Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target Lite v1.0

LESIKAR

SENSORS

Lesikar

2019-09-24

Created by

jtsec BEYOND IT SECURITY

GEN Create Common Criteria compliant documentation Simple and Easy

Table of contents

1 ST Introduction

1.1 ST Reference

Title: Motion Sensor for Digital (smart) Tachographs Lesikar TACH3 Security Target Lite

Version: v1.0

Author: Lesikar

Date of publication: 2019-09-24

This is the Security Target Lite for the Lesikar motion sensor TACH3.

This Security Target is based on and claims strict conformance with Digital Tachograph – Motion Sensor (MS PP) Protection Profile **[BSI-CC-PP-0093]**. Therefore, all security requirements, security objectives and security problem elements are the same of such protection profile. **[BSI-CC-PP-0093]** contemplates the security requirements defined in the 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 **[CIR-EU-2016/799]**.

Chapter 1 gives a description of the ST and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 2 states the conformance claims made.

In chapter 3, the security problem definition of the TOE is described. This includes threats against the TOE, assumptions about the operational environment of the TOE and organisational security policies that are to be employed to ensure the security of the TOE.

The Security Objectives stated in chapter 4 describes the intent of the Security Functions. The Security Objectives are divided into two groups of security objects, for the TOE and for the operational environment of the TOE.

No extended components are defined so chapter 5 is empty.

In chapter 6 the IT security functional and assurance requirements are stated for the TOE. These requirements are a selected subset of the requirements of part 2 and 3 of the Common Criteria standard.

A brief description of how the security functional requirements are implemented in the TOE is described in chapter 7.

NOTE: The Protection Profile **[BSI-CC-PP-0093]**, to which this Security Target claims strict conformance, includes several references to the European Regulation **[CIR-EU-2016/799]**.

However, at the date of release of this ST, the regulation **[CIR-EU-2018/502]** has been published, introducing several amendments to the original text of **[CIR-EU-2016/799]**. The text of the new regulation **[CIR-EU-2018/502]** has been reviewed, and it has been concluded that its contents are

compatible with those in the previous regulation **[CIR-EU-2016/799]**, which is referenced throughout **[BSI-CC-PP-0093]**. Thus, the TOE is compatible with both regulations.

Therefore, the references to **[CIR-EU-2016/799]** are maintained in this ST and they are not replaced with references to the new regulation.

1.2 TOE Reference

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.

1.3 TOE Overview

1.3.1 Introduction

1.3.1.1 Smart Digital Tachograph – System Overview

The smart digital tachograph as described on the European Commission web site **[DT-site]**:

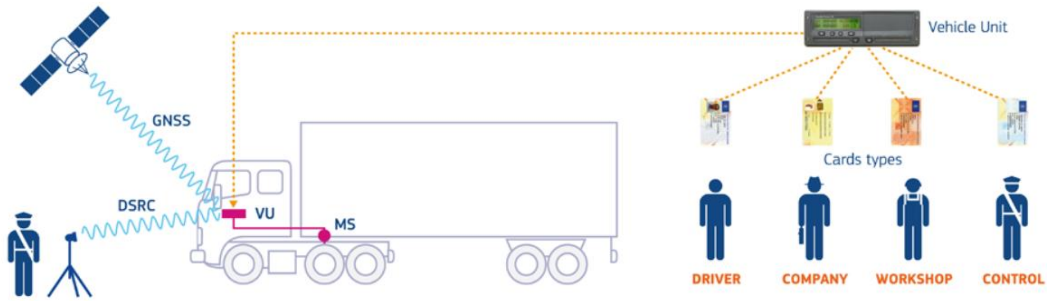


Figure 1 *The smart digital tachograph as described on the European Commission web site – V.U., M.S. and card types*

Scope:

The Smart Digital Tachograph is a recorder of the professional drivers' activities (rest and driving hours). It provides trustworthy information to EU enforcers controlling compliance with Social Regulation (EC) No 561/2006.

Objectives:

The digital tachograph was introduced to:

- Increase road safety, by controlling the activity of the drivers (limiting daily driving hours)
- Ensure minimum working conditions standards for professional drivers
- Guarantee fair competition between EU transport companies

Technical Requirements:

In order to fulfill these objectives, the digital tachograph requires a motion sensor paired with it and smartcards which are used to control secure access to the device and its data for drivers, law enforcers, companies and workshops.

1.3.1.2 Digital Tachograph – The Motion Sensor

The motion sensor (MS) is connected and sealed to the gearbox during installation. The vehicle unit (VU) is located in the driver compartment. The MS and VU are connected by a cable. The MS uses sensing elements to receive motion data from the mechanical interface that is processed and derived and output to the vehicle unit through the 4-pin connector. The requirements on the physical design of the 4-pin connector, the sealing area and the holes for the sealing cabling are specified in **[ISO15170-1]**.

To enable security (authentication and data integrity) a data channel is used in accordance with the interface specification **[ISO 16844-3:2004]**. This channel is used to respond to VU requests.

As a motion sensor compliant with **[BSI-CC-PP-0093]**, the TOE supports communication with second generation and first-generation vehicle units (VU).

