Certification Report

Cortex M35P r1p1

Sponsor and developer: ***Arm Limited***
110 Fulbourn Road
Cambridge
England CB1 9NJ

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-201210-CR**
Report version:	**1.1**
Project number:	**201210**
Author(s):	**Wouter Slegers, Hans-Gerd Albertsen**
Date:	**15 June 2020**
Number of pages:	**13**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cortex M35P r1p1. The developer of the Cortex M35P r1p1 is Arm Limited located in 06560 Valbonne, France and Arm Limited located in Cambridge, England CB1 9NJ 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 the set of functionalities, encoded in Verilog, for a processor in a Security microcontroller IC. The intended environment for the TOE is the Security IC for smart card applications or similar services as identified and described in *[PP]*. The TOE provides the functionality for software execution and controlling access to memory addresses in a Security IC.

The TOE is not in itself a Security IC, it supports development of a Security IC.

The evaluation and certification of this TOE was performed to enable re-use of the processor into an EAL6+ Security IC, hence to fulfil the composition requirements *[JIL-COMP]* assurance up to and including EAL6 augmented (EAL6(+)) is needed.

Due to the form of the TOE (Verilog), only a limited amount of attacks is directly applicable and countered by the TOE. For example, physical attacks are not countered by this TOE. **Users of the TOE, developers of a Security IC, must strictly follow the guidance and must successfully pass a composite CC evaluation against *[PP]* to claim full EAL4+ and/or AVA_VAN.5 resistance**.

During the composition into a full Security IC, significant vulnerability analysis and testing must be performed. However, the *[ETRfC]* and the guidance enable efficient re-use.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 13-02-2020 with the approval of the ETR. This certification report has been updated on 15-06-2020 with a minor clarification without impact on the certificate. 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 Cortex M35P r1p1, 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 Cortex M35P r1p1 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 provides 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) and ASE_TSS.2 (TOE Summary Specification with architectural design summary).

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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Cortex M35P r1p1 from Arm Limited located in 06560 Valbonne, France.

The TOE is comprised of the following main components:

	Name	Version
Hardware[2]	Cortex-M35P Synthesizable Verilog	AT627-MN-22110-r1p1-00rel0
Software	Cortex-M35P Execution Test Bench	AT627-MN-22010-r1p1-00rel0
	Cortex-M35P Functional Test Source	AT627-VE-70006-r1p1-00rel0
	Cortex-M35P RAM Integration Test Bench	AT627-MN-70002-r1p1-00rel0

To ensure secure usage a set of guidance documents is provided together with the Cortex M35P r1p1. Details can be found in section 2.5 of this report.

The life cycle covers the development of the TOE (i.e. phase 2 of *[PP]*. For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.6.

2.2 Security Policy

The TOE is the set of functionalities for a processor in a Security microcontroller IC. The intended environment for the TOE is the Security IC for smart card applications or similar services as identified and described in *[PP]*. The TOE provides the functionality for software execution and controlling access to memory addresses in a Security IC.

The user of the TOE is the designer of a Security IC microcontroller product that integrates the TOE into their design for the microcontroller product. The user is referred to as the IC Designer. The user of the TOE is also the programmer of the Security IC dedicated software and the programmer of the Security IC embedded software that use the TOE programming interfaces consisting of the TOE instruction set and exception handling. It is the responsibility of the IC designer to instruct the programmer how to use the TOE.

The TOE is delivered as source code to be integrated by the IC Designer into the source code of their Security microcontroller product.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.1.1 and 5.2.1 of the *[ST]*.

2.3.2 Clarification of scope

The TOE is the set of functionalities, encoded in Verilog, for a processor in a Security microcontroller IC. The intended environment for the TOE is the Security IC for smart card applications or similar services as identified and described in [PP]. The TOE provides the functionality for software execution and controlling access to memory addresses in a Security IC.

[2] This TOE comprises the design of a processor. As such, no physical hardware is delivered, but the synthesizable Verilog is intended to be integrated into a hardware solution.

The TOE is not in itself a Security IC, it supports development of a Security IC.

The evaluation and certification of this TOE was performed to enable re-use of the processor into an EAL6+ Security IC, hence to fulfil the composition requirements *[JIL-COMP]* assurance up to and including EAL6 augmented (EAL6(+)) is needed.

