EUCC Certification Report

ST54M A01

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:	**EUCC-3110-2026-2500107-01 Certification Report**
Report version:	**1.0.1**
Project number:	**EUCC-2500107-01**
Author:	**Alireza Rohani, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**26 August 2026**
Number of pages:	**18**
Number of appendices:	**0**

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

® TrustCB is a registered trademark. Any use or application requires prior approval by TrustCB.

CONTENTS

Foreword 3

International recognition of the certificate 4

1 Executive Summary 5

2 ICT Product details 7

2.1 Identification of the ICT Product 7
2.2 Contact information related to the evaluation of the ICT Product 7
2.3 Security services and policies 7
2.3.1 Security services 7
2.3.2 Vulnerability management 8
2.3.3 Assurance Continuity policies 8
2.3.4 Lifecycle management processes and production facilities 8
2.3.5 Patch management process 8
2.4 Assumptions and Clarification of Scope 8
2.4.1 Assumptions 8
2.4.2 Clarification of scope 8
2.5 Architectural Information 9
2.6 Supplementary Cybersecurity Information 9

3 Evaluation summary 10

3.1 Identification of used assurance components 10
3.2 EUCC State of the Art documents and Protection Profiles 10
3.3 ICT Product testing 10
3.3.1 Testing approach and depth 10
3.3.2 Independent penetration testing 11
3.3.3 Test configuration 11
3.3.4 Test results 12
3.4 ICT Product evaluation 12
3.4.1 Reused evaluation results 12
3.4.2 Evaluated configuration 12
3.4.3 Assessment against each assurance requirement 12
3.5 Results of the evaluation 15
3.6 Certificate information and scheme label 15
3.7 Comments and Recommendations 15

4 Security Target 16

5 Glossary 16

6 Bibliography 17

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

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

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ST54M A01, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is STMicroelectronics located in Rousset, France and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE is ST54M A01, which is included in the ST54M platform, a near-field communication (NFC)-compatible device that comprises a contactless front-end, and a secure element (ST54M_SE). The ST54M_SE is in the scope of this evaluation, while the NFC device is out of scope of this evaluation.

Furthermore, the ST54M_SE features a MIFARE Classic® cryptographic accelerator called Crypto1, and two specific cryptographic accelerators called SM3 and SM4 which are all out of the scope of this evaluation.

The ST54M A01 is a serial access microcontroller designed for secure mobile applications. It incorporates the most recent generation of Arm® processors for embedded secure systems. Their Arm® Cortex® M35P 32-bit RISC core is built on Armv8-M architecture with additional security features to help to protect against advanced forms of attacks.

The ST54M A01 provides high performance thanks to a fast Cortex® M35P processor, crypto-accelerators and improved Flash memory operation.

The Cortex® M35P core and its cache memory bring great performance and excellent code density thanks to the Thumb®-2 instruction set.

Strong and multiple fault protection mechanisms ensure a guaranteed high-detection coverage that facilitates the development of highly secure software. This is achieved by using two CPUs in locked-step mode, error codes in sensitive memories and hardware logic.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in [AN_SECU] section 2.3.1.1, and [UM-DG] section 25.2.1. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

The TOE claims conformance to the following Protection Profile and configuration *[PP] and [PPConfig]*:

- Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025, BSI-CC-PP-0084-V2-2026
- Security IC Platform Multi-assurance PP-Configurations, v 1.0, 16 December 2025, BSI-CC-PP-0125-2026

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500107-01**, dated 26-08-2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 18 June 2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets multi-assurance evaluation level:

- Global conformance:
  EAL5 augmented with ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and ASE_TSS.2.
- Sub-TSFs Loader 1, Loader 2 and Address-based Access Control:
  EAL6 augmented with ALC_FLR.2 and ASE_TSS.2.

The AVA_VAN level applied during the evaluation was AVA_VAN.5. This assurance level is recognised by article 52 of [CSA] as 'high'.