The PKI and smartcards are only used by the VU, not by the MS. All authentication between the MS and VU is based upon using the preinstalled cryptographic keys (motion sensor initial security data, see section 3.1) and TDES encryption/decryption (first generation VU) or AES encryption/decryption (second generation VU), in accordance with the interface specification **[ISO 16844-3:2004]**, and described in the ST, section 1.4.1.2 “The cryptographic security model establishing the root of trust”. No PKI, certificates or asymmetric keys are used for this authentication.

1.3.1.3 Intended Usage

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 typical motion sensor is described in the figure below.

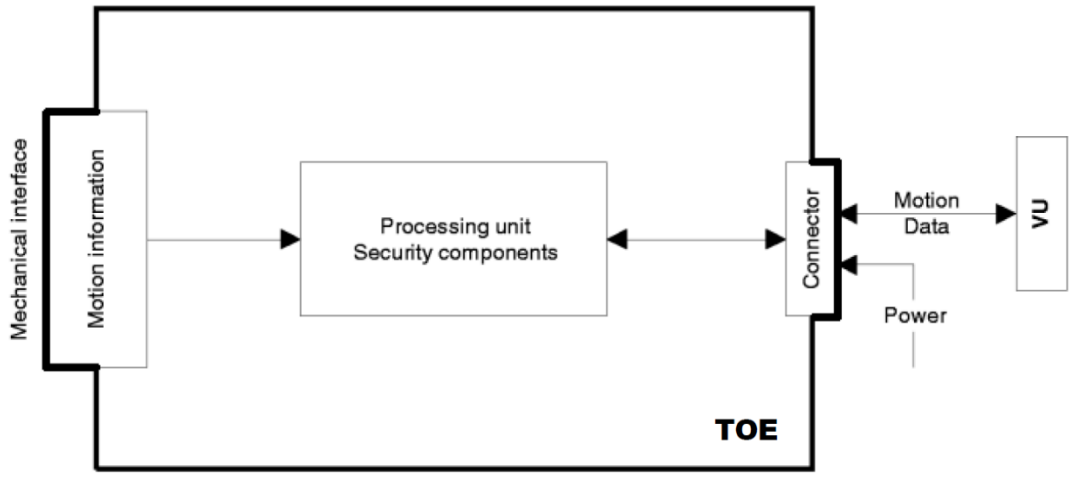


Figure 2 *The schematics for a typical motion sensor*

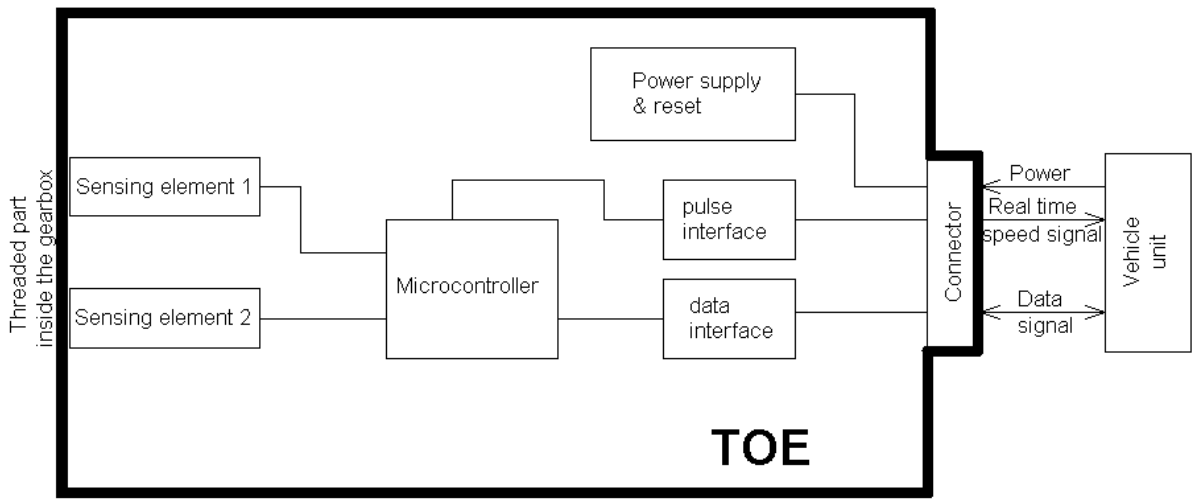


Figure 3 *The schematics for the Sensor for digital tachograph LESIKAR TACH3*

The security seal used to seal the TOE cannot be broken or removed and re-attached without the user being able to detect the manipulation; and thereby provide the means of detecting physical tampering with the mechanical interface.

During the manufacturing of the TOE some important aspects like the import of TOE security data (personalisation) need to be performed, see section 1.3.1.4.1. Also common security assurance requirements of the claimed EAL regarding product development, e.g. ADV and ALC, need to be fulfilled.

