RISC Microcontroller for Secure Element Platform	0.7
Security Application Note for STRONG_V3P00_ln04lpe	1.5
S5E9935 Chip Delivery Specification	0.3
STRONGV3P00_ln04lpe Secure Bootloader Manual for S5E9935	0.2
CORTEX-M35P Reference manual	0.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis was performed considering the attack methods in *[JIL-AM]* and *[JIL-AAPS]*.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 40 weeks. During that test campaign, 30% of the total time was spent on Perturbation attacks, 65% on side-channel testing, and 2% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of multiple site certificates and Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, Revision 0.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.
Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target of STRONGV3P00_ln04lpe of S5E9935 with Specific IC Dedicated Software, version 1.6, 05 December 2023 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DDR	Double Date Rate
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NVM	Non-Volatile Memory
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SOC	System on Chip
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report “STRONGV3P00_In04lpe of S5E9935 with Specific IC Dedicated Software” – EAL5+, 22-RPT-202, version 11.0, 06 December 2023

[ETRfC] Evaluation Technical Report for Composition “STRONGV3P00_In04lpe of S5E9935 with Specific IC Dedicated Software” – EAL5+, 22-RPT-203, version 7.0, 06 December 2023

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[PP] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ST] Security Target of STRONGV3P00_In04lpe of S5E9935 with Specific IC Dedicated Software, version 1.6, 05 December 2023

[ST-lite] ST-Lite of STRONGV3P00_In04lpe of S5E9935 with Specific IC Dedicated Software, version 0.6, 05 December 2023

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)