Swedish Certification Body for IT Security

Certification Report Lesikar TACH 2

Issue: 1.0, 2016-July-01

Authorisation: Imre Juhász, Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) consists of the hardware and firmware that together constitutes the motion sensor TACH 2 from Lesikar a.s. The TOE is a motion sensor which is meant to be a part of a tachograph system in accordance with the EU regulation [Regulation_2013]. 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 TOE’s main functionality is to provide VU with accurate and unforgeable information of the current speed of the vehicle. The TOE is placed inside a protective casing which is attached to the gearbox of the vehicle. The TOE is then paired with a specific VU, resulting in an exchange of a mutual encryption key. After the paring is made sensitive communication, only initiated by the VU, are conducted through the encryption of messages. Periodic integrity checks of stored data and software are conducted by the TOE. The TOE has a patented solution which protects the sensor from disturbances due to magnetic fields. In order to ensure full operability in a well-defined and correct manner with different VUs the TOE has been designed to comply with the requirements of [ISO16844-3].

The strength of the cryptographic algorithm was not rated in the course of this evaluation as they are defined in [Regulation_ 2013] and implemented accordingly.

The TOE is delivered as a fully functional sensor placed within a protective casing. The TOE is interfaced using a connector specified in [ISO15170-1]. In order to use the TOE a certified workshop must perform the paring with a VU also certified under the Common Criteria (CC) as specified by the EU regulation.

No conformance claims to any protection profile is made for the TACH 2 sensor. Although there is no PP to which the ST is claimed to be conformant to, the ST covers all requirements in the motion sensor generic ITSEC ST for motion sensor, vehicle unit and tachograph card as contained in [Annex1B_App10].

There are four assumptions made in the ST regarding the secure usage and environment for the TACH 2 sensor. The TOE relies on these assumptions being met in order to counter the eleven threats, and to fulfill the two organisational security policies (OSP) in the ST. The assumptions, the threats and the organisational security policies are described in chapter 4 Assumptions and Clarification of scope.

The evaluation has been performed by Combitech AB, and was completed on 2106-06-29. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL4, augmented by ATE_DPT.2 and AVA_VAN.4.

Combitech AB AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 4 + ATE_DPT.2 and AVA_VAN.4.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be reassessed if required and the sponsor applies for the certified product being monitored within the certificate surveillance program of the CSEC Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2015001
Name and version of the certified IT product	Sensor for digital tachograph LESIKAR TACH2 Models: M071, M071.1, M072, M073, M074, M075 and M076. The difference between the listed models are the length of the casing. Firmware and hardware versions: SW version 02, HW version 04
Security Target Identification	Security Target – Sensor for digital tachograph LESIKAR TACH2 [ST]
EAL	EAL4+ ATE_DPT.2 and AVA_VAN.4. *CCRA recognition for components up to EAL 2 and ATE_DPT.2 and AVA_VAN.4 only*
Sponsor	Lesikar a.s.
Developer	Lesikar a.s.
ITSEF	Combitech AB
Common Criteria version	3.1, revision 4
CEM version	3.1, revision 4
Certification date	*2016-07-01*

3 Security Policy

The TOE consists of eight security functions. Below is a short description of each of them. For more information, see Security Target [ST]

Audit Generation

A security audit record is generated when any type of security error in the MS occurs; e.g. data integrity error, authorisation error, or communication error. The data of the audit record is written to the MS NVRAM and the flag NARA (New Audit Record Available) is set in the next communication frame. When the VU detects that the NARA flag is set, it requests the new audit record. The sensor is not responsible for keeping the generated audit events but passes these on to the vehicle unit.

Access control

Access controls to TOE functions. All access to the TOE are possible after the paring. After the paring is made all access are conducted through the encryption of messages.

Identification and Authentication

Mutual authentication between the MS and the VU during pairing. Processed according to the ISO 16844-3, section 7.4.2. Authentication failure handling:

- After 20 unsuccessful authorisation attempts the TOE generates an audit record (error message). It is stored in the sensor memory (NVRAM) until the MS is properly connected to the authorised VU and then the MS sends its error file to the VU.
- After 20 unsuccessful authorisation attempts the MS also stops responding, until the authorised VU is connected (blocks unauthorised key testing / hacking).
- Unforgeable user identification and authentication before any action.

Crypto

Crypto, including cryptographic key distribution, import and destruction, encryption and decryption and data exchange integrity.

- The import of a session key (KS) from the VU during pairing. Processed according to the ISO 16844-3, section 7.4.6.
- The export of a pairing key (KP) to the VU during pairing. Processed according to the ISO 16844-3, section 7.4.4.3.
- Destruction of old session key by replacement with new session key. The old session key is replaced with the new session key when the MS is successfully paired with a VU.
- Data exchange integrity for MS data import and export. MS data that is exported is first checked for integrity of all the data, and then every frame sent has a checksum in accordance with the ISO 16844-3.
- Encryption and decryption of data, with the session key, for the transmission of data between the MS and the VU.