1.3.1.4 TOE Life Cycle

The typical life cycle of the motion sensor is described in the following figure:

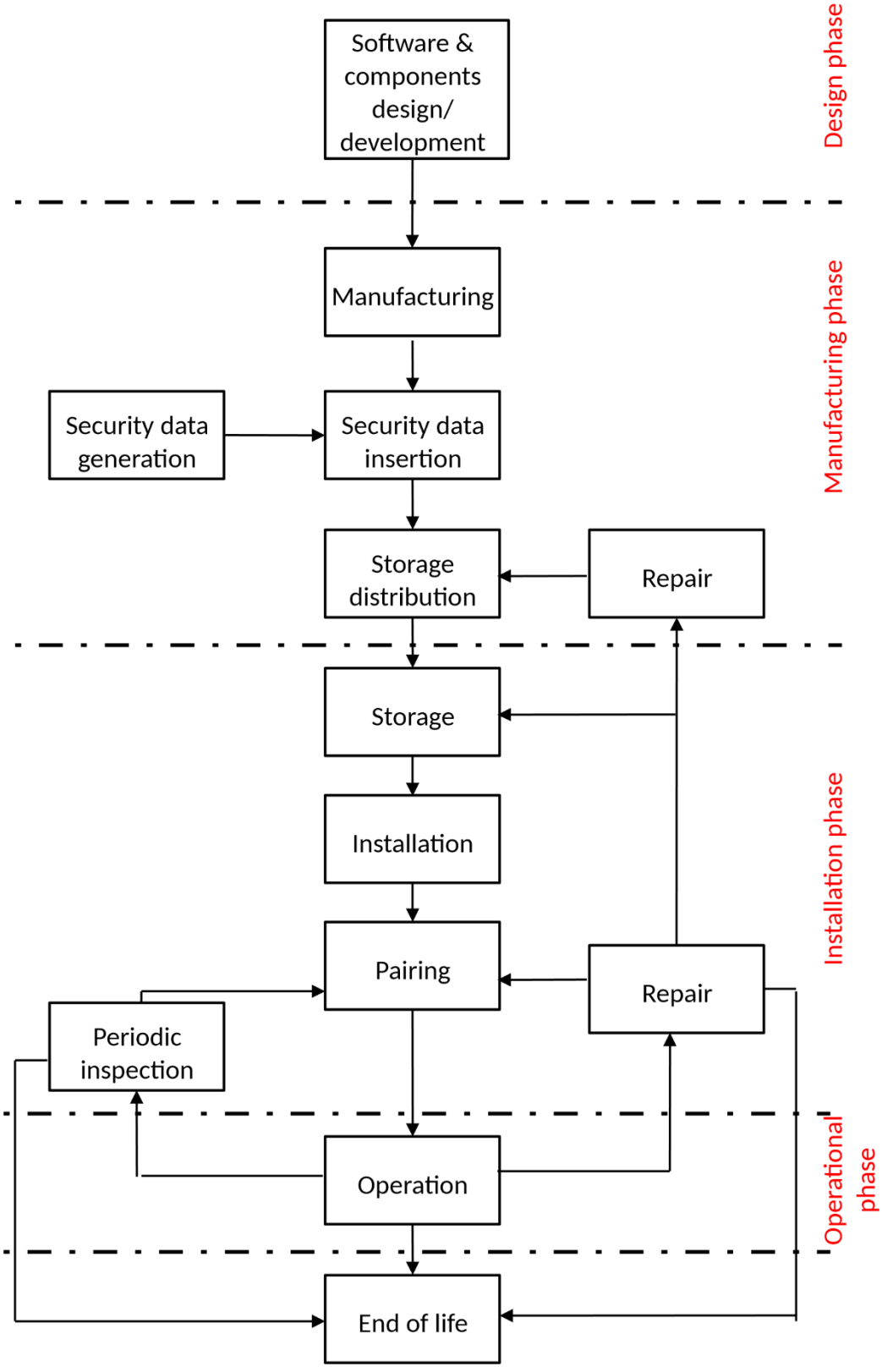


Figure 4 The life-cycle for a typical motion sensor

Figure 4 shows the typical motion sensor life-cycle as defined in **[BSI-CC-PP-0093].**

In the case of this TOE, there is a small difference with respect to the life-cycle described in the Protection Profile: this TOE is not designed to be repaired, therefore, if functioning problems are found during periodic inspections or in general during installation or operation phases, the TOE will need to be replaced.

On the other side, the **TOE is delivered after the insertion of security data** (manufacturing phase in the life-cycle diagram), which is explained in detail in section 1.3.1.4.1.

During installation phase, the TOE is installed in the vehicle by an approved and trusted fitter or workshop. After this step, the approved workshop attaches a security seal according to regulation **[EN 16882:2016]**.

Once the TOE has been installed in the vehicle and the security seal has been attached, the TOE is paired with the vehicle unit (VU). 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. See section 1.4.1.2.

1.3.1.4.1 The important life-cycle phases of the TOE in the context of this ST

This section describes in detail some of the important actions that take place in the different life-cycle phases of the TOE as described in figure 4.

Manufacturing phase

- **Generation of security data:** The motion sensor identification data (including the extended serial-number of the motion sensor, N_S) and the motion sensor pairing key, K_P, is generated by Lesikar during manufacturing phase. N_S and K_P are sent to Transportstyrelsen (the Member State Certification Authority). Transportstyrelsen replies by sending Lesikar the rest of the initial security data: the extended serial-number of the motion sensor encrypted with the identification key, ${}^{e}K_{ID}$ (N_S); and the pairing key of the motion sensor encrypted with the master key, ${}^{e}K_m$ (K_P).
- **Insertion of security data.** Once the security data has been generated, the next step in the production is to insert all motion sensor identification data and all motion sensor initial security data into the motion sensor.

