TrustCB B.V.

TRUST AND VERIFY

Certification Report

STSafe S320 v2.2.1

Sponsor and developer:	***STMicroelectronics S.r.l*** **Zona Industriale Marcianise SUD** **81025 Marcianise (CE)** **Italy**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2200059-01-CR**
Report version:	**1**
Project number:	NSCIB-**2200059-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**10 November 2023**
Number of pages:	**11**
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 STSafe S320 v2.2.1. The developer of the STSafe S320 v2.2.1 is STMicroelectronics S.r.l located in Marcianise, Italy 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 an embedded secure element (eSE) with a Java Card System compliant with Java Card specifications version 3.0.5 with all the mandatory features, plus the following additions:

- support for the int type (including the intx package) and object deletion.
- support for Sensitive Results augmentation package

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 13 November 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 STSafe S320 v2.2.1, 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 STSafe S320 v2.2.1 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) 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).

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 STSafe S320 v2.2.1 from STMicroelectronics S.r.l located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST33K1M5C/ST33K1M5T (maskset K460)	C
Software	Firmware	3.1.4
	Operational OS	2.2.1
	Neslib	6.8.2
	StoreKeeper	4.1.2
	Weaver application	1.7
	Firmware upgrade OS	2.2.1

To ensure secure usage a set of guidance documents is provided, together with the STSafe S320 v2.2.1. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, section 1.4.5 or *[ST-lite]*, section 1.5.5.

2.2 Security Policy

The TOE is an embedded secure element (eSE) with a Java Card System compliant with Java Card specifications version 3.0.5 with all the mandatory features, plus the following additions:

- support for the int type (including the intx package) and object deletion.
- support for Sensitive Results augmentation package

The TOE provides two different applications for accessing two separate secure memories. The OEM Secure Storage is the default application; it is operational only on logical channel 0, while Weaver application is operational only on logical channel 1.

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 4.2.2 of the *[ST]* or section 4.1.2 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.

2.4 Architectural Information

The TOE is a composition of a Java Card OS with an open configuration with the ST33K1M5 IC platform (including Neslib and Storekeeper). It can also host and manage Java Card applets from different stakeholders (user, original equipment manufacturer (OEM), hardware integrator, service provider). The TOE also includes additional functionality to support the secure storage (OEM Secure Storage, Weaver and Storekeeper).

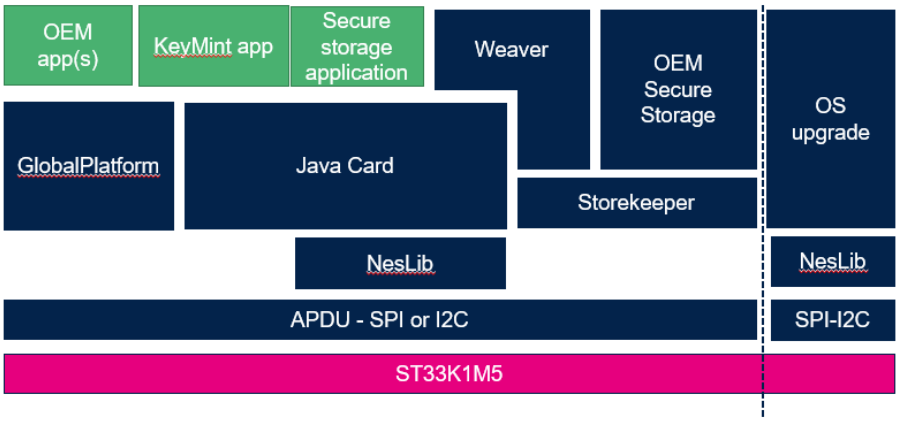

Figure 1 TOE components

Figure 1 shows the high level architecture of the TOE. In pink the underlying platform, in blue the software components and interfaces and in green the out of scope applications.

2.5 Documentation

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

Identifier	Version
STSAFES320 Preparative Procedure, dated September 15 2023	Revision G
STSAFES320 Operational Guidance, dated September 15 2023	Revision H

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 methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can 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 is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge

gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AM]. An important source for assurance in this step is the technical report [ETRfC-HW] of the underlying platform.

- All potential vulnerabilities are 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 are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 13 weeks. During that test campaign, 43% of the total time was spent on Perturbation attacks, 50% on side-channel testing, and 7% on logical tests.

2.6.3 Test configuration

The following version was used for testing:

- STSafe S320 v2.2.1

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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

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 software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of one site audit as reported in NSCIB-CC-0635023 and two 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 STSafe S320 v2.2.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and 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 STSafe S320 v2.2.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with**

ALC_DVS.2 and AVA_VAN.5. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

2.10 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: Weaver protocol.

3 Security Target

The STSafe S320, Version G, Dated 18 September 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:

IC	Integrated Circuit
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OEM	Original Equipment Manufacturer
PP	Protection Profile
SM	Secure Messaging
TOE	Target of Evaluation

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

[ETR] Evaluation Technical Report STSafe S320 – EAL5+, 23-RPT-344, Version 3.0, Dated 10 November 2023

[ETRfC] Evaluation Technical Report for Composition “STSafe S320” – EAL5+, 23-RPT-1082, Version 2.0, Dated 10 November 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 2.6, 02 August 2022

[PP] Java Card System - Open Configuration Protection Profile, April 2020, Version 3.1, registered under the reference BSI-CC-PP-0099-V2-2020

[ST] STSafe S320, Version G, Dated 18 September 2023

[ST-lite] STSafe S320 Security Target Lite, Version A, Dated 10 November 2023

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

(This is the end of this report.)