Reference: 2018-9-INF-2874-v2
Target: Limitada al expediente
Date: 27/04/2023

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-9**
TOE	**Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43**
Applicant	**26018748 - Lesikar, a.s.**

References

[EXT-3856] Certification request

[EXT-5343] Evaluation Technical Report version M0

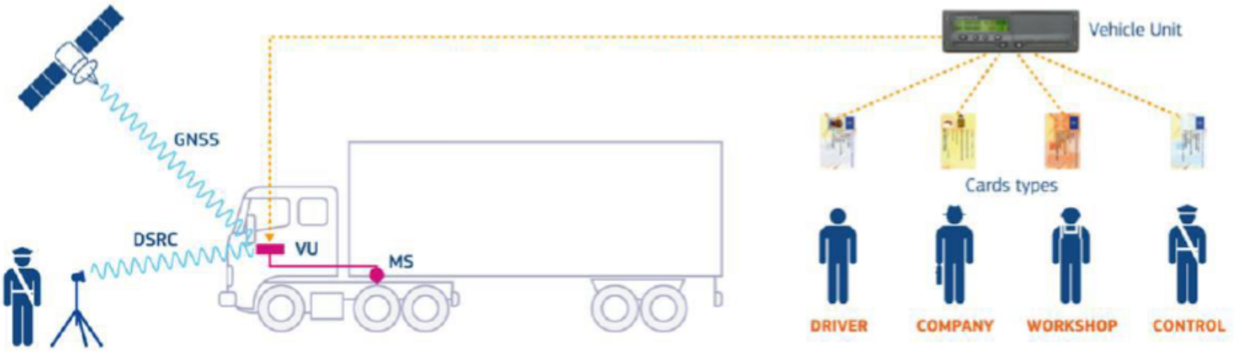
Certification report of the product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43, as requested in [EXT-3856] dated 12/03/2018, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5343] received on 23/09/2019.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43.

The smart digital tachograph as described on the European Commission web site[1]:



The certified TOE is the motion sensor (MS in the picture). The motion sensor is intended to be installed in road transport vehicles. Its purpose is to provide a vehicle unit (VU) with secured motion data representative of vehicle's speed and distance travelled.

Developer/manufacturer: Lesikar, a.s.

Sponsor: Lesikar, a.s.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories

Protection Profile: Digital Tachograph - Motion Sensor (MS PP) v1.0 (BSI-CC-PP-0093) with strict conformance.

Evaluation Level: Common Criteria v3.1 r5 - EAL4 + ATE_DPT.2 + AVA_VAN.5.

Evaluation end date: 23/09/2019.

All the assurance components required by the evaluation level EAL4 (augmented with ATE_DPT.2 and AVA_VAN.5) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, as defined by the Common Criteria v3.1 r5 and the CEM v3.1 r5.

Considering the obtained evidences during the instruction of the certification request of the product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43, a positive resolution is proposed.

[1] European Commission – Joint Research Center – Digital Tachograph https://dtc.jrc.ec.europa.eu/dtc_smart_tachograph.php

TOE SUMMARY

The certified TOE is a motion sensor for a digital tachograph. The intended use of the sensor is as a motion sensor inside the gear box of a vehicle to fulfil the EU regulations [CIR-EU-2016/799] (Annex 1C included) about using digital tachographs as recording equipment in road transport. The motion sensor is intended to be used together with a vehicle unit and smart cards for the drivers.

The motion sensor is intended to be installed in road transport vehicles. Its purpose is to provide a vehicle unit (VU) with secured motion data representative of vehicle's speed and distance travelled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement can be representative of vehicle's speed or distance travelled. It is located in the vehicle's gear box. In its operational mode, the motion sensor is connected to a VU.