Installation phase

- **Installation in the vehicle and sealing.** The TOE is installed in the vehicle by an approved and trusted fitter or workshop. After installation the approved workshop attaches a security seal according to regulation **[EN 16882:2016]**.
- **Pairing.** After installation in the vehicle and sealing, the TOE is paired with the VU. Pairing is performed by an approved fitter or workshop, see Figure 4 and Figure 9.

Application note: no other connections to the sensor different than the VU paired are contemplated and the TOE won't respond to any requests through the communication interface with VU, other than those coming from the authenticated and paired VU. This should be considered regarding footnote 4 of **Application Note:** footnote 4 of **[BSI-CC-PP-0093]**.

Operational phase
After pairing the TOE is installed as part of a digital tachograph system. This is the end-user operational phase, see Figure 4.

1.3.2 TOE Type

The TOE type is the Motion Sensor Unit in accordance with **[CIR-EU-2016/799]**.

Therefore, TOE type is compatible with TOE type of **[BSI-CC-PP-0093]**.

1.3.3 TOE Usage & Major Security Features

The TSF 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, K_S, from the VU during pairing.
- The export of a pairing key, K_P, 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.

"MS data" is information, it refers to all the kinds of data the TOE can contain, i.e. all the assets listed in the asset list in section 3.1.

1.3.3.1 Authentication

The PKI and smartcards are only used by the VU, not by the MS. All authentication between the MS and VU is based upon using the preinstalled cryptographic keys (motion sensor initial security data, see section 3.1) and TDES encryption/decryption (for first-generation VU) and AES encryption/decryption (for second generation VU) in accordance with the interface specification **[ISO 16844-3:2004]** and described in the ST, section 1.4.1.2 "The cryptographic security model establishing the root of trust". No PKI, certificates or asymmetric keys are used for this authentication.

1.3.3.2 The authentication of the Vehicle Unit to the Motion Sensor during pairing

The VU is authenticated to the MS during pairing as described in **[ISO 16844-3:2004]**, sections 7.4.3 and 7.4.4; and in the ST, Figure 9:

- The vehicle unit initialises the pairing by transmitting instruction No. 40 to the motion sensor.
- The extended serial-number of the motion sensor, N_S, is sent to the vehicle unit in plain text as response to received instruction No. 40.
- The vehicle unit encrypts the extended serial number of the motion sensor, using the identification key and transmits it, ${}^{e}K_{ID}$ (N_S), to the motion sensor with instruction No. 41.
- The motion sensor then compares the received data with the stored encrypted extended serial number. If they are equal, it is assumed that the authentication of the vehicle unit to the motion sensor is correct, see **[ISO 16844-3:2004]** section 7.4.4.3.

1.3.3.3 Authentication of the Motion Sensor to the Vehicle Unit during pairing

The MS is authenticated to the VU during pairing as described in **[ISO 16844-3:2004]**, sections 7.4.4.3, 7.4.5, 7.4.6 and 7.4.7; for second generation tachograph in Annex 1C, Appendix 11, Part B, chapter 12 of **[CIR-EU-2016/799]** and in the ST, Figure 9:

- If the VU is successfully authenticated to the MS as described above. The motion sensor transmits a pairing key which is encrypted with the master key to the vehicle unit, ${}^{e}K_m$ (K_P).
- The VU decrypts the pairing key with the master key. If the use of the pairing key later is successful this proves that the MS is in possession of the ${}^{e}K_m$ (K_P), i.e. the pairing key encrypted with the real master key.
- The VU sends the session key encrypted with the pairing key, ${}^{e}K_P$ (K_S), and transmits it with instruction No. 42 to the motion sensor.
- The VU encrypts the pairing information with the pairing key, ${}^{e}K_P$ (P_D), using two-key triple DES and transmits it with the instruction No. 43 to the motion sensor.

- The vehicle unit requests the motion sensor for pairing information and authentication using instruction No. 50 to the motion sensor.
- The motion sensor responds by submitting the pairing information encrypted with the session key, ${}^{e}K_S$ (P_D).
- The vehicle unit decrypts the data bytes with the session key and compares the decrypted data with the pairing information of the current pairing. If they are equal, it is assumed that the authentication of the motion sensor to the vehicle unit is correct and that the motion sensor is using the correct session key.

The pairing process of motion sensor and VU for second generation tachograph system is described in Annex 1C, Appendix 11, Part B, chapter 12, CSM_217 of **[CIR-EU-2016/799]**. It uses symmetric AES keys in the lengths of 128, 192 and 256 bits.

The procedure follows steps in Table 6 in **[ISO 16844-3:2004]** with these additions:

CMS_217 2: The VU reads all available $K_{M\text{-}WC}$ keys from the workshop card, inspects their key version numbers and chooses the one matching the version number of the VU's K_M-VU key. If the matching $K_{M\text{-}WC}$ key is not present on the workshop card, the VU aborts the pairing process and shows an appropriate error message to the workshop card holder.