Due to the form of the TOE (Verilog), only a limited amount of attacks is directly applicable and countered by the TOE. **For example, physical attacks are not countered by this TOE**. **Users of the TOE, developers of a Security IC, must strictly follow the guidance and must successfully pass a composite CC evaluation against *[PP]* to claim full EAL4+ and/or AVA_VAN.5 resistance**.

During the composition into a full Security IC, significant vulnerability analysis and testing must be performed. However the *[ETRfC]* and the guidance enable efficient re-use.

See *[ST]* chapter 5.1.3 and 5.2.3 for details regarding threats and policies that are countered by the environment.

2.4 Architectural Information

The TOE is the set of functionalities for a processor in a Security microcontroller IC.

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:

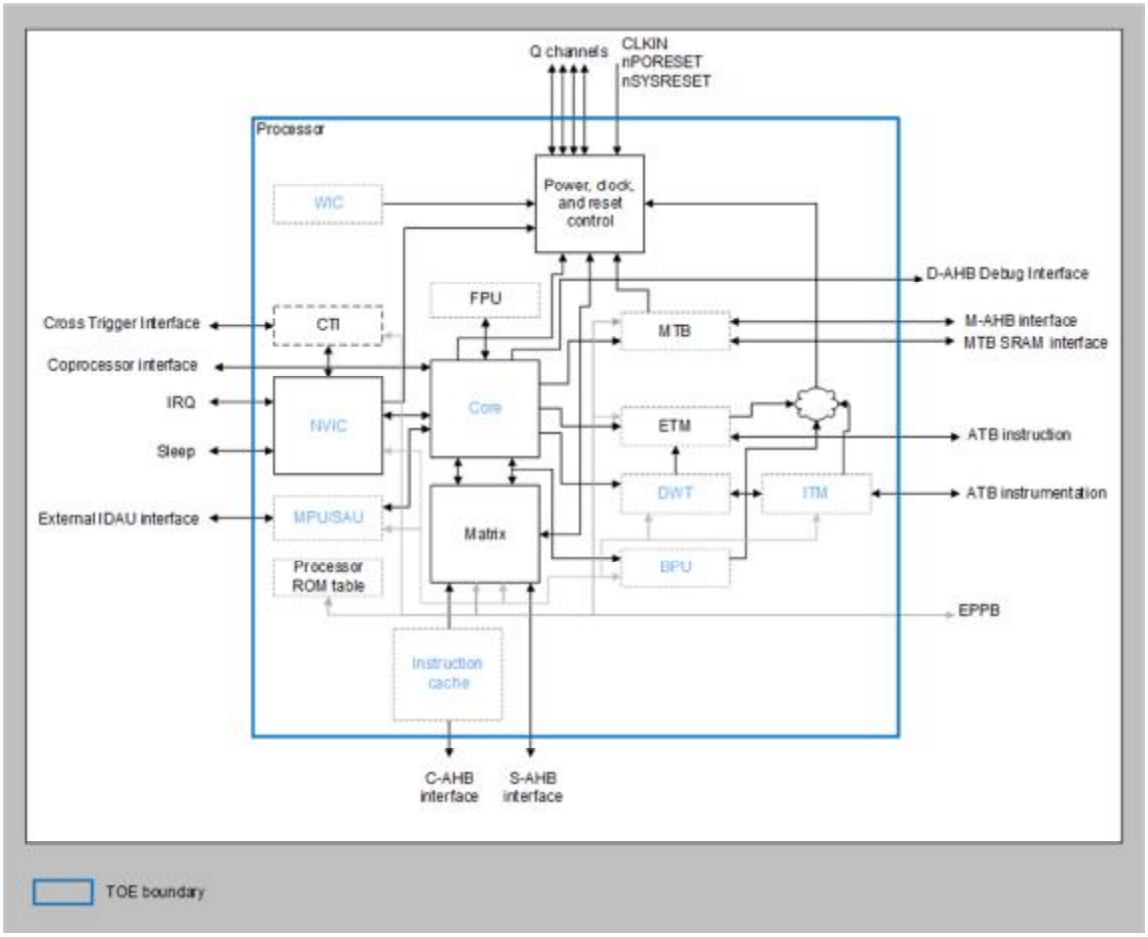

Figure 1. Logical architecture of the TOE.

