Reference: 2021-23-INF-4038- v1
Target: Limitada al expediente
Date: 11.04.2023

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2021-23**
TOE	**Samsung SP of S3B512C revision 3**
Applicant	**124-81-00998 - SAMSUNG Electronics Co. Ltd**

References

[EXT-6767] Certification Request

[EXT-8173] Evaluation Technical Report

Certification report of the product Samsung SP of S3B512C revision 3, as requested in [EXT-6767] dated 15/05/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6767] received on 15/12/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Samsung SP of S3B512C revision 3.

The TOE is the SP (Secure Processor) of the Biometric Smart Card with security functionalities are finger image capture, feature extraction, and secure transmission of fingerprint features to the Secure Element of the Biometric Smart Card by AES encryption. All the matching and decision of fingerprint authentication mechanism is in SE of S3B512C which is not TOE.

Developer/manufacturer: SAMSUNG Electronics Co. Ltd

Sponsor: SAMSUNG Electronics Co. Ltd.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: No.

Evaluation Level: Common Criteria Version 3.1 Revision 5 - EAL2.

Evaluation end date: 23/02/2023.

Expiration Date[1]: 08/04/2028.

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the Common Criteria Version 3.1 Revision 5 and the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5.

Considering the obtained evidences during the instruction of the certification request of the product Samsung SP of S3B512C revision 3, a positive resolution is proposed.

TOE SUMMARY

The SP of S3B512C single-chip CMOS micro-controller is designed and packaged specifically for "Biometric Smart Card" applications.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

The Cortex-M33 CPU architecture of the SP of S3B512C microcontroller follows the Harvard style, that is, it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.

The main security features of the SP of S3B512C integrated circuit are:

- Secure fingerprint image capture and feature extraction provided by TOE SP firmware, integrity protected.
- Access control of Users to Flash memory positions where SP firmware is executed.
- TOE Unique Identification
- Countermeasures to avoid attackers reproduction of fingerprint data.
- An AES hardware block supporting AES encryption and decryption with 128-bit, 192-bit and 256-bit keys in ECB mode. The AES block supports encryption of fingerprint features to be sent to SE of S3B512C.

The TOE is dedicated to application as within the context of banking and finance applications for credit or debit cards electronic purse (stored value cards) and electronic commerce, where the biometric fingerprint identification is a cardholder’s authentication method, the TOE is intended to acquire the fingerprint image of the cardholder, process it and pass the fingerprint extracted features to the Secure Element.

Note SE (Secure Element) is not TOE.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1

	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the functional requirements declared in section 6 *"IT SECURITY REQUIREMENTS"* of the [ST] according to Common Criteria v3.1 R5 Part 2 extended.

IDENTIFICATION

Product: Samsung SP of S3B512C revision 3

Security Target: Security Target of Samsung SP of S3B512C Secure 32-Bit RISC Microcontroller for Biometric Smart Cards, version 0.8, 22/07/2022.

Protection Profile: No.

Evaluation Level: Common Criteria Version 3.1 Revision 5 - EAL2.

SECURITY POLICIES

The use of the product Samsung SP of S3B512C revision 3 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 "Organizational Security Policies".

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.4 "Assumptions".

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Samsung SP of S3B512C revision 3, although the agents implementing attacks have the attack potential according to a *Basic* attack potential according to EAL2 assurance components of Part 3 of Common Criteria Version 3.1 Revision 5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.2 "Threats".

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 "Security Objectives for the operational Environment".

ARCHITECTURE

LOGICAL ARCHITECTURE

The main security features of the SP of S3B512C integrated circuit are:

- Secure fingerprint image capture and feature extraction provided by TOE SP firmware, integrity protected.
- Access control of Users to Flash memory positions where SP firmware is executed.
- TOE Unique Identification
- Countermeasures to avoid attackers reproduction of fingerprint data.
- An AES hardware block supporting AES encryption and decryption with 128-bit, 192-bit and 256-bit keys in ECB mode. The AES block supports encryption of fingerprint features to be sent to SE of S3B512C.

PHYSICAL ARCHITECTURE

The main hardware blocks of the SP of S3B512C Integrated Circuit are described in Figure 1 below:

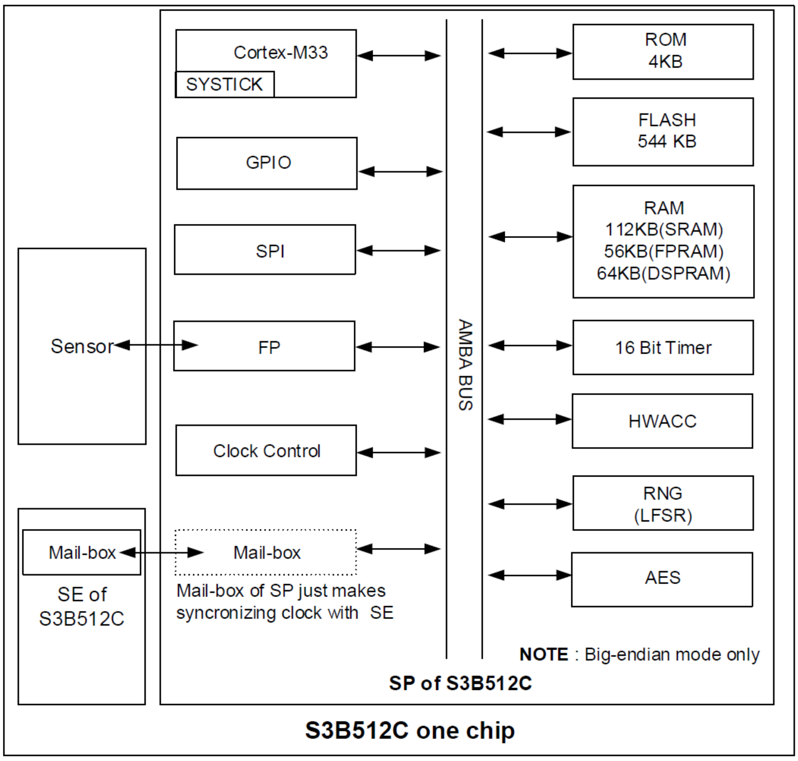

Figure 1 **SP of S3B512C Block Diagram**

NOTE: The Sensor chip is out of the TOE
NOTE: The SE of S3B512C chip is out of the TOE
NOTE: SE has all responsibilities of Mail-box communication between SE and SP

The TOE configuration is summarized below

Item type	Item	Version	Form of delivery
Hardware	SP Hardware	1.0	Wafer or Module
Software	SP Firmware	4.0[2]	Softcopy
Software	SP Data	3.0[3]	Softcopy
Document	S3B512C_SP_Firmware_AN	0.7	Softcopy

[2] Checksum of SP Firmware is part of Firmware identification. For given FW version, checksum is ‘06CE’.

[3] Checksum of SP Firmware data is part of Firmware identification. For given FW Data version, checksum is ‘2C49’.

Document	S3B512C_SP_Loader_TN	0.3	Softcopy
Document	S3B512C_SP_UM	0.4	Softcopy
Document	S3B512C_SP_DV	0.5	Softcopy

The delivery method is summarized below:

- Hardware - Secure carrier
- Documents - Documents are encrypted by PGP encryption and then delivered by email.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- S3B512C SP Firmware Application Note, version 0.7, 02/05/2022.
- S3B512C SP Loader Technical Note, version 0.3, 15/10/2021.
- S3B512C SP Hardware User's Manual, version 0.4, 15/10/2021.
- S3B512C SP Chip Delivery Specification, revision 0.5. October 2021.

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a test for each of the TSFI of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The TOE software and hardware requirements are summarized section PHYSICAL ARCHITECTURE of this certification report. Toe consumers shall be provided with all documentation identified in section DOCUMENTS.

TOE consumers can identify the TOE evaluated configuration following indications of section 6.2 of document S3B512C SP Chip Delivery Specification, revision 0.5. October 2021. TOE consumers shall check that

- Checksum of SP Firmware is ‘06CE’ and it is provided as part of the firmware identification mapped at flash memory Flag Area.
- Checksum of SP Firmware data is ‘2C49’ and it is provided as part of the firmware identification mapped at flash memory Flag Area.

EVALUATION RESULTS

The product Samsung SP of S3B512C revision 3 has been evaluated against the Security Target Security Target of Samsung SP of S3B512C Secure 32-Bit RISC Microcontroller for Biometric Smart Cards, version 0.8, 22/07/2022.

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the Common Criteria Version 3.1 Revision 5 and the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Samsung SP of S3B512C revision 3, a positive resolution is proposed.

The certifier recommends potential TOE consumers to observe Evaluation Team recommendations, strictly following the TOE guidance referenced in section DOCUMENTS and to analyse the assumptions defined in the security problem definition in section 3 of the [ST].

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SE	Secure Element
SP	Secure Processor
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] Security Target of Samsung SP of S3B512C Secure 32-Bit RISC Microcontroller for Biometric Smart Cards, version 0.8, 22/07/2022.

SECURITY TARGET / SECURITY TARGET LITE

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Security Target of Samsung SP of S3B512C Secure 32-Bit RISC Microcontroller for Biometric Smart Cards, version 0.8, 22/07/2022.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Security Target of Samsung SP of S3B512C 32-bit RISC Microcontroller for Biometric Smart Card, version 0.0, 07/03/2023.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.