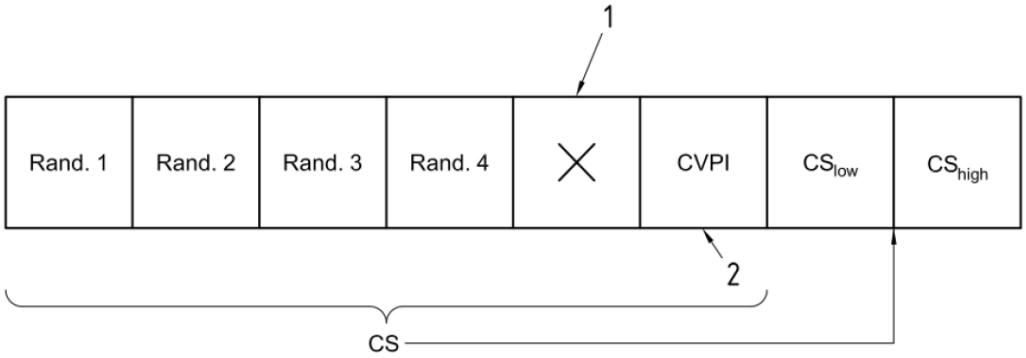
CMS_217 5: The motion sensor matches the encrypted serial number consecutively with each of the encryptions of the serial number it holds internally. If it finds a match, the VU is authenticated. The motion sensor notes the generation of K_{ID} used by the VU and returns the matching encrypted version of its pairing key, i.e. the encryption that was created using the same generation of K_M.

1.3.3.4 Data Integrity

The data integrity as specified in **[ISO 16844-3:2004]**, sections 7.1, 7.5 and 7.6; uses parity bits, LRC, checksums, counters and TDES / AES encryption:

- The transfer of data is serial and asynchronous with a baud rate of 1 200 Baud. The structure of one byte is: 1 start bit, 8 data bits, 1 parity bit (even) and 1 stop bit.
- Each message sent between the MS and the VU or vice versa has a checksum based on arithmetical XOR over the bytes in the message, a longitudinal redundancy check, LRC.
- Available **[ISO 16844-3:2004]** instructions: 10, 11, 40, 41, 42, 43, 50, 70 or 80. 40-50 is used for pairing; 10-11 is used for request for information (files) and 70-80 is for normal operation.
- Instructions 10 and 70 both start with the VU sending authentication data to the MS encrypted with the session key. This data consists of a random number that is bitwise XORed with the MS serial number in the response message (the response to instruction 11 or 80):
    - The authentication data sent from the VU to the MS (see Figure 5, Structure of authentication data after decryption): Authentication data 8 bytes (4 bytes random number and 4 bytes control information) encrypted with the session key, ${}^{e}K_S$(DA). DA = Authentication Data.
    - Authentication data after decryption: The motion sensor may check that no information was lost since the reception of the last instruction by means of the CVPI

(check value previous instruction), see Figure 5. The authentication is correct if the checksum from byte 0 to byte 5 is equal to the value of byte 6 and byte 7. Value CVPI shall be set to 0 by the vehicle unit when the communication is started the very first time after pairing of vehicle and sensor unit.



Key

1 In the case of instruction No.10, the file number shall be found at this position; in the case of instruction No. 70, this byte is left unspecified.

2 CheckSumlow of the previous instruction (instruction No. 10 or No 70) XORed with the low byte of the actually latched counter value.

Figure 5 *Structure of authentication data after decryption, DA*

- The motion sensor has a counter:
    - The 16-bit counter in the motion sensor is decremented with each pulse of the speed signal.
- The motion sensor responds to instruction 80 by submitting the sensor data encrypted with the session key, ${}^{e}K_S(DS)$. DS = Sensor Data.
- The sensor data consists of: Duty cycle, Random number from instruction No. 70 XOR the Serial-number of the motion sensor, Counter value of the motion sensor and Additional information (e.g. the NARA flag, new audit record available). See Figure 6, Structure of sensor data after decryption.
    - Duty cycle: the motion sensor is measuring, as a percentage, the duty cycle of the real-time speed signal, and the reset bit shows the occurrence of a system reset and shall be set after reset and automatically cleared when byte CVPI indicates that the message has been accepted by the authenticated vehicle unit.

Duty cycle	Random number from instruction No. 70 XOR Serial-number of the motion sensor				Counter value of the motion sensor		Additional information
DC	Rand.1 ⊕ Serno.1	Rand.2 ⊕ Serno.2	Rand.3 ⊕ Serno.3	Rand.4 ⊕ Serno.4	LSB	MSB	MF

Key

DC: duty cycle

LSB: least significant byte

MSB: most significant byte

MF: multi function byte

Figure 6 Structure of sensor data after decryption, DS

- The motion sensor responds to instruction 10 by submitting the data of the requested file encrypted with the session key, ${}^{e}K_S$(DFS). DFS = data of file selected.
- Also the Data for authentication (see Figure 5) containing the Number of Selected File and a checksum over all data is sent in the same response message, see **[ISO 16844-3:2004]**, section 7.6.3.3.

1.3.4 Non-TOE Hardware/Software/Firmware

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 Annex 1C of **[CIR-EU-2016/799]**, the motion sensor 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 (VU), the only component intended to communicate with the TOE.
- A smart card (SC) 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, see section 1.4.1.2. The following keys are generated, distributed and handled by the certification authorities. They are not part of the TOE:

- The master key, Km. Km = Km_{VU} XOR Km_{WC} . Km is not stored in any part of the tachograph system.

