TRUST AND VERIFY

Version 2023-11

# Certification Report

# STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1

| | |
|---|---|
| Sponsor and developer: | ***SAMSUNG Electronics Co. Ltd.***<br>**Innovative AP Development Team(S.LSI)**<br>**DSR, Samsungjeonja-ro 1-1,**<br>**Hwaseong-si, Gyeonggi-Do**<br>**South Korea** |
| Evaluation facility: | ***TÜV Informationstechnik GmbH***<br>**Am TÜV 1**<br>**45307 Essen**<br>**Germany** |
| Report number: | **NSCIB-CC-2300043-01-CR** |
| Report version: | **1** |
| Project number: | NSCIB-**2300043-01** |
| Author(s): | **Jordi Mujal** |
| Date: | **11 December 2024** |
| Number of pages: | **13** |
| Number of appendices: | **0** |

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

# 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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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

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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1. The developer of the STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1 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), implemented in a SoC as defined in the Protection Profile *[PP]*. The TOE implements a processing unit, security components as well as volatile and non-volatile memories (hardware). The TOE also comprises dedicated firmware for loading the composite software from TOE-external memories and software components for cryptographic purposes and random number generation.

The evaluation and certification of this TOE was performed to support reuse of the 3S into the final SoC that is targeting conformance to *[PP]* to fulfil the composition requirements *[COMP]*. **The TOE has dependencies to be considered when integrated into the final SoC that need to be verified before the TOE is fully integrated into the final SoC.** In accordance with [PP] integration guidance *[AGD_IIG]* is provided for the TOE. **The users of the TOE, developers of the SoC, must strictly follow the guidance and must successfully pass an (integration) certification of this 3S TOE integrated in the final SoC in order for the 3S SoC product to claim EAL5+ and/or AVA_VAN.5 resistance and before starting a subsequent composite evaluation with its Embedded Software (ES).**

The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 11 December 2024 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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1, 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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1 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), AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_FLR.2 (Flaw Reporting Procedures).

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).

TrustCB 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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1 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 | STRONGV3P10_In04lpe TRONGV3P10 | 2.0 |
| | Secure JTAG Controller of SoC | 2.0/2.1 |
| Software | Secure Boot loader | 1.2 |
| | AH3 Secure RSA/ECC/SHA Library (optional) | 1.03 |
| | DTRNG Library | 1.2 |

To ensure secure usage a set of guidance documents is provided, together with the STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1. For details, see section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-Lite]*, Chapter 1.3.5.

## *2.2 Security Policy*

The TOE encompasses the following features:

- Security sensors or detectors including High and Low Temperature detectors, High and Low Supply Voltage detectors and Supply Voltage Glitch detector
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- 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
- Memory encryption and bus scrambling
- Integrity checks on memories and buses
- Secure TDES and AES Symmetric Cryptography support
- TORNADOTM-H cryptographic coprocessor
- Key Manager: KDF
- ECC/ Parity/ CRC-32 calculators
- One True Random Number Generator (TRNG HS_MRO9) that meets PTG.2 class of BSI-AIS-20/31
- SHA-2/ SHA-3/ HMAC hardware engines
- SHA3 / SHAKE

- Secure AXI Bridge
- Memory Management Unit (MMU)
- Secure JTAG Controller
- The IC Dedicated Software includes:
    - AH3 Secure RSA/ECC/SHA library for the support of RSA, ECC and SHA cryptographic operations (optional)
    - DTRNG library built around a TRNG hardware block
    - Secure Boot Loader is a loader for copying the firmware from an external FLASH storage into the internal SRAM

## *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 4.2 of the *[ST-Lite]*.

### 2.3.2 Clarification of scope

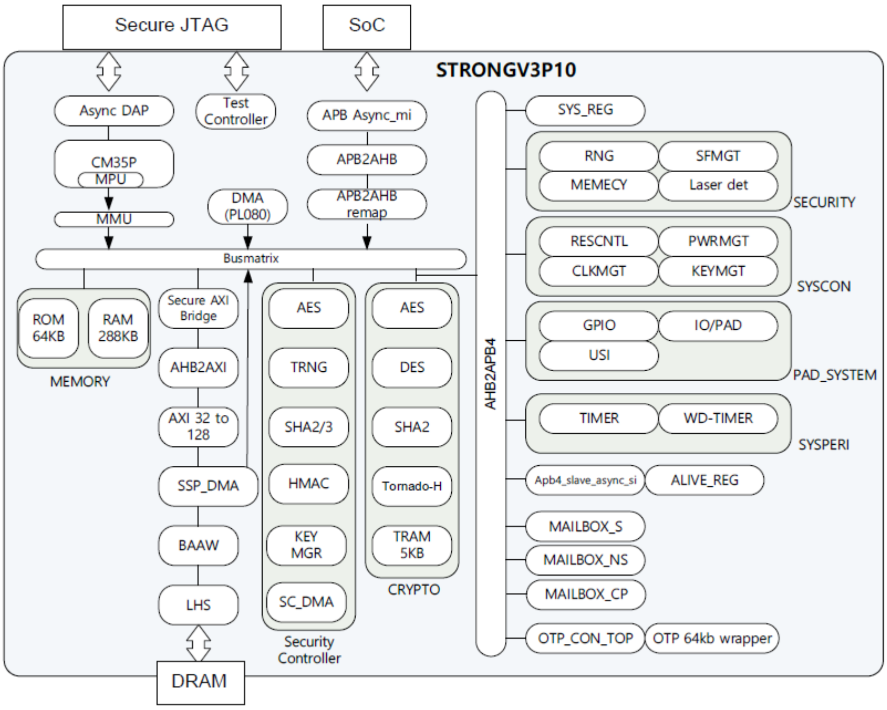
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