Consumers of this ICT Product 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.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

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 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product ST54M A01 from STMicroelectronics located in Rousset, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST54M	IC Maskset name: K4R0 IC version: C Master identification number: 0x02A2
Software	Firmware	4.1.4

Additional requirements for the operational environment of the certified ICT product are described in section 3.4 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information”.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	STMicroelectronics
Address:	190 avenue Celestin Coq, ZI de Rousset-Peynier, 13106 ROUSSET, FRANCE
Certified product contact details	**Samantha.rigaudie@st.com**

Developer of the certified ICT Product

ICT product developer	STMicroelectronics

Identification of CAB

The Certification Assessment Body for this ICT Product is **TrustCB B.V.** in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

SGS Brightsight B.V. in Delft, The Netherlands

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security services and policies

2.3.1 Security services

ST54M A01 offers a unique combination of high performances and very 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/AIS31 class PTG.2 compliant True Random Number Generator,
- Arm® Cortex® M35P Memory Protection Unit,
- A Library Protection Unit (LPU) to isolate protected code,
- Hardware Security Enhanced DES accelerator,
- Hardware Security AES accelerator,
- NExt Step CRYPTography accelerator (Nescrypt Fast) for public key cryptography algorithms,
- PQC hardware accelerators: Keccak-p, KNTT, DNTT and DMF for post-quantum cryptography algorithms like ML-KEM and ML-DSA.

NESCRYPT FAST coprocessor and NTT (DNTT/KNTT) and DMF accelerators in the PQC coprocessor provide only primitive operations. They include several security mechanisms enforcing or supporting several SFRs of the Security Target *[ST]*, but are not addressing any specific cryptographic SFR.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the ST54M A01

Document reference: Available in PSIRT webpage, https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.6.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 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 3.4 of the *[ST]*.

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.

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Threats addressed by the TOE and the IT environment are presented in Section 3.2 of *[ST]*, and include the threats as presented in the *[PP]* and *[PPConfig]*, but also includes additional threats. The assumed level of expertise of the attacker for all identified threats is High.

The Organizational Security Polices (OSPs) are the same as in *[PP]* and *[PPConfig]*. No OSPs have been added, removed or modified.

2.5 Architectural Information

The TOE (ST54M A01) is included in the ST54M platform, a near-field communication (NFC)-compatible device that comprises a contactless front-end (referred to as the ST54M_CLF), and a secure element (referred to as the ST54M_SE). The ST54M_SE is in the scope of this evaluation, while the ST54M_CLF is out of scope of this evaluation.

2.6 Supplementary Cybersecurity Information

The following website link was provided for the ST54M A01 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.st.com/en/secure-mcus/st54m.html

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ST54M A01.
- The period during which the ST54M A01 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated aligning with the certificate validity.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the ST54M A01.
- the online repository listing publicly disclosed vulnerabilities related to the ST54M A01 and to any relevant cybersecurity advisories .

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ST54M A01:

Reference	Identifier	Version
DS_ST54M	NFC controller and secure element system on chip – Preliminary data, ST54M - Datasheet	0.3
UM_ST54M_SE	ST54M_SE OS developer's guide – Preliminary data, User manual	0.6
UM_ST54M_SE_FW	ST54M_SE firmware - User manual	7
100883_0102_00_en	Arm® Cortex-M35P Processor Technical Reference Manual	r1p2
AN_SECU_ST54M_SE	Security guidance of the ST54M_SE secure MCU subsystem – Application note	1
UM_ST54M_SE_TRNG14	Random number generation V1.4 for ST54M_SE - User manual	1

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were multi-assurance evaluation level:

- Global conformance:
  EAL5 augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5, and ASE_TSS.2.
- Sub-TSFs Loader 1, Loader 2 and Address-based Access Control:
  EAL6 augmented with ALC_FLR.2 and ASE_TSS.2

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

- Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025, BSI-CC-PP-0084-V2-2026
- Security IC Platform Multi-assurance PP-Configurations, version 1.0, 16 December 2025, BSI-CC-PP-0125-2026

3.3 ICT 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.

3.3.1 Testing approach and depth

The developer test approach distinguishes between two parts of the TOE (SE):

- IC Hardware (HW), including all hardware parts of the TOE
- Dedicated Software = Firmware (FW)

Both TOE parts are subjected to two global test steps:

1. Verification tests are performed during development and include extensive simulation and emulation

testing on source code (FW) as well as digital and analog parts of the HW. For the HW, these simulations also include timing analysis steps to determine the correct operation. Further, the developer uses code coverage methodologies to verify that all functionality of the FW and HW is sufficiently covered. Any test gaps that are identified in this phase are investigated and remedied either by implementing additional test cases or by alternative means.