- K_{ID} (derived from Km). K_{ID} is not stored in any part of the tachograph system.
- K_{VU} (The part of Km put in the VU)
- K_{WC} (The part of the K_M put in the smart card for the workshop)

For the cryptographic keys and other security data that is part of the TOE, see the asset list in section 3.1.

1.4 TOE Description

1.4.1 Introduction

1.4.1.1 System Overview

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. It is designed to be connected to the gearbox of the vehicle, and sealed. The rotation of a mechanical part of the gearbox is used to generate the speed signal.

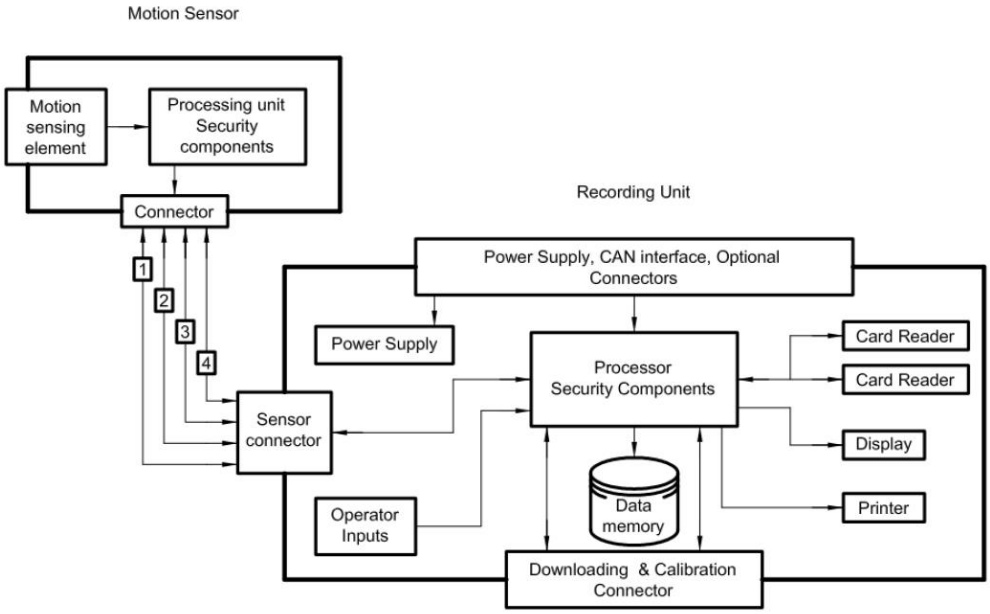
The interface between the motion sensor and the vehicle unit (physical, electrical and protocol levels) is designed to be compliant with **[ISO 16844-3:2004]**, Cor 1:2006 **[ISO 16844-3:2004]**. Input / Output signals and power are exchanged through an **[ISO15170-1]** 4 pin connector.

The motion sensor provides two types of motion information to the vehicle unit it is connected to; the real-time analog speed pulses (pin 3), and the digital motion data (pin 4). The digital motion data is considered an asset in the TOE and is integrity protected by the TSF – the analog real-time speed pulses are not.

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.

In order to prevent manipulation of the tachograph system; a secure channel (trusted path) between the MS and the VU is established by the use of pre-installed shared secrets, that is used to mutually authenticate the MS and the VU, and to get a common shared session key used for encryption and decryption. This process is called pairing, for details see section 1.4.1.2. For pairing to work, the VU must have both the VU Key, K_{VU}, and the Workshop Key, K_{WC}, which is stored on the workshop smart card. The pairing information for the first pairing is stored once in the MS, as the First Pairing, and never changed. The pairing information for any subsequent pairing is stored in the MS, as the Last Pairing.

A typical tachograph system is shown below.



Key

1 positive supply
2 battery minus
3 speed signal, real time
4 data signal in/out

Figure 7 A typical tachograph system

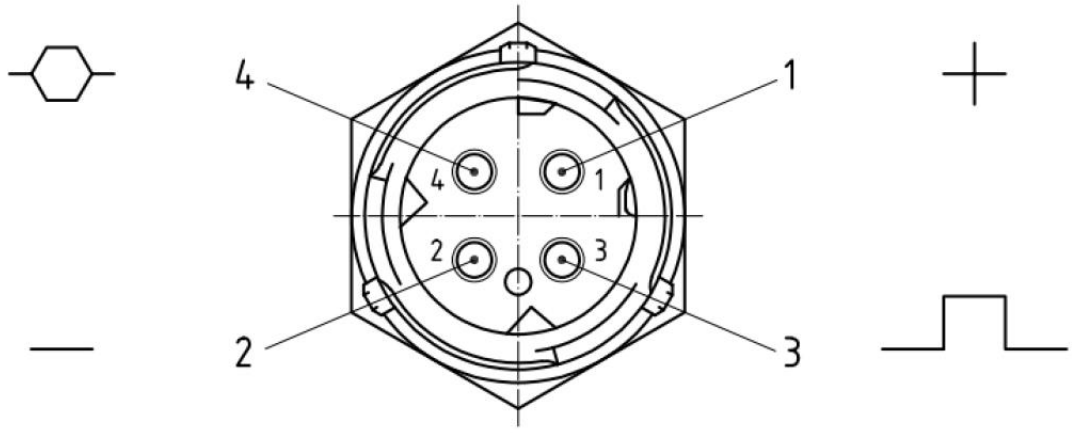


Figure 8 The ISO 15170-1 4 pin connector

1.4.1.2 The cryptographic security model establishing the root of trust

The cryptographic operations dictated in Annex 1C of **[CIR-EU-2016/799]** and **[ISO 16844-3:2004]** for mutual authentication and data encryption between the motion sensor (MS) and the vehicle unit (VU) of first generation:

