Certification Report

ST33K1M5A and ST33K1M5M B01

Sponsor and developer: ***STMicroelectronics***
190 avenue Celestin Coq, ZI de Rousset-Peynier
13106 Rousset
France

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

Report number: **NSCIB-CC-0428014-CR2**

Report version: **1**

Project number: **0428014_2**

Author(s): **Jordi Mujal**

Date: **17 August 2022**

Number of pages: **12**

Number of appendices: **0**

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.

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 ST33K1M5A and ST33K1M5M B01. The developer of the ST33K1M5A and ST33K1M5M B01 is STMicroelectronics located in Rousset, France 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 serial access microcontroller designed for secure mobile applications and compliant with *[PP_0084]*. It incorporates the most recent generation of Arm® processors for embedded secure systems.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 10 May 2022. The first re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 17 August 2022 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”:

- TOE configuration added a new IC version B. This version has only limited local (functional) changes at metal level in respect to the previously certified IC version A.

- TOE configuration added a new Firmware version 3.1.4 for IC version B. There are only functional changes between this version and the previously certified 3.1.3.

- Development environment has a change of one site address.

- User guidance updates.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ST33K1M5A and ST33K1M5M B01, 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 ST33K1M5A and ST33K1M5M B01 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation).

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 ST33K1M5A and ST33K1M5M B01 from STMicroelectronics located in Rousset, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST33K1M5A	IC Maskset name: K4A0, Master identification number:0x0260, IC version: A or B
	ST33K1M5M	IC Maskset name: K4A0, Master identification number:0x024B, IC version: A or B
Software	Firmware	3.1.3 (IC version A) or 3.1.4 (IC version B)

To ensure secure usage a set of guidance documents is provided, together with the ST33K1M5A and ST33K1M5M B01. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-lite]*, Chapter 1.7.

2.2 Security Policy

The TOE offers powerful features for high level security:

- Two instances of the Arm® Cortex-M35P CPU connected in lockstep mode
- Die integrity
- Monitoring of environmental parameters
- Highly efficient protection against faults
- AIS20/31 class PTG.2 compliant True Random Number Generator
- Memory Protection Unit and Library Protection Unit
- Hardware security enhanced AES accelerator
- Hardware security enhanced 3-key triple DES accelerator
- Secure Flash Loader
- NESCRYPT LLP coprocessor for public key cryptography algorithm (the TOE offers this functionality, there is no TOE security requirement that relies on this coprocessor however, in order to support a composite evaluation, the Vendor asked the Lab to carry out additional testing that is included in the *[ETRfc]*)

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]*.