2. Once silicon is available, the developer performs validation tests on engineering samples. During this phase, specific characterisation tests exercising features that cannot be covered by simple functional tests are performed and all security critical macrocells are tested. In addition, the FW tests are repeated on silicon to verify the integration of FW and HW.

The bulk of the ATE_COV/ATE_DPT analysis has been performed based on the various coverage analysis tools and rationales as base. Therefore, the following aspects were taken into account:

- A witnessing session was performed in STM's site in Rousset (France).
- The witnessing session is used to gain insight in certain aspects of the developer testing like:
  - Presentation of test results
  - Test environment and execution
  - Tests will be selected that cover various aspects of the TOE, as well as areas where the code coverage approach has limitations (e.g. crypto operations).
- To this end, three categories of tests are defined:
  - Category 0: TOE identification

- Category 1: Details on test approach and test environment
- Category 2: Actual tests.

3.3.2 Independent penetration testing

The bulk of the ATE_COV/ATE_DPT analysis has been performed based on the various coverage analysis tools and rationales as base. Therefore, the following aspects were taken into account:

- A witnessing session was performed in STM's site in Rousset (France).
- The witnessing session is used to gain insight in certain aspects of the developer testing like:
  - Presentation of test results
  - Test environment and execution
  - Tests will be selected that cover various aspects of the TOE, as well as areas where the code coverage approach has limitations (e.g. crypto operations).
- To this end, three categories of tests are defined:
  - Category 0: TOE identification
  - Category 1: Details on test approach and test environment
  - Category 2: Actual tests.

This section contains information with regard to the evaluator testing effort, mandated to be included in the ETR by AVA_VAN.5-5, AVA_VAN.5-10 and AVA_VAN.5-12.

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. This analysis was performed according to the attack methods in [JIL-AM].
- 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 spent in the period between November 2025 and May 2026 with 31 man-weeks in total for testing and reporting. During the test campaign, 3% of the total time was spent on physical attacks, 26% on perturbation attacks, 7% on retrieving keys with FA, 61% on side-channel attacks and 3 % on RNG.

3.3.3 Test configuration

The ITSEF tested the TOE in the following configuration

- ST54M K4R0 HW Rev A FW 4.0.2
- ST54M K4R0 HW Rev B FW 4.1.4
- ST54M K4R0 HW Rev C FW 4.1.4 (This is the same configuration as stated in the ST)

The ITSEF assessed the differences between these versions and concluded the test results obtained on the different versions are fully applicable to the version of the TOE stated in the *[ST]*.

Assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

3.3.4 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]* for details.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

There is no reuse of evaluation results in this certification.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 22 Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number ST54M A01.

3.4.3 Assessment against each assurance requirement

Global set of SARs:

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.2

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5
TSF internals	ADV_INT.2
Implementation representation	ADV_IMP.1
TOE design	ADV_TDS.4

PTG

PTG	
Random number generation	PTRNG.2

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.2

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

AVA

AVA	
Vulnerability analysis	AVA_VAN.5

SARs applicable to the sub-TSFs Loader 1, Loader 2, and Address-based Access Control

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2

TOE summary specification	ASE.TSS.2

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5
TSF internals	ADV_INT.3
Security policy modelling	ADV_SPM.1
Implementation representation	ADV_IMP.2
TOE design	ADV_TDS.5

PTG

PTG	
Random number generation	PTRNG.2

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

ALC

ALC	
CM capabilities	ALC_CMC.5
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.3

ATE

ATE	
Coverage	ATE_COV.3
Depth	ATE_DPT.3
Functional tests	ATE_FUN.2
Independent testing	ATE_IND.2

AVA

AVA	
Vulnerability analysis	AVA_VAN.5

3.5 Results of the evaluation

The ITSEF documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the evaluation results the ITSEF concluded the ST54M A01, to be **CC:2022 R1 Part 2 extended, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**High**', with **AVA_VAN 5** and to meet the following multi assurance package requirements:

- Global conformance: EAL5 augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5, and ASE_TSS.2.
- Sub-TSFs Loader 1, Loader 2 and Address-based Access Control: EAL6 augmented with ALC_FLR.2 and ASE_TSS.2.