- CSM_036: The European certification authority shall generate Km_{VU} and Km_{WC} , two independent and unique Triple DES keys, and generate Km (the master key) as:
- $Km = Km_{VU}$ XOR Km_{WC}
- The European certification authority shall forward these keys, under appropriately secured procedures, to Member States certification authorities at their request.
- The Component Personaliser (Lesikar) generates the extended serial-number of the motion sensor in plain text, N_S; and the pairing key of the motion sensor in plain text, K_P, and sends them to the Member State certification authority (Transportstyrelsen).
- CSM_037: Member States certification authorities shall:
    - use Km to encrypt motion sensor data requested by motion sensor manufacturers (data to be encrypted with Km is defined in ISO 16844-3),
        - Generate identification key:
            - Constant control vector CV: 48 21 5F 00 03 41 32 8A || 00 68 4D 00 CB 21 70 1D hexadecimal.
            - $K_{ID} = Km$ XOR CV
        - the extended serial-number of the motion sensor in plain text, NS, is encrypted with the identification key:
            - ${}^{e}K_{ID}(N_S)$;
        - the pairing key of the motion sensor, K_P , is encrypted with the master key:
            - ${}^{e}Km(K_P)$.
    - forward Km_{VU} to vehicle unit manufacturers, under appropriately secured procedures, for insertion in vehicle units,
    - ensure that Km_{WC} will be inserted in all workshop cards (SensorInstallationSecData in Sensor_Installation_Data elementary file) during card personalisation.
- I.e. Km_{VU} is put in the VU and Km_{WC} is put on the workshop smart card. Both these keys are needed for pairing the MS to the VU (to get the master key, Km).
- The following security data is stored in the MS – The MS is now ready for pairing:
    - the extended serial-number of the motion sensor in plain text, N_S;
    - the extended serial-number of the motion sensor encrypted with the identification key, ${}^{e}K_{ID}(N_S)$;
    - the pairing key of the motion sensor in plain text, K_P;
    - the pairing key of the motion sensor encrypted with the master key, ${}^{e}Km(K_P)$.

- This additional security data is stored in the MS after pairing:
    - The session key, K_S , received from the VU .
    - The pairing data, P_D (also called pairing information):
        - $K'_P = K_P$ XOR (N_S ||N_S)
        - n4 byte is a 4 byte-long random number generated by the vehicle unit.
        - $P_D = {}^eK'_P$ [($n_{4\ byte}$)||(date of pairing)||(VU type approval number)||(VU serial number)]

The sequence of instructions for pairing, see **[ISO 16844-3:2004]**, Table 6.

Vehicle unit	Direction of data transfer	Motion sensor	Remark
40	→		Initialise pairing
	←	ACK	
	←	Response	N_S
41	→		${}^eK_{ID}(N_S)$
	←	ACK	
	←	Response	IF (VU authorised) ${}^eKm(K_P)$
42	→		${}^eK_P(K_S)$
	←	ACK	
43	→		${}^eK_P(P_D)$
	←	ACK	
50	→		Request for authentication
	←	ACK	
	←	Response	${}^eK_S(P_D)$

Figure 9 The sequence of instructions for pairing

VU – Motion Sensor Pairing and Communication using AES.

CSM_218 of Annex 1C of **[CIR-EU-2016/799]** states the different procedure with AES keys that the one stated in ISO 16844-3. Since the AES block size is 16 bytes, the length of an encrypted message must be a multiple of 16 bytes, compared to 8 bytes for TDES. Moreover, some of these messages will be used to transport AES keys, the length of which may be 128, 192 or 256 bits. Therefore, the number of data bytes per instruction in Table 5 of **[ISO 16844-3:2004]** shall be changed as shown in table below:

Instruction	Request/reply	Description of data	#of plaintext data bytes according to [ISO 16844-3]	# of plaintext data bytes using AES keys	# of encrypted data bytes when using AES keys of bitlength		
					128	192	256
10	request	Authentication data + file number	8	8	16	16	16
11	reply	Authentication data + file contents	16 or 32, depend on file	16 or 32, depend on file	16/32	16/32	16/32
41	request	MoS serial number	8	8	16	16	16
41	reply	Pairing key	16	16/24/32	16	32	32
42	request	Session key	16	16/24/32	16	32	32
43	request	Pairing information	24	24	32	32	32
50	reply	Pairing information	24	24	32	32	32
70	request	Authentication data	8	8	16	16	16
80	reply	MoS counter value + auth. data	8	8	16	16	16

CSM_220 In case the plaintext data length (using AES keys) is not a multiple of 16 bytes, padding method 2 defined in ISO 9797-1 shall be used.

It is not possible to pair a second-generation VU to a first-generation motion sensor.

It is not possible to use a first-generation workshop card for coupling a second-generation VU to a motion sensor.