The security functionality of the motion sensor provides the following security features:

- Mutual authentication between the MS and the VU during pairing.
- Authentication failure handling.
- Unforgeable user identification and authentication before any action.
- The import of a session key, KS, from the VU during pairing.
- The export of a pairing key, KP, to the VU during pairing.
- Destruction of old session key by replacement with new session key.
- Destruction of old session key by replacement with new session key.
- Stored data integrity monitoring.
- Data exchange integrity for MS data import and export.
- Encryption and decryption of data, with the session key, for the transmission of data between the MS and the VU.
- Access control to TOE functions.
- Information flow control for MS data import and export.
- The TSF provides a protective casing capable of being sealed that together with the security seal provide physical tampering detection.
- The TSF provides protection against magnetic fields tampering by the use of two sensors and special processing.
- Security audit data generation.
- TSF self-testing.
- Failure with preservation of secure state.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional components ATE_DPT.2 and AVA_VAN.5, according to Common Criteria v3.1 r5.

Requirement Class	**Requirement Component**
Security Target (ASE)	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
Design (ADV)	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV.IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic Modular Design
Guidance (AGD)	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Life cycle (ALC)	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DVS.1 Identification of security measures ALC_TAT.1 Well-defined development tools ALC_DEL.1 Delivery procedures ALC_LCD.1 Developer defined life-cycle model
Testing (ATE)	ATE_COV.2 Analysis of coverage ATE_DPT.2 Testing: security enforcing modules ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample

Vulnerability assessment (AVA)	AVA_VAN.5 Advanced methodical vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 r5:

Requirement Class	**Requirement Component**
Security audit (FAU)	GEN.1 Audit data generation STG.1 Protected audit trail storage STG.4: Prevention of audit data loss
Cryptographic Support (FCS)	CKM.4/1 Cryptographic key destruction CKM.4/2 Cryptographic key destruction COP.1/1:AES Cryptographic operation COP.1/2:TDES Cryptographic operation
User data protection (FDP)	ACC.1 Subset access control ACF.1: Security attribute based access control ETC.1: Export of user data without security attributes ETC.2: Export of user data with security attributes ITC.1: Import of user data without security attributes SDI.2: Stored data integrity monitoring and action
Identification and authentication (FIA)	AFL.1: Authentication failure handling ATD.1: User attribute definition UAU.2/1: User authentication before any action UAU.2/2: User authentication before any action UAU.3: Unforgeable authentication UID.2: User identification before any action
Protection of the TSF (FPT)	FLS.1: Failure with preservation of secure state PHP.2: Notification of physical attack PHP.3/1: Resistance to physical attack

	PHP.3/2: Resistance to physical attack TDC.1/1: Inter-TSF basic TSF data consistency TDC.1/2: Inter-TSF basic TSF data consistency TST.1: TSF testing
Resource Utilization (FRU)	PRS.1 Limited priority of service
Trusted path/channels (FTP)	ITC.1: Inter-TSF trusted channel

IDENTIFICATION

Product: Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43

Security Target: Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target version 0.16, 2019-09-11.

Protection Profile: Digital Tachograph - Motion Sensor (MS PP) v1.0 (BSI-CC-PP-0093) with strict conformance.

Evaluation Level: Common Criteria v3.1 r5 - EAL4 + ATE_DPT.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The complete list of security policies can be found in the Security Target, section 3.4.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The complete list of assumptions can be found in the Security Target, section 3.5.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43, although the agents implementing attacks have the attack potential according to the attack potential **high** of EAL4 + AVA_VAN.5 and ATE_DPT.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The complete list of threats can be found in the Security Target, section 3.3.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized in the Security Target, in the section 4.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

The security functionality of the motion sensor provides the following security features:

- Mutual authentication between the MS and the VU during pairing.
- Authentication failure handling.
- Unforgeable user identification and authentication before any action.
- The import of a session key, KS, from the VU during pairing.
- The export of a pairing key, KP, to the VU during pairing.
- Destruction of old session key by replacement with new session key.
- Destruction of old session key by replacement with new session key.
- Stored data integrity monitoring.
- Data exchange integrity for MS data import and export.
- Encryption and decryption of data, with the session key, for the transmission of data between the MS and the VU.
- Access control to TOE functions.
- Information flow control for MS data import and export.
- The TSF provides a protective casing capable of being sealed that together with the security seal provide physical tampering detection.
- The TSF provides protection against magnetic fields tampering by the use of two sensors and special processing.