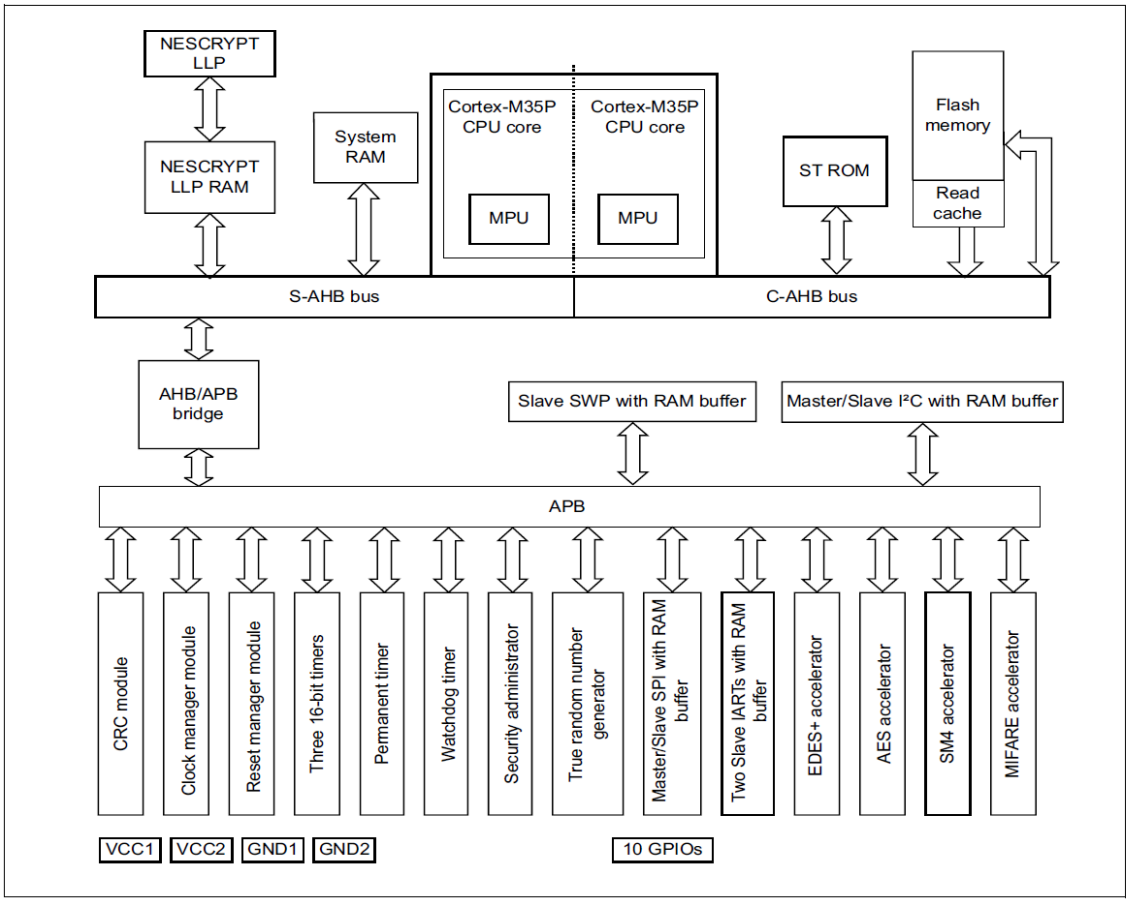
2.3.2 Clarification of scope

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

Please note that although the TOE contains HW accelerators for SM4, MIFARE, CRC and public key cryptography (NESCRYPT LLP), the functionality and security of these features have not explicitly been addressed in this evaluation. Therefore, if these features are required by the composite product the developer/evaluator should do their own security analysis and/or testing. In case of NESCRYPT LLP, in order to support this analysis, the Vendor asked the Lab to carry out additional testing that is included in the *[ETRfC]*.

2.4 Architectural Information

The TOE architecture is depicted below.



2.5 Documentation

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

Identifier	Version	Date
Automotive, high-speed secure MCU with 32-bit Arm Cortex-M35P CPU with SWP, ISO, SPI and I²C interfaces and high-density Flash memory - ST33K1M5A Datasheet, DS_ST33K1M5A	0.6	May 2022
High-speed secure MCU with 32-bit Arm® Cortex®-M35P CPU with SWP, ISO, SPI and I²C interfaces and high-density Flash memory - ST33K1M5M Datasheet, DS_ST33K1M5M	0.7	May 2022
Security Guidance of the ST33K Secure MCU platform - Application note, AN_SECU_ST33K	1.0	September 2021

ST33K platform firmware V3 - User manual, UM_ST33K_FWv3	6	April 2022
Arm® Cortex®-M35P Processor Technical Reference Manual, 100883_0101_00_en	r1p1	December 2018
Arm® Cortex®-M35P Armv8-M Architecture Supplement, PJDOC-466751330-1229	1.0	November 2018
Random number generation V1.4 - User manual, UM_ST_TRNG14	6	May 2022
ST33K Platform- TRNG Reference implementation: Compliance tests, AN_ST33K_TRNG	1	October 2020

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.

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.

During this re-evaluation, due to the limited and localized changes on the HW, the developer performed on Rev B a subset of the tests that were performed on Rev A. For the firmware, all the tests were repeated with a specific validation focus on the functionalities that were changed from the previous validated firmware version. Regarding the evaluator testing, a very specific subset of the independent testing was repeated.

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 used 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.

During the baseline evaluation, the total test effort expended by the evaluators was 21 weeks. During that test campaign, 7% of the total time was spent on Physical attacks, 46% Perturbation attacks, 40% on side-channel testing, and 7% on logical tests.

During this re-evaluation, the total test effort expended by the evaluators was 7 weeks. During that test campaign, 58% of the total time was spent on Perturbation attacks and 42% of the time was spent on side-channel testing.

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]*. Specifically, during this re-evaluation the hardware version B was used with firmware version 3.1.4 for independent evaluator testing and penetration testing. In addition, during baseline evaluation and this re-evaluation, some specific additional testing was based on a derivative hardware platform. The minor differences between the TOE and the derivative hardware platform were assessed by the Lab, and the Lab determined that the test results on the derivative hardware platform are equally applicable to the TOE.

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).

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

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used. The evaluator has renewed the vulnerability analysis and performed a penetration testing campaign.

There has been extensive reuse of the ALC aspects involved in the development and production of the TOE, by use of 26 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 ST33K1M5A and ST33K1M5M B01 together with the IC and firmware version identifiers.

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 ST33K1M5A and ST33K1M5M B01, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ALC_FLR.1**. 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_0084]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

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.

3 Security Target

The ST33K1M5A and ST33K1M5M B01 SECURITY TARGET, SMD_ST33K1M5AM_ST_21_001, Rev. B01.1, July 2022 *[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
DFA	Differential Fault Analysis
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NESCRYPT LLP	Next Step Cryptography Accelerator Lite Low Power
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
SHA	Secure Hash Algorithm
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]	Evaluator Assessment of Changes Report (EAR) ST33K1M5A and ST33K1M5M B01 – Partial ETR, 22-RPT-663, v3.0, 3 August 2022
[ETRfC]	Evaluation Technical Report for Composition “ST33K1M5A and ST33K1M5M B01” – EAL6+, 22-RPT-783, version 2.0, 03 August 2022.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[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_0084]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	ST33K1M5A and ST33K1M5M B01 SECURITY TARGET, SMD_ST33K1M5AM_ST_21_001, Rev. B01.1, July 2022
[ST-lite]	ST33K1M5A and ST33K1M5M B01 SECURITY TARGET FOR COMPOSITION, SMD_ST33K1M5AM_ST_21_002, Rev. B01.1, July 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)