Certification Report

J-Tacho v1.2.6

Sponsor and developer: ***STMicroelectronics***
Z.I. Marcianise SUD
81025 Marcianise (CE)
Italy

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

Report number:	**NSCIB-CC-222356-CR**
Report version:	**1**
Project number:	**222356**
Author(s):	**NLNCSA/Carolina Lavatelli**
Date:	**17 April 2019**
Number of pages:	**12**
Number of appendices:	**0**

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-222356**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**STMicroelectronics** **Z.I. Marcianise SUD** **81025 Marcianise (CE), Italy**
Product and assurance level	**J-Tacho v1.2.6** Assurance Package: ▪ EAL4 augmented with ATE_DPT.2 and AVA_VAN.5 Protection Profile Conformance: ▪ Digital Tachograph – Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091, Version 1.0, 9 May 2017
Project number	**222356**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL 7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **18-04-2019** Certificate expiry : **18-04-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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.

TÜVRheinland®
Precisely Right.

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 J-Tacho v1.2.6. The developer of the J-Tacho v1.2.6 is STMicroelectronics (STM) located in Marcianise, Italy. STM is 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.

J-Tacho v1.2.6 (TOE) is a contact Digital Tachograph card compliant with European regulation *[EU-TACH]* and Tachograph Protection Profile *[PP-TACH].* J-Tacho v1.2.6 implements Generation 1 and Generation 2 modes and supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card. The Tachograph card type is set during the personalization phase. J-Tacho v1.2.6 provides the following main functionalities:

- Store card and user identification data. This data is used by the Vehicle Unit to identify the user, provide services and grant data access rights accordingly
- Store data related to the user including activity data, events and faults, and control data.

The TOE is composed of the IC and dedicated embedded software, the Java Card closed system with a limited set of GlobalPlatform functionalities and the Tachograph application. The TOE can be delivered under different form factors such as wafer, micro-module or contact card.

This evaluation has been performed as a composite evaluation on ST31G480 D01, which has been certified under the reference ANSSI-CC-2019/12 *[IC-CERT]*.

The TOE has been evaluated by Brightsight B.V. in Delft, The Netherlands. The evaluation was completed on April 9th 2019 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the J-Tacho v1.2.6, 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 J-Tacho v1.2.6 are advised to verify that their own environment is consistent with the security target, to apply the recommendations provided in the security guidance *[AGD_PRE] and [AGD_OPE]* 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 it meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ATE_DPT.2 (Testing security enforcing modules) 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]*.

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 J-Tacho v1.2.6 from STMicroelectronics located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	Component Identifier	Version
Hardware/ Software	STMicroelectronics security controller	ST31G480 D01
	NESLib cryptographic library	v6.2.1
	J-SAFE3 Java Card Platform (including the native Operating System)	v1.2.6
	J-Tacho Tachograph Application	v1.13

The guidance documents referenced in section 2.5 of this report are provided together with the TOE to ensure its secure usage. They are considered integral to the TOE.

For a detailed and precise description of the TOE lifecycle refer to *[ST-Lite]* section 5.1.9.

2.2 Security Policy

J-Tacho v1.2.6 is a contact Tachograph card that implements the EU directive *[EU-TACH]*, which comprises the following main functions:

- Store card and user identification data. This data is used by the Vehicle Unit to identify the user, provide services and grant data access rights accordingly
- Store data related to the user including activity data, events and faults, and control data.

J-Tacho v1.2.6 supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card.

The main security features of the TOE are the following:

- Authenticate the Personalization agent that is allowed to read/write sensitive data and to transition to the irreversible end usage phase.
- Prevent and detect unauthorised data access or manipulation.
- Enforce integrity and authenticity of the data exchanged with the recording equipment.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target, none of which are covered by the TOE itself, lead to a set of security objectives to be fulfilled by the TOE Environment. Detailed information on the assumptions and security objectives for the TOE environment can be found in *[ST-Lite]* sections 7.5 and 7.6.2, respectively.

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.

Refer to the certification report *[IC-CERT]* for clarification of the scope of the evaluation of the underlying IC.