- Security audit data generation.
- TSF self-testing.
- Failure with preservation of secure state.

The TOE provides these interfaces:

- Mechanical interface between the sensor element and the gear box.
- The [ISO15170-1] connector to the VU and the power according to [ISO 16844-3:2004]. Four pins:
    - 1: Positive supply
    - 2: Battery minus
    - 3: Speed signal, real-time (no integrity protection or authentication)
    - 4: Data signal, in/out

More information regarding the logical scope of the TOE can be found in the Security Target, in the section 1.4.2.

PHYSICAL ARCHITECTURE

The physical scope of the TOE includes the following:

- TOE hardware, delivered by courier delivery:
    - The whole motion sensor including the casing.
        - Sensor for digital tachograph LESIKAR TACH3, models: M171, M171.1, M172, M173, M174, M175, M176 and M193.
- The real-time speed signal on pin 3 is depending upon the secured data channel on pin 4 for data integrity. Only the data signal in/out (pin 4) has integrity and confidentiality protection by the use of cryptographic support. The real-time speed signal (pin 3) has not. I.e. trusted sensor data is provided only on pin 4. The VU is able to use the real-time signal on pin 3 by periodically comparing the data to the secured data on pin 4.
- TOE software (embedded in the hardware and therefore delivered with it):
    - The motion sensor software. This is a firmware software entirely and specifically developed by Lesikar for the motion sensor.
    - User data.
    - TSF data (security data).
- The TOE documentation, delivered by PGP-encrypted e-mail.

- The TOE preparative procedures (Preparative Procedures - Installation Manual of LESIKAR TACH3, version 0.11, in digital format as a PDF file).
- The TOE operational guidance (LESIKAR TACH 3 - Operational Guidance, version 0.5, in digital format as a PDF file).

