

Certification Report

NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02

Sponsor and developer: **STMicroelectronics**
Lambroekstraat, 5 Building B
1831 Diegem
Belgium

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

Report number: **NSCIB-CC-2300177-01-CR**

Report version: **2**

Project number: **NSCIB-2300177-01**

Author(s): **Jordi Mujal**

Date: **16 February 2024**

Number of pages: **12**

Number of appendices: **0**

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

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	7
2.3.1 Assumptions	7
2.3.2 Clarification of scope	7
2.4 Architectural Information	7
2.5 Documentation	8
2.6 IT Product Testing	8
2.6.1 Testing approach and depth	8
2.6.2 Independent penetration testing	9
2.6.3 Test configuration	9
2.6.4 Test results	9
2.7 Reused Evaluation Results	9
2.8 Evaluated Configuration	10
2.9 Evaluation Results	10
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

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 NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02. The developer of the NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 is STMicroelectronics located in Diegem, Belgium 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 consists of a certified hardware platform and a secure cryptographic library, built on this platform. The HW platform is a serial access microcontroller compliant with [PP_0084]. For details of the hardware platform, see the corresponding security target [HW-ST-lite] and certification report [HW-CERT]. The secure cryptographic library is a software library, providing additional cryptographic functions that can be operated on the hardware platform.

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 24 November 2022 ([CC-22-0587353/2](#)). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 29 January 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 major changes from previous evaluations are:

- The underlying HW was recertified.
- Update some guidance and adding a new guidance document.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02, 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 NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 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), ALC_FLR.1 (Basic Flaw Remediation) 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.

This document was re-issued on 16 February 2023 as version 2 to add a new ETRfc reference [ETRfc-v4.0]. The ETRfc was updated to correct an editorial issue. The validity for reuse of the ETRfc has not changed due to this process. The original validity dates from [ETRfc-v2.0] still apply.

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 NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 from STMicroelectronics located in Diegem, Belgium.

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)
Software	NesLib on ST33K1M5A and ST33K1M5M B02	6.7.4

To ensure secure usage a set of guidance documents is provided, together with the NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02. 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 HW Platform offers multiple features for high level security (see *[HW-CERT]* for more details):

- Two instances of the Arm® Cortex-M35P CPU connected in lockstep mode
- Die integrity
- Monitoring of environmental parameters
- 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 *[HW-ETRFC]*).

Specific to the Crypto Library:

- A symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard algorithm (DES) and Triple DES.
- A symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES).
- A cryptographic support module that provides hash functions (SHA-1, SHA-2, SHA-3, Keccak, and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3).
- An asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA), and Diffie-Hellman.
- An asymmetric key cryptographic support module that provides very efficient basic functions to build up protocols using Elliptic Curves Cryptography on prime fields GF(p) with elliptic curves in

short Weierstrass form, and provides support for ECDH key agreement and ECDSA generation and verification.

- A module for supporting elliptic curve cryptography on curve edwards25519, in particular ed25519 signature generation, verification and point decompression.
- A module for supporting elliptic curve cryptography on curve curve25519, in particular X25519 for key agreement.
- Support for Deterministic Random Bit Generators (DRBG).
- Prime number generation and RSA key pairs generation.
- It also provides a set of basic functions to securely manipulate data: Copy, Compare, Swap, Shift, XOR.

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].