2.4 Architectural Information

The TOE consists of ST31G480 D01, which provides the cryptographic library, J-SAFE 3 platform[2], and a unique application, J-Tacho, which provides Generation 1 and Generation 2 tachograph modes, as shown in Figure 2-1. The TOE does not allow card content operations (load/delete applications) in the end-usage phase.

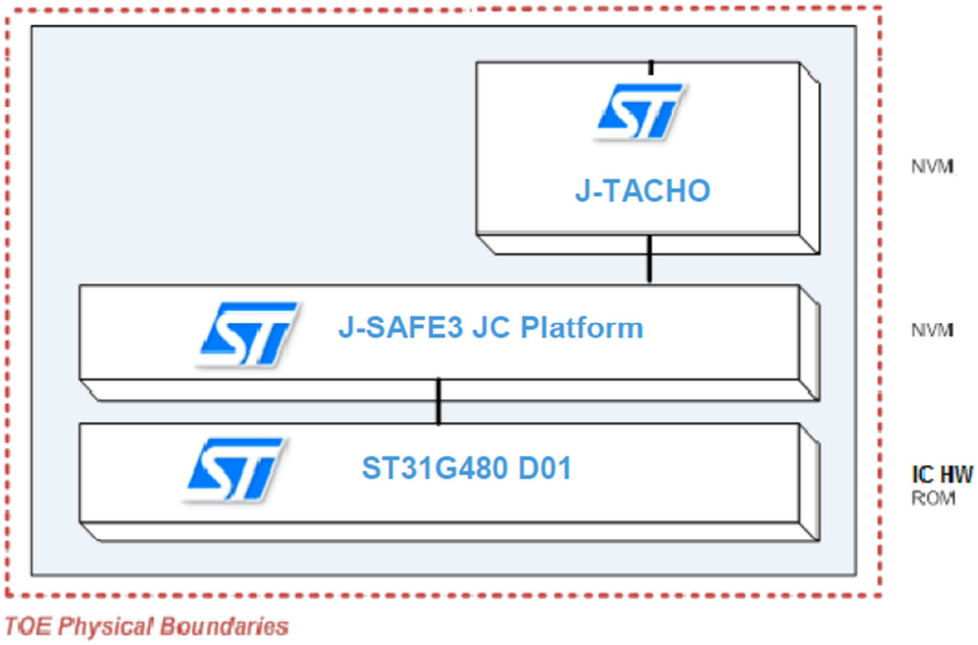

Figure 2-1: TOE scope

2.5 Documentation

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

Identifier	Version
[AGD_PRE] J-TACHO – Preparative Procedure	Rev. 1, 28-3-2019
[AGD_OPE] J-TACHO – Operational User Guidance	Rev. 1, 27-3-2019

2.6 IT Product Testing

The evaluator examined the documentation of the developer's testing activities and verified that they meet the testing assurance requirements.

2.6.1 Testing approach and depth

The developer has performed extensive testing of TOE security functionality at the external interface, subsystem and module levels, and has also successfully passed the commercial UL Smart Tachograph test suite, which satisfies the minimal functional test requirements as defined in Appendix 9 of Annex 1C of *[EU – 2016/799]*.

[2] J-SAFE 3 is compliant with Java Card 3.0.4 and GlobalPlatform 2.2.1; however, card content management is permanently disabled before TOE delivery.

The evaluator has performed test witnessing at developer's site, and has defined spot-checks on the calculation of code-coverage as used by the developer to demonstrate the completeness of the testing.

2.6.2 Independent Penetration Testing

The independent penetration test plan has been designed based on the evaluator's white box vulnerability analysis, in compliance with the attack methodology *[JIL-AM]* for products claiming resistance to attackers with high attack potential (AVA_VAN.5) and the composite evaluation methodology *[JIL-COMP].*

The vulnerability analysis has followed the two main steps of the method described in *[AIS34]*:

- Examine sources publicly available.
- Conduct a methodical analysis of TOE evidence including the ETR for composition *[IC-ETRfC]* and the TOE implementation representation.

The vulnerability analysis gave rise to two perturbation and one side-channel penetration tests.