Note that Figure 1 only shows the main interfaces of the TOE. For more detailed descriptions of all interfaces, see [IIM] and [TRM]. Although the MPU is part of the MPU extension and therefore can be optionally included or excluded during processor integration, it should always be included for a certified configuration. Components in blue are configurable during processor integration. For

example, the number of programmable memory regions in the MPU and SAU can be configured during processor integration.

The TOE has the following features:

- Processor core (Core)
- Instruction cache.
- Security attribution and memory protection (MPU/SAU)
- Floating Point Unit (FPU)
- Nested Vectored Interrupt Controller (NVIC)
- Wake-up Interrupt Controller (WIC)
- Power, clock, and reset control (PCR)
- Cross Trigger Interface Unit (CTI)
- Matrix

Additionally, the TOE provides the following debug features:

- Embedded Trace Macrocell (ETM)
- Micro Trace Buffer (MTB)
- Debug and trace additional components
  - Configurable Breakpoint Unit (BPU)
  - Configurable Data Watchpoint and Trace unit (DWT)
  - Instruction Trace Macrocell (ITM)
  - ROM table

As per Security Guidance [SG] (see table in chapter 2.5), the debug functionality shall not be used in the certified configuration. For more information on each individual component, see *[ST].*

2.5 Documentation

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

Reference	Name	Version
[ERR]	Arm® Cortex®-M35P Product Errata Notice	AT627-DC-11000-r1p1-00rel0
[RN]	Arm® Cortex®-M35P Release Note	AT627-DC-06003-r1p1-00rel0
[TRM]	Arm® Cortex®-M35P Processor Technical Reference Manual	AT627-DA-03001-r1p1-00rel0
[IIM]	Arm® Cortex®-M35P Processor Integration and Implementation Manual	AT627-DC-70047-r1p1-00rel0
[UGRM]	Arm® Cortex®-M35P Processor User Guide Reference Manual	AT627-DA-03005-r1p1-00rel0
[AS]	Arm® Cortex®-M35P v8-M Architecture Supplement	AT627-DC-50000-r1p1-00rel0
[SG]	Arm® Cortex®-M35P r1p1 Security Guidance	PJDOC-466751330-8802 3.1

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 has tested the TOE according to the developer's IP verification strategy. A verification plan has been made that covers the complete development life-cycle of the TOE, and testing has been performed at all development stages, commensurate with the maturity of the product at the corresponding stage. The testing comprises:

- (Multi-)Unit level tests, which test (combinations of) parts of the TOE based on the UVM methodology,
- Top level tests, which test the whole TOE using both pre-defined and randomised test suites,
- System level tests, which test the TOE in some example environments with simple payloads, and
- Formal verification, which is applied at various levels using System Verilog.

Additionally, the developer has performed an analysis of the coverage provided by the testing, both from a code and a functional perspective. Any gaps in the coverage have been assessed and they have either been amended by additional testing, or shown to be irrelevant.

The developer tested the TOE in the following configuration: Cortex-M35P r1p1. This is the same configuration as stated in the ST.

Almost all test results were as expected. For the tests where this was not the case, the developer provided a proper rationale for this.

For unit-level tests and top-level RIS tests, these 'false failures' are analysed as follows. Each run corresponds to a randomly generated seed that results in a number of error messages or signatures.

- During regression testing, all seeds are examined for each signature.
- During cumulative testing, one seed is examined per signature, unless it is a critical error.

It is then confirmed whether these are indeed 'false failures'.

For system level tests all results were as expected.

The evaluator has witnessed at the developer's premises at least one test for each (multi-)unit level test bench not related to debug functionality, one test for each top level test bench, and a single system level payload. This collection of tests provided a good coverage of security features.

The evaluator has defined an independent test subset aimed at verifying the presence of claimed security functions and security mechanisms. These tests were chosen as they investigate behaviour that is not directly visible at the functional interfaces, whereas the developer has already shown through their coverage and depth analysis that all functional interfaces and design aspects are properly tested.

2.6.2 Independent Penetration Testing

The methodical vulnerability 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-AAPS].*
- 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.

In total 4 perturbation tests have been performed. The overall time spent for penetration testing was 14 days.