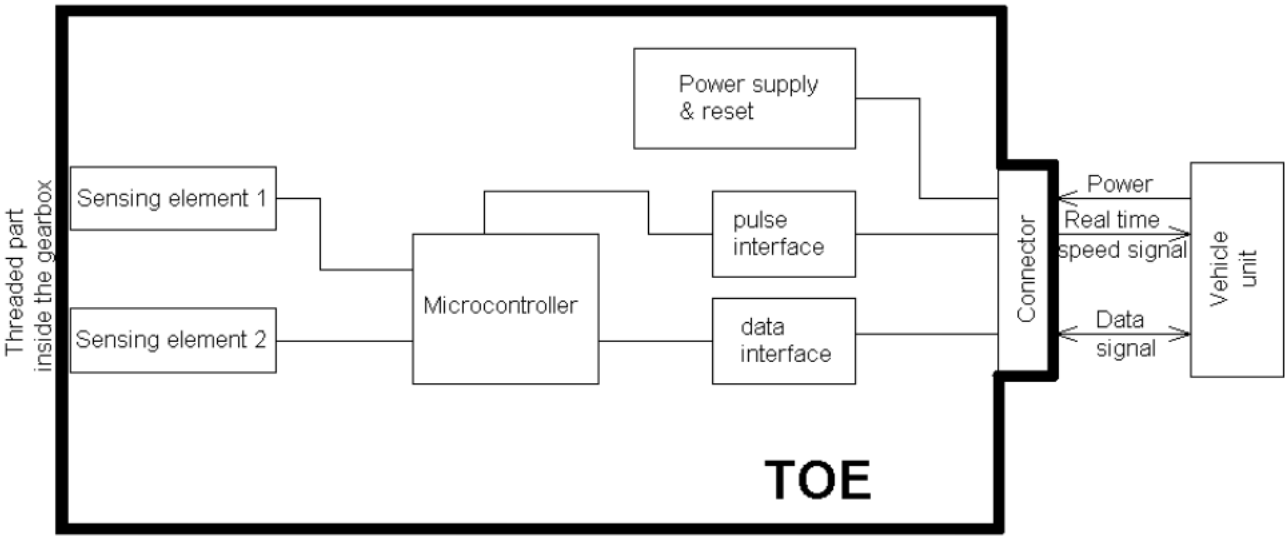


Figure 1: The schematics for the Sensor for digital tachograph LESIKAR TACH3

DOCUMENTS

The product includes the following documents that shall be delivered by PGP-encrypted e-mail and made available together to the users of the evaluated version.

- The TOE preparative procedures (Preparative Procedures - Installation Manual of LESIKAR TACH3, version 0.11, in digital format as a PDF file).
- The TOE operational guidance (LESIKAR TACH 3 - Operational Guidance, version 0.5, in digital format as a PDF file).

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated a sample of the developer functional tests in the developer premises. In addition, the lab has devised an independent test plan, which covers the TOE interfaces. These tests complements the vendor test plan for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer. By following this testing strategy, all TSFIs and SFRs are covered by testing TSFIs and SFRs are covered by testing.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The evaluated TOE is:

- TOE Name: Motion Sensor for Digital (smart) Tachographs Lesikar TACH3
- TOE Developer: Lesikar
- TOE Version: HW version 02, SW version 03 r43

The sensor LESIKAR TACH3 has following models (they differ only in length of case): M171, M171.1, M172, M173, M174, M175, M176 and M193. The chosen model to be evaluated has been the M173. All the installation and configuration process is described in the guidance documents.

The test configuration comprised the following components:

- sensor TACH3 type M173
- sensor holder with adjustable distance from the cogwheel
- a cogwheel connected to the engine with rotation regulation
- stabilized power supply (Statron type 2229)
- oscilloscope (Escort 300 C 20 MHz)
- rotation counters
- reference sensor (Lesikar M068 rotational sensor)

Additional components applicable only to some test cases are:

- computer with testing software
- development environment Ride7 version 7.40.12.014
- Vehicle Unit

EVALUATION RESULTS

The product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 HW version 02, SW version 03 r43 has been evaluated against the Security Target: Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target version 0.16, 2019-09-11.

All the assurance components required by the evaluation level EAL4 + ATE_DPT.2 + AVA_VAN.5 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ATE_DPT.2 + AVA_VAN.5, as defined by the Common Criteria v3.1 r5 and the CEM v3.1 r5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

There is no additional recommendation from the evaluation team in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

Since all the classes of the evaluation have a Pass verdict, the overall evaluation verdict is Pass.

Therefore, from the Laboratory point of view, the product is considered compliant with the CC standard with an assurance level of EAL4 augmented by ATE_DPT.2 and AVA_VAN.5.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product, a positive resolution is proposed.

(Comment added on 27/04/2023 to this certification report): The evaluation and certification of the TOE were performed before the publication of the Protection Profile clarification (JIL Tachograph MS PP Clarification v1.0, July 2022) in the SOG-IS website. Therefore, it is up to the users’ consideration the impact assessment of this PP clarification in their use cases.

Moreover, the user guidance must be read and understood in order to operate the TOE in an adequate and secure manner according to the security target.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[CIR-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

[ISO15170-1] ISO 15170-1:2001 Road vehicles – Four-pole electrical connectors with pins and twist lock – Part 1: Dimensions and classes of application.

[BSI-CC-PP-0093] Digital Tachograph - Motion Sensor Protection Profile (MS PP) v1.0.

[CCDB-2006-04-004] ST sanitising for publication

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target version 0.16, 2019-09-11.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target Lite version 1.0, 2019-09-24.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.
The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.