This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

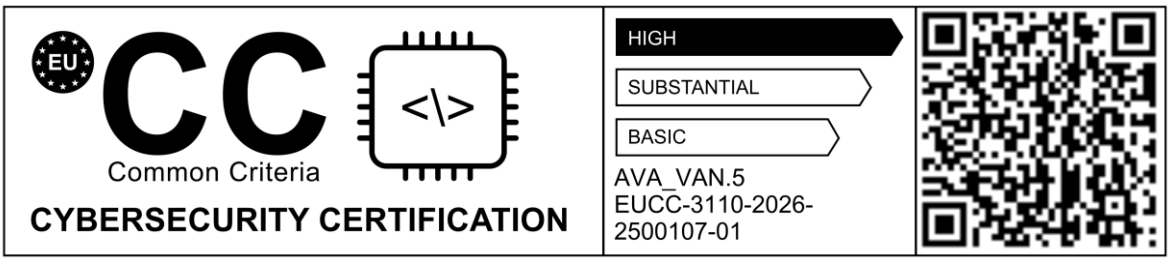
Security Target claims 'strict' conformance to the Protection Profile *[PP]* and *[PPConfig]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500107-01

Date of issuance: 26-08-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. This TOE is critically dependent on the guidance (especially section 2.3.1.1 of [AN_SECU] and section 25.2.1 of [UM_DG]) in order to be protected against the attackers with high attack potential. . Therefore, it is vital to maintain meticulous adherence to the user guidance as listed in section 2.6 of this report. .

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).

4 Security Target

The certification references the following security target:

ST54M A01 Security Target, SMD_ST54M_ST_24_001, Rev A01.4, June 2026 *[ST]*.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report

6 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, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022, 2023-04-20
[DEV_DOCS]	[CI-list Rev_A] SMD_ST54M_A01_CFGL_25_001_v1_0
	[AN_SECU] Security guidance of the ST54M_SE secure MCU subsystem – Application note, AN_SECU_ST54M_SE, v1, May 2026
	[DS] NFC controller and secure element system in package - ST54M preliminary datasheet, version 0.3, March 2026
	[UM_DG] ST54M_SE OS developer's guide - Preliminary data - User Manual, version 0.6, April 2026
	[UM_FW] ST54M_SE firmware - User manual, version 7, April 2026
	[ARM_TRM] Arm® Cortex-M35P Processor Technical Reference Manual, version r1p2, October 2021
	[UM_TRNG] Random number generation V1.4 for ST54M_SE - User manual, version 1.0, May 2026
[ETR]	Evaluation Technical Report "ST54M A01" – EAL5+/6+, 25-RPT-1509, version 3.0, 18 June 2026
[ETRfC]	Evaluation Technical Report for Composition "ST54M A01" – EAL5+/6+, 26-RPT-690, version 2.0, 18 June 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[PP]	Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025, registered under the reference BSI-CC-PP-0084-V2-2026
[PPConfig]	Security IC Platform Multi-assurance PP-Configurations, version 1.0, 16 December 2025, registered under the reference BSI-CC-PP-0125-2026

[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA ADV_SPM]	EUCC STATE-OF-THE-ART DOCUMENT ADV_SPM.1 interpretation for CC:2022 transition Version 1.1, October 2025
[SotA_CC_IC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Common Criteria to integrated circuits Version 2.0, December 2024
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, February 2025.
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025.
[EUCC-AgreedCrypto]	EUCC Scheme, Guidelines on Cryptography, Agreed Cryptographic Mechanisms Version 2, May 2025
[AIS 20/31]	A Proposal for Functionality Classes for Random Number Generators, Version 3.0, September 10, 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[SP800-90A]	NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP800-90B]	NIST Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation
[ST]	ST54M A01 Security Target, SMD_ST54M_ST_24_001, Rev A01.4, June 2026
[ST-lite]	ST54M A01 Security Target for composition, SMD_ST54M_ST_24_002, Rev A01.4, June 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2, ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)