2.6.3 Test Configuration

The penetration testing has not been performed on a final product (as the TOE is not a final product), but on an FPGA that implements the TOE in the environment (i.e. representative of a final product). This is similar to performing penetration testing on an Integrated Circuit TOE without Operating System and Application which is not a final product. Some modifications were made to the RTL to enable testing of resistance against sidechannel and perturbation attacks. These modifications consisted of adding lines that are connected to an external bus and to an internal signal in order to alter the internal signal by XOR-ing it with the output of the external bus (or some other logical operation).

2.6.4 Testing 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.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Re-used evaluation results

There has been re-use of the ALC aspects for the site involved in the development and production of the TOE, by use of one Site Certificate and one Site Technical Audit Report (for Arm Sophia Antipolis).

The site Austin has been visited as part of this evaluation. A Site Technical Audit Report *[STAR]* has been created. See also chapter 2.9.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cortex M35P r1p1. The TOE can be identified using the procedure described in the Arm Cortex-M35P Processor Release Note [RN], which includes verifying the checksums of the received files.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* and Site Technical Audit Report for the Austin site *[STAR]*[3] which references ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to 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 Cortex M35P r1p1, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ALC_FLR.1 and ASE_TSS.1.** This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target is based on *[PP]* but does **not** claim conformance to the Protection Profile *[PP]*. Nevertheless, composite evaluations based on this TOE can claim *[PP]* conformance.

[3] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 because no cryptographic operations are part of the TOE. Therefore, rating is not applicable.

The independent vulnerability analysis has been performed according to *[CC]* and other methods and standards as listed in Appendix C of *[ETRfC]*. The penetration testing has not been performed on an actual product, but on an FPGA that implements the design comprising the TOE.

The level of access to the TOE cannot be identically reproduced in a real attack scenario on a composite product with a physical implementation. For this reason, it is not possible to include attack potential calculations according to *[JIL-AAPS]*.

If any of the attack scenarios as documented in the *[ETRfC]* is relevant in a composite evaluation, the composite evaluator should note the following regarding the rating of required knowledge of this TOE (i.e., the processor design). The TOE comprises the implementation representation which is available under a licensing agreement with the developer. Hence, any required knowledge of the implementation representation of the TOE shall not be rated higher than Restricted in an attack potential calculation.

The TOE does not perform speculative execution, and as such attacks relying on this feature (e.g. Spectre, Meltdown) are not applicable. Attacks that rely on the physical implementation of the TOE (e.g. row hammer) shall be considered by the composite evaluator if they are applicable.

3 Security Target

The Arm Cortex-M35P r1p1 Security Target, Version 4.1,16.01.2020 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

BPU	Break Point Unit
CTI	Cross Triger Interface
DWT	Data Watchpoint and Trace
EMA	Electromagnetic Analysis
ETM	Embedded Trace Macrocell
FPU	Floating Point Unit
IC	Integrated Circuit
IT	Information Technology
ITM	Instruction Trace Macrocell
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MPU	Memory Protection Unit
MTB	Micro Trace Buffer
MTX	Matrix
NSCIB	Netherlands scheme for certification in the area of IT security
NVIC	Nested Vectored Interrupt Controller
PCR	Power, clock, and reset control
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
SAU	Security Attribution Unit
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
WIC	Wake-up Interrupt Controller

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 “Cortex-M33 r0p4” and “Cortex-M35P r1p1”-EAL6+, 19-RPT-895, Version 5.0, 06-02-2020.
[ETRfC]	Evaluation Technical Report for Composition “Cortex-M35P r1p1”-EAL6+, 19-RPT-897, Version 5.0, 06-02-2020.
[JIL-AAPS]	JIL, (Mandatory) Application of Attack Potential to Smartcards, Version 2.9, January 2013
[JIL-COMP]	JIL, Composite product evaluation for Smart Cards and similar devices, version 1.5.1 May 2018.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the referenced BSI-PP-0084-2014.
[ST]	Arm Cortex-M35P r1p1 Security Target, Version 4.1,16.01.2020.
[ST-Lite]	Arm Cortex-M35P r1p1 Lite Security Target, Version 1.1, 16.01.2020.
[STAR]	Site Technical Audit Report Arm Austin, 19-RPT-672, Version 3.0, 06.02.2020
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).