2.6.3 Test Configuration

Developer's testing has been performed on the TOE as defined in 2.1, that is on J-Tacho v1.2.6.

Evaluator's penetration testing has been performed on J-Tacho v1.2.4 followed by the review of the changes introduced by subsequent versions J-Tacho v1.2.5 and v1.2.6. The evaluator concluded that the changes did not add any potential vulnerability and that the testing results obtained on J-Tacho v1.2.4 are valid for the TOE.

2.6.4 Testing Results

The testing activities, including the 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 produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and technical specifications.

No exploitable vulnerabilities were found with the independent penetration tests. No residual vulnerabilities were found.

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 public domain, i.e. from the current best cryptanalytic attacks published, has been considered. The strength of the implementation of the cryptographic functionality used by the TOE has been assessed as part of the evaluation of the NESLib 6.2.1 (see *[IC-CERT]*).

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential": The TOE uses cryptographic primitives with security level lower than 100 bits, namely two-key TDES, 1024-bit RSA and SHA-1. The usage of such cryptographic primitives is required by the EU regulation *[EU-TACH]* for backward compatibility with 1st Generation tachograph cards. This is compliant with NSCIB Scheme Interpretation *[NSI_08]* since the TOE does not support composition on top of it.

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).

2.7 Re-used evaluation results

The sites involved in the development and production of the IC were re-used by composition through the IC certificate *[IC-CERT]*.

The development and production of the TOE's embedded software have been performed in STMicroelectronics site in Marcianise, Italy. The Site Technical Audit Report *[STAR]* for Marcianise has been re-used to fulfil ALC assurance requirements.

No site has been visited as part of this evaluation. The ALC reuse process has been performed according to NSCIB internal procedures.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number J-Tacho v1.2.6, which refers to the hardware and software components identified in section 2.1.

2.9 Results of the Evaluation

The evaluation laboratory documented their evaluation results in the *[ETR]*[3], which references the developer evidences.

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

Based on the above evaluation results the evaluation laboratory concluded that J-Tacho v1.2.6 meets the requirements of EAL 4 augmented with ATE_DPT.2 and AVA_VAN.5 as required in the Security Target *[ST]*, which is strictly conformant with the Protection Profile *[PP-TACH]*.

2.10 Comments/Recommendations

Certain aspects of the TOE's security functionality 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 as described in section 2.5.

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 their risk management process. In order for the evolution of attack methods and techniques to be covered, the process should define the period of time until a re-assessment of 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 for satisfying the AVA_VAN.5 "high attack potential". In order to be protected against attackers with a "high attack potential", sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

[3] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The STM J-Tacho Security Target, rev. F *[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:

DES	Data Encryption Standard
IC	Integrated Circuit
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

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

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013 (controlled distribution).

[JIL-COMP] Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, Joint Interpretation Library, May 2018.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[NSI_08] NSCIB Scheme Instruction 08, Performing Testing, Version 2.4, 1 June 2018.

[EU-TACH] [EU – 2016/799] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components.

[EU – 2018/502] Commission Implementing Regulation (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components.

[EU – 1360/2002] Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex 1B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71).

[PP-TACH] Digital Tachograph – Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091, Version 1.0, 9 May 2017.

[IC-ETRfC] ETR Lite for Composition Elixir 3 Project, version 1.3.

[IC-CERT] Rapport de certification ANSSI-CC-2019/12. ST31G480 D01 including optional cryptographic library NESLIB v6.2.1, and optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6

[ST] STM J-Tacho Security Target, rev. F.

[ST-Lite] STM J-Tacho, Security Target Public Version, rev. B.

[AGD_OPE] J-TACHO – Operational Procedure, rev. 1, 27 March 2019

[AGD_PRE] J-TACHO – Preparative Procedure, rev. 1, 28 March 2019

[ETR] Evaluation Technical Report STM J-Tacho – EAL4+, ref. 19-RPT-221, v2.0, 8 April 2019. Replaced by 19-RPT-221 v3.0, dated 16 April 2019, which fixes some typographical errors.

(This is the end of this report).