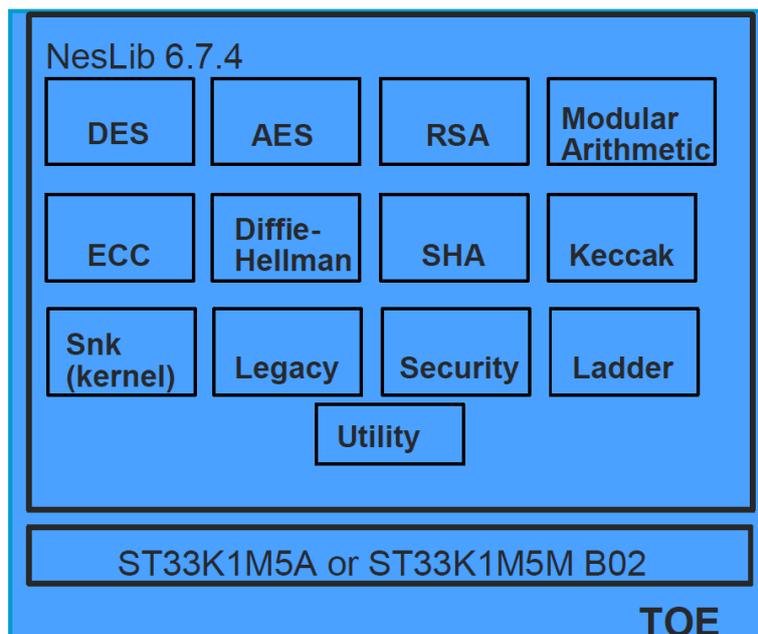
2.3.2 Clarification of scope

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 - when not used through NESLIB interface), the functionality and security of these features have not explicitly been addressed in the HW evaluation [HW-CERT]. 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 usage of NESCRYPT LLP without NESLIB, in order to support this analysis, the Vendor asked the Lab to carry out additional testing that is included in the [HW-ETRC].

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 (NesLib)	Version	Date
NesLib cryptographic library NesLib 6.7 – User manual	4	02 December 2021
NesLib 6.7 security recommendations for the ST33K platform secure microcontrollers –Application note	4	22 February 2022
NesLib 6.7.4 for ST33K Platforms – Release note	2	February 2023
NesLib - Limitation of NesLib_AES_CMAC - Technical note	1	February 2023
Identifier (HW Platform)	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	3	May 2023
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	3	May 2023
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_FW	7	March 2023
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	7	April 2023
ST33K Platform- TRNG Reference implementation: Compliance tests, AN_ST33K_TRNG	3	May 2023

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 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. In the baseline evaluation 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, the developer repeated all the functional tests. The evaluators considered the impact of the TOE changes and how these had been demonstrated through the developer testing, and as a result, the functional testing done by evaluators was not 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 was performed using 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 this re-evaluation the total test effort expended by the evaluators was 4 weeks. During that test campaign, 25% of the total time was spent on Perturbation attacks and 75% 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].

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-v4.0] for details.

2.7 Reused Evaluation Results

Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

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 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 NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02.

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-v4.0] 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. Please, note that this document needs to be used together with the [HW-ETRFC].

The verdict of each claimed assurance requirement is “Pass”.

Based on the above evaluation results the evaluation lab concluded the NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02, 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.1**. Check that both the EAL and augmentation are in bold text when fields are updated. 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. 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 NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 SECURITY TARGET, Revision 03.2, August 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
DFA	Differential Fault Analysis
DRBG	Deterministic Random Bit Generators
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
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) Cryptographic library NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 – Partial ETR, 23-RPT-1465, version 4.0, 29 January 2024.
[ETRfC-v2.0]	Evaluation Technical Report for Composition “NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02” – EAL5+, 23-RPT-1466, version 2.0, 29 January 2024.
[ETRfC-v4.0] ²	Evaluation Technical Report for Composition “NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02” – EAL5+, 23-RPT-1466, version 4.0, 13 February 2024.
[HW-CERT]	Certification Report ST33K1M5A and ST33K1M5B B02, NSCIB-CC-2300112-01-CR, version 2, 03 November 2023.
[HW-ETRfC]	Evaluation Technical Report for Composition “ST33K1M5A and ST33K1M5M B02” – EAL6+, 23-RPT-975, version 1.0, 30 August 2023
[HW-ST]	ST33K1M5A and ST33K1M5M B02 SECURITY TARGET, Rev. B02.1, May 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	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_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]	NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 SECURITY TARGET, Revision 03.2, August 2023
[ST-lite]	NesLib 6.7.4 on ST33K1M5A and ST33K1M5M B02 SECURITY TARGET FOR COMPOSITION, Revision 03.2, August 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)

² The ETRfC was updated to correct an editorial issue. The validity for reuse of the ETRfC has not changed due to this process. The original validity dates from [ETRfC-v2.0] still apply.