Flow

Information flow control for MS data import and export.

The VU is always the communication master. The VU sends a request and the MS responds, if the VU is authorized.

Integrity

Integrity protection, checksums.

- Stored data integrity monitoring. Integrity checks are made on stored data during start-up and periodically during operation by the use of checksums.
- TSF self-testing. Stored data and software code are checked for integrity during start-up and periodically during operation by the use of checksums.

Failure with preservation of secure state.

When a self-test failure occurs, the MS stops the secured data communication on pin 4 and continues the direct speed pulse generation on pin 3. An audit record is then generated and stored.

Magnetic Fields

Resistance from tampering with magnetic fields is achieved by using two sensor elements.

Casing

The sensor is placed in a protective casing which are then inserted into the gearbox of the vehicle and then sealed.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following assumption about the usage are made:

A.Approved_Workshops: The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections and repairs.

A.Controls: Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).

A.Regular_Inspections Recording: equipment will be periodically inspected and calibrated.

A.Seal: A security seal is used to seal the TOE and thereby its mechanical interface, to the gearbox. The security seal is applied during installation of the motion sensor in the vehicle. The security seal used to seal the TOE cannot be broken or removed and re-attached without the user or the inspector being able to detect the manipulation; and thereby provide the means of detecting physical tampering with the mechanical interface.

4.2 Clarification of Scope

Two categories of threat agents are defined in the Security Target:

- The threat agent “Malicious user” is any user aiming for compromising the security of the tachograph system. The attack potential of the malicious users may vary from basic attack potential to high attack potential.
- The threat agent “Malfunction” is the cause of any fault in hardware or software. Since it is not a conscious threat agent, the attack potential would be related to the consequences of the adverse action.

The threats against the TOE defined in the Security Target are listed below:

- T.Access: Users could try to access functions not allowed to them
- T.Faults: Faults in hardware, software, communication procedures could place the motion sensor in unforeseen conditions compromising its security
- T.Environment: Users could compromise the motion sensor security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, …)
- T.Hardware: Users could try to modify motion sensor hardware
- T.Mechanical_Origin: Users could try to manipulate the motion sensor input (e.g. unscrewing from gearbox, …)
- T.Motion_Data: Users could try to modify the vehicle’s motion data (addition, modification, deletion, replay of signal)
- T.Power_Supply: Users could try to defeat the motion sensor security objectives by modifying (cutting, reducing, increasing) its power supply
- T.Security_Data: Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment
- T.Software: Users could try to modify motion sensor software
- T.Stored_Data: Users could try to modify stored data (security or user data).

- T.Magnetic_Fields: Users could try to tamper with motion detection using magnetic fields.

Two Organisational Security Policies are defined in the Security Target:

- OSP.Audit: The motion sensor must audit attempts to undermine system security and should trace them to associated entities.
- OSP.Processing: The motion sensor must ensure that processing of input to derive motion data is accurate

5 Architectural Information

5.1 TOE Design

5.1.1 Hardware

The TOE consists of two magnetic sensing elements, pulse coupler, microprocessor unit, reset & power supply unit, pulse interface, data interface and connector.

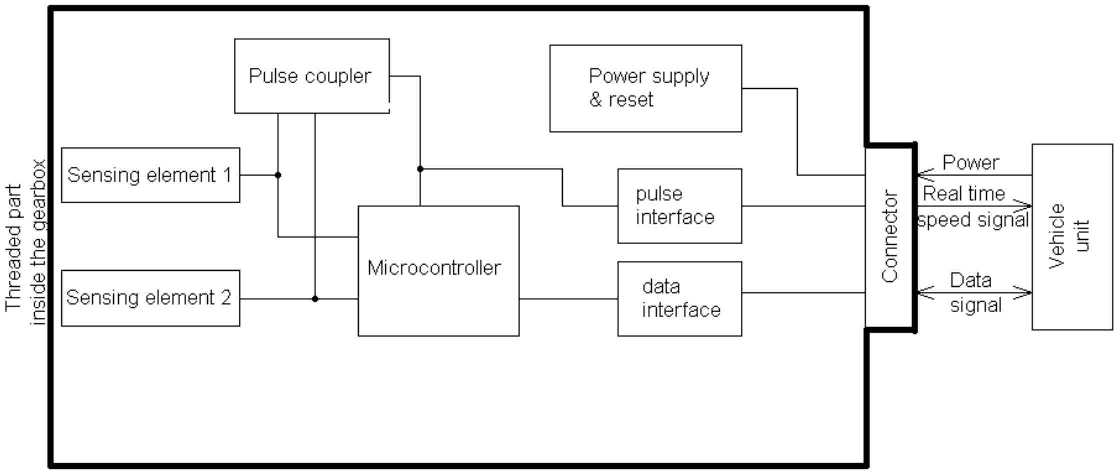

Figure 1, TOE hardware structure

Two magnetic sensing elements are placed in the threaded part intended to be facing cogged wheel inside the gearbox of the vehicle.

