Certification Report

J-Tacho v.1.3.1

Sponsor and developer:	***ST Microelectronics S.r.l*** **Zona Industriale Marcianise SUD,** **81025 Marcianise (CE),** **Italy**
Evaluation facility:	***Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-222356-CR2**
Report version:	**2**
Project number:	**222356**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**28 July 2021**
Number of pages:	**12**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

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

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the J-Tacho v.1.3.1. The developer of the J-Tacho v.1.3.1 is ST Microelectronics S.r.l located in Marcianise, Italy and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a composite TOE, consisting of a Java Card Platform (including the native operating system), a library which provides cryptographic functions, and an underlying platform, which is a secure microcontroller and the Tachograph application package.

The composite TOE is a Tachograph Card, which can be configured as a driver card, workshop card, control card or company card in accordance with the EU regulation for tachograph cards. The TOE supports both 1st and 2nd generation tachograph application functionalities.

The OS part of the TOE is compliant with the Java Card 3.0.4 and GlobalPlatform 2.2.1 standards which provide a set of APIs and technologies to perform in a secure way the operations involved in the management of the applications hosted by the card. However this functionality is not claimed in the Security Target. As J-TACHO is a closed product, the card content management interface is permanently disabled before card delivery, so at the end of life cycle phase 5. After TOE delivery GP functionality is only available for the purpose of TOE Identification.

The cryptographic library used by the TOE is part of the certified IC. The eventual plastic card is outside the scope of the evaluation.

The TOE was evaluated initially by Brightsight B.V. located in Delft, The Netherlands and was certified on 18th April 2019. The re-evaluation of the TOE has also been conducted by Brightsight B.V. and was completed on 05 July 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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

The major changes are that the underlying hardware platform, the ST31G480 D02 was re-assessed on July 23rd 2020 as reported in *[SUR]*. The re-assessed hardware includes the optional NesLib crypto library version 6.2.1 that is also used by the J-Tacho. The changes in the hardware re-certification were taken into account for this J-Tacho re-certification.

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 J-Tacho v.1.3.1, 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 v.1.3.1 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 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]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will

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

be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the J-Tacho v.1.3.1 from ST Microelectronics S.r.l located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST31G480 IC	Version D01
Software	J-SAFE3 Java Card Platform (including the native Operating System)	V1.3.1
	J-TACHO Tachograph Application package	v1.13

To ensure secure usage a set of guidance documents is provided, together with the J-Tacho v.1.3.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

J-Tacho v1.3.1 is a contact Tachograph card that implements the EU directive *[EU_2016_165]*, 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 v.1.3.1 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

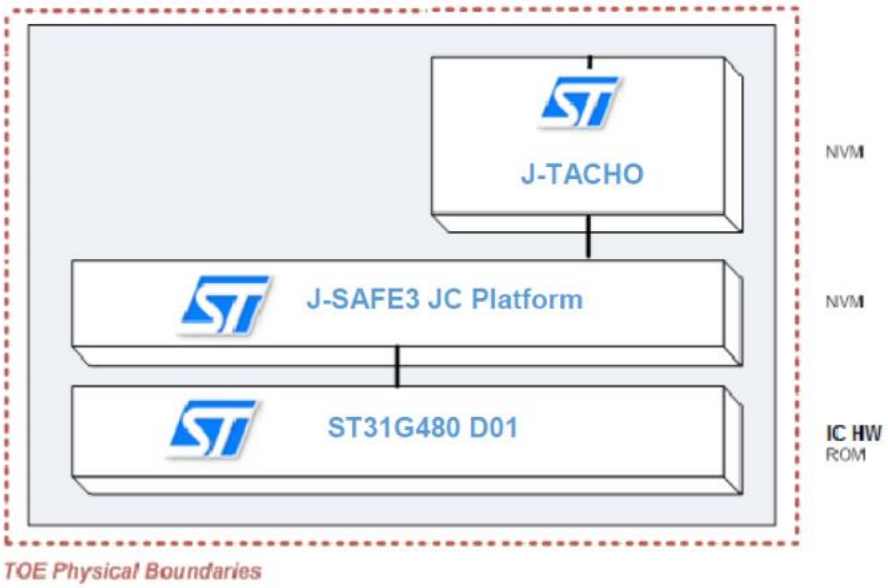
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 7.6.2 of the *[STLite]*.

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.

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 the figure below. The TOE does not allow card content operations (load/delete applications) in the end-usage phase.



TOE Physical Boundaries

2.5 Documentation

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

Identifier	Version
J-TACHO – Preparative Procedure	Rev. E, 11-5-2021
J-TACHO – Operational User Guidance	Rev. D, 11-5-2021

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 developer ran the UL Smart Tachograph test suite with focus on the externally available tachograph functionality. Successful execution of this test suite satisfies the minimal functional test requirements described in Appendix 9 of Annex 1C of *[EU_2016_165]*.

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

Besides the repetition of developer tests, the evaluator defined spot-checks on the calculation of code-coverage as used by the developer to demonstrate their completeness of testing. As developer functional testing was rigorous, no additional tests were defined by the evaluator.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD, no potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on version 1.2.4 of the TOE. During this attack oriented analysis the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in [JIL-AP]. An important source for assurance against attacks in this step is the [HW-ETRfC] of the underlying platform; no additional potential vulnerabilities were concluded from this.
- Delta implementation review rounds were performed for later versions 1.2.5, 1.2.6 and 1.3.1 of the TOE. Changes were found to be functional and did not result in additional potential vulnerabilities.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 50% of the total time was spent on Perturbation attacks and 50% 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.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number J-Tacho v.1.3.1 as described in the identification part of this report.

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the J-Tacho v.1.3.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ATE_DPT.2 and AVA_VAN.5** . 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]*.

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 STM J-Tacho, Security Target, rev H, 07 June 2021 *[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:

DES	Data Encryption Standard
IC	Integrated Circuit
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
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
[ETR]	Evaluation Technical Report “STM J-TACHO” – EAL4+, 19-RPT-211, Version 4.0, 6 July 2021
[EU_2016_165]	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.
[HW-CERT]	Rapport de certification ANSSI-CC-2019/12 ST31G480 D01 including optional cryptographic library NESLIB v6.2.1, and optional technologies MIFARE DESFirew EV1 v4.8.12 and MIFARE Plus X v2.4.6, 05 March 2019
[HW-ETRfC]	ETR Lite for Composition Elixir 3 Project, version 1.3, 15 February 2019
[SUR]	Rapport de surveillance, ANSSI-CC-2019/12-S01, ST31G480 D02, 23 July 2020
[HW-ST]	ST31G480 D01 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target for composition, rev D01.3, October 2018
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Protection Profile Machine Digital Tachograph – Tachograph Card (TC PP) - Version 1.0, 19 May 2017 registered under the reference BSI-CC-PP-0091-2017.
[ST]	STM J-Tacho, Security Target, rev H, 07 June 2021
[ST-lite]	STM J-Tacho, Security Target Public Version, rev D, 07 June 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report J-Tacho v.1.3.1, 21-RPT-500 STAR Marcianise v2.0, Version 2.0, 6 July 2021

(This is the end of this report.)