Certification Report

J-TACHOG2V2 v.1.0.2

Sponsor and developer: ***ST Microelectronics S.r.l***
Zona Industriale Marcianise SUD
81025 Marcianise (CE)
Italy

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

Report number: **NSCIB-CC-0635023-CR**

Report version: **1**

Project number: **0635023**

Author(s): **Kjartan Jæger Kvassnes**

Date: **12 December 2022**

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.

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-TACHOG2V2 v.1.0.2. The developer of the J-TACHOG2V2 v.1.0.2 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 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 according to *[EU_2016_165]* and *[EU_2021_1228]*.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 12 December 2022 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-TACHOG2V2 v.1.0.2, 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-TACHOG2V2 v.1.0.2 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 ALC_DVS.2 (Sufficiency of security measures), ALC_DPT.2 (Testing: security enforcing module) 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 be listed on the NSCIB Certified Products list. 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 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the J-TACHOG2V2 v.1.0.2 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	ST31P450	B04
Software	J-TACHOG2V2 Java Card Platform (including the native Operating System)	v1.0.2
	J-TACHOG2V2 Digital tachograph card Application	package version 1.3.1

To ensure secure usage a set of guidance documents is provided, together with the J-TACHOG2V2 v.1.0.2. For details, see section 2.5 “Documentation” of this report.

The ST31P450 B04 identified in *[HW-MAINT]* is the same version as the one mentioned in the IC certificate *[HW-CERT]* which was confirmed to be identical for the scope of the composite TOE.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 5.1.9 or *[ST-Lite]*, chapter 5.1.9.

2.2 Security Policy

The TOE has the following features:

- Storage of card identification and user identification data. This data is used by the Vehicle Unit to identify the human user, provide functions and data access rights accordingly;
- Storage of data related to the human user, among which are user activities data, events and faults data and control activities
- Preservation of card identification data and user identification data stored during the card personalization process;
- Safe storage of user data stored in the card by Vehicle Units
- Allowance of specific write operations onto the cards to only an authenticated Vehicle Units
- Protection of data that is stored in such a way as to prevent unauthorized access to and manipulation of the data, and to detect any such attempts;
- Protection of the integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

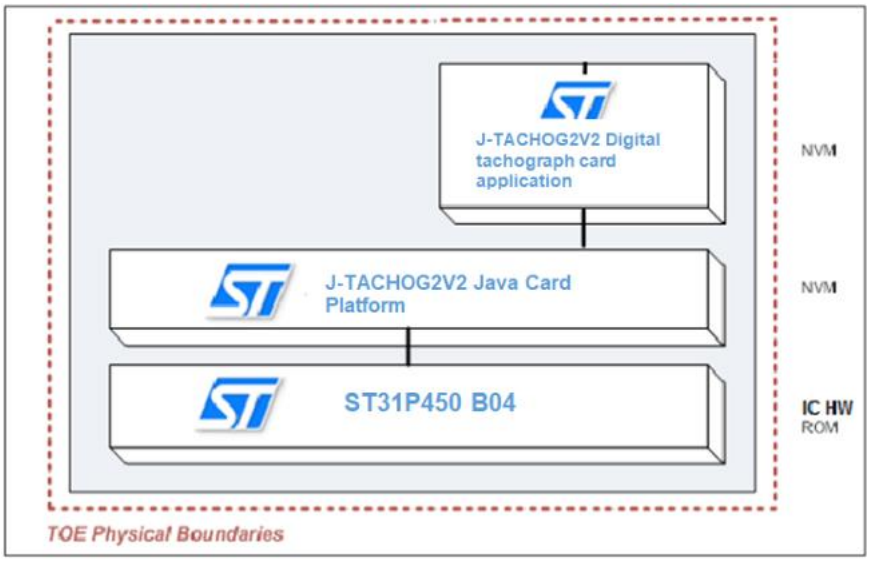
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 7.6.2 of the *[ST]*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

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

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



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-TACHOG2V2 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.

2.5 Documentation

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

Identifier	Version
[UG-PRE] J-TACHOG2V2 – Preparative Procedure, dated 7 September 2022	Revision B
[UG-OPE] J-TACHOG2V2 – Operational User Guidance, dated 26 August 2022	Revision B

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 performed extensive testing of TSFI´s for 1st and 2nd generation functionalities for all tachograph configurations. These where the same configurations as defined in section 2.6.3 which covers the expected behaviour defined in *[EU_2016_165]* and *[EU_2021_1228]*. The tests cover all security functions and aspects of the TSF. Testing is performed during development as well as for acceptance/release. The developer used a set of test suites (industry standard and proprietary ones)

and tools to test the TOE as well as an emulator and simulator as some tests could only be performed in such environment.

Tests are performed as “System Test” using “Black Box” approach. If needed, “Grey Box” approach is also used. Functional requirements from Tachograph specification have been verified using a standardized tool. Security requirements have been covered by additional test cases defined by the developer, and by the test tool where the test cases are adequate to verify the security requirements (in the operational stage).

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 tachograph test suite.

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 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.
- 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, 100% of the total time was spent on Perturbation attacks.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- STM J-TACHOG2V2 v.1.0.2
  - Driver configuration
  - Control configuration
  - Workshop configuration
  - Company configuration

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There has been no reuse of the ALC aspects for the sites involved in the software component of the TOE. 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-TACHOG2V2 v.1.0.2.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the J-TACHOG2V2 v.1.0.2, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, 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_0091]*.

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>, which are out of scope as there are no security claims relating to these.

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).

[2] 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.

3 Security Target

The J-TACHOG2V2 Security Target Common Criteria for IT security evaluation, Revision F, Dated 30 November 2022 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation
API	Access Control List
IC	Integrated Circuit
JIL	Joint Interpretation Library

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018 Must be retained for all composite smartcard TOEs
[ETR]	Evaluation Technical Report “J-TACHOG2V2 v.1.0.2” – EAL4+, 22-RPT-1016, Version 6.0, 12 December 2022
[HW-CERT]	Rapport de certification ANSSI-CC-2020/05 ST31P450 B02 including optional cryptographic library NesLib 6.4.7, and optional technology MIFARE Plus® EV1 version 1.1.2, dated February 18, 2020
[HW-MAINT]	Rapport de maintenance ANSSI-CC-2020/05-M01 ST31P450 B04 including optional cryptographic library NESLIB version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2, February 2022
[HW-ETRfC]	THALES evaluation Technical Report for composite evaluation Project: MANDALA with library Surveillance, v2.0, January 2022
[HW-ST]	ST31P450 B04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFIRE EV1 and MIFARE PLUS X Security Target for composition, Rev B04.1, August 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[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_0091]	Digital Tachograph – Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091-2017, Version 1.0, 19 May 2017
[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.
[EU_2021_1228]	COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components.
[ST]	J-TACHOG2V2 Security Target Common Criteria for IT security evaluation, Revision F, Dated 30 November 2022
[ST-lite]	J-TACHOG2V2 Security Target Public Version Common Criteria for IT security evaluation, Revision B, Dated 30 November 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

[STAR] STAR Marcianise, J-TACHOG2V2 v.1.0.2, [22-RPT-1220], 1.0, 28 October 2022

(This is the end of this report.)