TOE is connected with the vehicle unit (tachograph), forming the logging system for the vehicle speed and distance data. TOE sends the actual speed through two signals, e.g. pulses and encrypted digital data signal. Speed pulses signal is essential for the real time performance of the system (real time speed displaying, high-density distance measuring), while the data signal is used for integrity check of the speed pulses signal. Data signal is encrypted according to the [ISO 16844-3]. By the usage of the two sensing elements according to patent WO 2014/ 135132 A1 the TOE is immune to the magnetic fields applied from outside environment to the TOE, at least one sensing element always should stays functional

Sensing element

Hall principle based self-adjusting digital output rotary position gear tooth sensor. Each sensing element is coupled with its bias magnet.

Pulse coupler

Hardware circuit, which couples both outputs to one output (edge coupled set-reset). This circuit is used to generate output signal (for pin 3) independent to the microprocessor. It is made from discrete components.

Microprocessor

Monolithic CMOS automotive grade single chip microprocessor with on chip RAM, FLASH, EEPROM memories.

Power & Reset circuitry

Low drop voltage stabilizer 5V and reset circuit, which generates reset signal when the serial bus (pin 4) is held down for longer time.

Data interface

Hardware decoupling circuit to connect and protect data signal on pin 4. Based on a few discrete components.

Pulse interface

Hardware decoupling circuit to connect and protect pulse signal on pin 3. Based on a few discrete components.

5.1.2 Software (firmware)

The TOE is interrupt driven; no real time operating system is used. Interrupt routines handle input from the Hall sensors, receiving and transmitting data over the UART interface. There are two “tick” functions checking and handling the input/output from the interrupt routines.

6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

1. Guidance Documentation – LESIKAR TACH2 [Guidance document]
2. Catalogue list LESIKAR TACH2 [Catalogue list]

7 IT Product Testing

The main part of the testing effort was performed at the developer site in the city of Tabor in the Czech republic.

Some parts of the penetration testing, mainly the SPA and DPA testing, was performed at the ITSEFs site in Växjö , Sweden

7.1 Developer Tests

The developer provided a test case set which includes a full coverage of all security functionality as well as functional testing of the TOE. The developer's testing covers the security functional behaviour of all TSFIs and SFRs.

The developer tests are divided into the following test groups:

- Test Group 1: Sensor Tests
- Test Group 2: VU Communication
- Test Group 3: Security Functions

7.2 Independent Evaluator Tests

The evaluator's independent tests were chosen to complement the developer's tests in covering as much of the security functional behavior of the TSFIs and SFRs.

The sampling was based upon the most important functions of the TOE. The tests that were repeated are the pairing, data transfer, the function of the magnetic sensor, voltage drop and all the tests of the security functions.

The repeated tests verified that the developer testing covered that:

- Pairing is performed correctly and that the TOE reaches the evaluated configuration.
- The data transfer between the sensor and the vehicle unit works as intended.
- That the MS handles different strength and variation of input voltage and currents.
- The sensitivity to interference of magnetic fields.

By the selection of the above the evaluator get a sufficient independent verification of both the basic TOE functions and a complete independent verification of the security functionalities present in the TOE.

No issues was identified during the execution of the independent tests.

7.3 Penetration Tests

The identified vulnerabilities were various attacks on the protocol, side channel attacks and manipulation of environmental variables. The evaluator focused the testing effort on four different types of possible attacks:

1. Interference and logical tampering
2. Bypass of security enforcement functionality
3. Physical tampering
4. Test of security functions

Three different test configurations were used in order to best utilize the testing effort.

Several different penetration tests were crafted in order to test the sensors capability to withstand different kinds of interference and logical tampering. Tests were executed focused on the used protocol including: flooding, fake synchronization, fake package format, different man-in-the-middle attacks and fuzzy-based protocol tests.

Several different penetration tests were crafted in order to test the sensors capability to withstand different kinds of physical tampering. The following tests were executed focused on alterations of environmental variables: Random magnetic field alteration using a magnet with 300mT, under-voltage, fault-injections using glitches.

Both Single power analysis and Differential power analysis penetration tests were executed in the area of side-channel attacks. Several tests were conducted with different number of traces and with some modifications for the test setup. None of the tests gave any proof of leakage.

All penetration testing had negative outcome, i.e. no vulnerabilities were found. The actual results of all test cases were consistent with the expected test results and all tests were judged to pass.