**The TOE has dependencies to be considered when integrated into the final SoC that need to be verified before the TOE is fully integrated into the final SoC.** The evaluation and certification of this TOE was performed to support reuse of the 3S into the final SoC that is targeting conformance to *[PP]* to fulfil the composition requirements *[COMP]*. The integration of the TOE into the specific final SoC is out of the scope for this evaluation.

During integration of the 3S into the final SoC, specific evaluation activities must be performed. The *[ETRfI]* and the integration guidance *[AGD_IIG]*) were generated to support this process.

## *2.4 Architectural Information*

A simplified TOE architecture, originating from the Security Target *[ST-Lite]* 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 |
|---|---|
| KITT2 HW DTRNG FRO M and DTRNG FRO M Library Application Note | 1.2 |
| PKA Library API Manual (AH0 Secure RSA/ECC/SHA Library API Manual) | 1.05 |
| STRONGV3P10 of S5AV920 32-bit RISC Microcontroller for Secure Element Platform User’s Manual | 0.4 |
| Security Application Note For STRONGV3P10 for S5AV920 | 0.8 |
| S5AV920 Chip Delivery Specification | 0.0 |
| STRONG Secure Bootloader Manual for S5AV920 | 1.03 |
| CORTEX-M35P Reference manual | 0.0 |
| Integration Guide | 0.6 |

## 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

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created during vulnerability analysis the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE’s operational environment. While doing this, also the aspects of the security architecture were considered for penetration testing.

Source code reviews of the provided implementation representation accompanied the development of test cases and were used to find input for testing. The code inspection also supported the testing activities because they enabled the evaluator to verify implementation aspects that could hardly be covered by test cases. For penetration testing the evaluator took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities.

The total test effort expended by the evaluator was 132 person days or 18.86 weeks. During that test campaign, 2% of the total time was spent on physical attacks, 5% overcoming sensors and filters, 18% perturbation attacks, 26% retrieving keys with FA, 37% side-channel attacks, 5% exploitation of test features, 7% attacks on RNG.

### 2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was performed on a test vehicle that was consistent with the TOE components 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 SoC integration) evaluations of the TOE integrated in the final SoC environment, please consult the *[ETRfI]* for details.

For embedded SW 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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1.

## 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 integration evaluations to an SoC a derived document [ETRfI] was provided and approved. To support future 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 the integrated 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 STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with specific IC Dedicated Software, version 2.0 and 2.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.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]*.

## 2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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.

The evaluation and certification of this TOE was performed to support reuse of the 3S into the final SoC that is targeting conformance to *[PP]* to fulfil the composition requirements *[COMP]*. **The TOE has dependencies to be considered when integrated into the final SoC that need to be verified before the TOE is fully integrated into the final SoC.** In accordance with [PP] integration guidance *[AGD_IIG]* is provided for the TOE. **The users of the TOE, developers of the SoC, must strictly follow the guidance and must successfully pass an (integration) certification of this 3S TOE integrated in the final SoC in order for the 3S SoC product to claim EAL5+ and/or AVA_VAN.5 resistance and before starting a subsequent composite evaluation with its Embedded Software (ES).**

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 Taurus1, STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with Specific IC Dedicated Software, Version 2.0/2.1, ST (Security Target), version 0.10, 07 November 2024 *[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.

[AGD_IIG] Integration Guide, version 0.6, 07 November 2024.

[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 SUMMARY (ETR SUMMARY), 8120782768 / NSCIB-CC-2300043-01, version 5, 09 December 2024

[ETRfC] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), 8120782768 / NSCIB-CC-2300043-01, version 4, 11 November 2024

[ETRfI] EVALUATION TECHNICAL REPORT FOR INTERGATION (ETR INT), 8120782768 / NSCIB-CC-2300043-01, version 2, 11 November 2024

[JIL-VA-SoC] Guidance for Vulnerability Analysis and Penetration Testing of a Secure Sub-System within a System-on-Chip, Version 3.0, March 2023 (sensitive with controlled distribution).

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024

[JIL-AMS] Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[PP] Secure Sub-System in System-on-Chip (3S in SoC), Version 1.5, 28 February 2022, registered under the reference BSI-CC-PP-0117

[ST] Taurus1, STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with Specific IC Dedicated Software, Version 2.0/2.1, ST (Security Target), version 0.10, 07 November 2024

[ST-lite] Taurus1, STRONGV3P10_In04lpe of S5AV920/S5AV820/S5AV720 with Specific IC Dedicated Software, Version 2.0/2.1, ST (Security Target Lite), version 0.1, 07 November 2024

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

(This is the end of this report.)