8 Evaluated Configuration

The TOE is the product in the operational stage ready for pairing. Before use, the TOE first needs to be installed in the vehicle by an approved and trusted fitter or workshop. After installation the approved workshop attach a security seal according to regulations. During pairing with a VU, mutual authentication occurs and the TOE also gets a session key from the VU that is used to encrypt the communication between the TOE and the VU. It is not possibly to repair the sensor if broken or malfunctioning. If needed, the sensor needs to be replaced and a new pairing needs to be completed.

8.1 Dependencies to Other Hardware, Firmware and Software

The TOE is self-contained and the TSF does not rely on any non-TOE hardware, software or firmware for its security functionality. However, to be able to function as part of a tachograph system in accordance with the EU regulation , the motion sensor, TOE needs to be used together with these non-TOE components:

- A transport vehicle with a gear box from which the motion data is derived.
- A vehicle unit, the only component intended to communicate with the TOE.
- A smart card for the vehicle unit – one for each driver
- A smart card for the workshop, needed for calibration of the VU and for pairing the VU with the motion sensor (MS).
- A security seal is used to seal the mechanical interface of the TOE to the gearbox. The security seal is applied during installation of the motion sensor in the vehicle.

Cryptographic keys need to be generated, distributed and inserted in different parts of the tachograph system in accordance with the regulation. The following keys are generated, distributed and handled by the certification authorities. They are not part of the TOE:

- The master key, Km. Km = KmVU XOR KmWC. Km is not stored in any part of the tachograph system.
- KID (derived from Km). KID is not stored in any part of the tachograph system.
- KVU (The part of Km put in the VU)
- KWC (The part of the KM put in the smart card for the workshop)

9 Results of the Evaluation

The verdicts for the assurance classes and components are summarized in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	Pass
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security Problem Definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Authorization controls	ALC_CMC.4	Pass
Implementation representation CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass
Development	ADV	Pass
Security Architecture description	ADV_ARC.1	Pass
Functional specification with complete summary	ADV_FSP.4	Pass
Architectural design	ADV_TDS.3	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: Basic design	ATE_DPT.2	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Vulnerability analysis	AVA_VAN.4	Pass

10 Evaluator Comments and Recommendations

The evaluator has no recommendation for the TOE.

In addition all aspects of assumptions, threats physical personnel and procedural means as outlined in the Security Target are not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

Periodical checkups checks are recommended during which the following should be taken into consideration:

- The control officer or fitter has to check the graving of the metal case.
- The lead sealing shall be checked.
- If multiple audit records indicate that uncommon events have occurred multiple times, e.g. the MS has lost connection with the VU, this needs to be investigated further. This could be an indication that some form of manipulations of the MS has taken place.

One or more abnormalities which can’t be explained should lead to a detailed checking of the complete system to detect potential attack efforts. In this case the motion sensor should be taken out of the gearbox by a qualified workshop for detailed check, e.g. using magnifier, check cable between MS and VU, repairing of the MS and the VU, etc.

11 Glossary

CC	Common Criteria
CR	Change Request
DPA	Differential Power Analysis
ITSEC	Information Technology Security Evaluation Criteria
KS	Session key
KP	Pairing Key
MS	Motion Sensor
NARA	New Audit Record Available
NVRAM	Non-Volatile Random-Access Memory
OSP	Organisational Security Policies
PP	Protection Profile
SC	smart card
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
VU	Vehicle Unit

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[ST] Security Target – Sensor for digital tachograph LESIKAR TACH2, Version 2.5, 2016-06-23

[Guidance document] Guidance Documentation – LESIKAR TACH2, Version 1.2, 2015-07-02

[Catalogue list] Catalogue list LESIKAR TACH2, Version 06, 2016-05-02

[Regulation_ 2013] Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (OJ L 370, 31.12.1985, p. 8), updated up until 2013 with these two latest updates "M15 Commission Regulation (EU) No 1266/2009 of 16 December 2009 in Official Journal L 339, page 3, 22.12.2009" and "M16 Council Regulation (EU) No 517/2013 of 13 May 2013 in Official Journal L 158, page 1, 10.6.2013".

[Annex1B_ App10] Appendix 10 of [Annex1B]

[ISO16844-3] ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface. Corrected with ISO 16844-3:2004/Cor 1:2006.

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

Appendix A QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2015-06-17:

QMS 1.17.3 valid from 2015-01-29

QMS 1.18 valid from 2015-06-18

QMS 1.18.1 valid from 2015-08-21

QMS 1.19 valid from 2016-02-05

QMS 1.19.3 valid from 2016-05-30

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.19”.

The certifier concluded that, from QMS 1.17.3 to the current QMS 1.19.3, there are no changes with impact on the result of the certification.