1.4.2 TOE Logical Scope

sThe TOE measures motion data representative of vehicle's speed and distance travelled and passes this information along to the vehicle unit in a secure way to comply with EU regulations.

- Motion data detection and transmission to the VU
- Pairing with a VU – mutual authentication and the exchange of a session key, K_S.
- Sending data at VU request
- Security audit data generation

1.4.2.1 Logical Scope of the TSF (security features)

The TSF 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, K_S, from the VU during pairing.
- The export of a pairing key, K_P, to the VU during pairing.
- 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.

1.4.2.2 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

1.4.2.3 Configuration and Modes

Two modes are considered for the motion sensor:

- The MS ready for pairing – this is the mode of the TOE when delivered, the first phase in section 1.3.1.4.1.
    - The TOE is delivered as a motion sensor ready for pairing. The steps required becoming ready for pairing regarding the cryptographic security model and the establishment of trust is described in section 1.4.1.2. All MS identification data and all MS initial security data have been installed.
- The MS after pairing with the VU (pairing is only performed by an approved fitter or workshop). After installation, sealing and pairing the TOE is installed as part of a digital tachograph system. This is the end-user operational phase, the last phase in section 1.3.1.4.1. See also Figure 4.

1.4.2.4 User categories

Two external user categories are used – both are external entities:

- Authenticated VU
- Unauthenticated VU

The name “Unauthenticated VU” is used for anything else than an authenticated VU, i.e. the TSF do not even know if it is a VU since it is not authenticated.

1.4.3 TOE Physical Scope

The physical scope of the TOE includes the following; see also Figure 3, The schematics for the Sensor for digital tachograph LESIKAR TACH3.

- 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).

The different models of the motion sensor only differ by their length (to be able to fit in different kinds of vehicles).
The physical boundary of the TOE is defined by the MS casing, the mechanical interface and the 4-pin connector **[ISO15170-1]**. The real-time speed signal is transmitted from the MS to the VU on pin 3. All other communication between the MS and the VU is performed on pin 4. All this communication is performed according to the interface specification **[ISO 16844-3:2004]** and Annex 1C Appendix 11, Part B of **[CIR-EU-2016/799]**.

2 Conformance Claims

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R5.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R5P2].
- Conformance with [CC31R5P3].

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of April 2017, version 3.1 revision 5 with an evaluation assurance level of EAL4 + ATE_DPT.2 + AVA_VAN.5.

This Security Target claims conformance with the following protection profiles:

- Protection profile BSI-CC-PP-0093 with strict conformance.

3 Security Problem Definition

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE
- The organizational security policies that the TOE has to adhere to
- The TOE usage assumptions in the suggested operational environment.

We will begin defining Assets and Agents of threats.

3.1 Assets

MOTION DATA (MOD): Motion data (see Glossary for more details)

AUDIT DATA (AUD): Details of events

IDENTIFICATION DATA (IDD): Name of manufacturer, serial number, approval number, embedded security component identifier, operating system identifier.

KEYS TO PROTECT DATA (SDK): Enduring secret keys and session keys used to protect security and user data held within and transmitted by the TOE, and as a means of authentication.

TOE DESIGN AND SOFTWARE CODE (TDS): Design information and source code (uncompiled or reverse engineered) for the TOE that could facilitate an attack.

TOE HARDWARE (THW): Hardware used to implement and support TOE functions

3.2 Threat Agents

VEHICLE UNIT: Vehicle unit (authenticated), to which the motion sensor is paired. The term “user” is also used within this ST to refer to a vehicle unit.

OTHER DEVICE: Other device (not authenticated) to which the motion sensor may be connected. This includes an unauthenticated vehicle unit.

ATTACKER: A human, or process acting on their behalf, located outside the TOE. For example, a driver could be an attacker if he attempts to interfere with the motion sensor. An attacker is a threat agent (a person with the aim of manipulating user data, or a process acting on their behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the maintained assets. The attacker is assumed to possess at most a high attack potential.

3.3 Threats to Security

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

T.ACCESS: Access control – A **Vehicle Unit** or other device (under control of an **Attacker**) could try to use functions not allowed to them, and thereby compromise the integrity or authenticity of **Motion data (MOD)**.

T.DESIGN: Design knowledge - An **Attacker** could try to gain illicit knowledge of the motion sensor design (**TOE design and software code (TDS)**), either from manufacturer's material (e.g. through theft or bribery) or from reverse engineering, and thereby more easily mount an attack to compromise the integrity or authenticity of **Motion data (MOD)**.

T.ENVIRONMENT: Environmental attacks – An **Attacker** could compromise the integrity or authenticity of **Motion data (MOD)** through physical attacks on the motion sensor (thermal, electromagnetic, optical, chemical, mechanical).

T.HARDWARE: Modification of hardware - An **Attacker** could modify the motion sensor hardware (**TOE hardware (THW)**), and thereby compromise the integrity or authenticity of **Motion data (MOD)**.

T.MOTION_DATA: Interference with motion data – An **Attacker** could add to, modify, delete or replay the vehicle's motion data, and thereby compromise the integrity or authenticity of **Motion data (MOD)**.

T.SECURITY_DATA: Access to security data - An **Attacker** could gain illicit knowledge of secret cryptographic keys (**Keys to protect data (SDK)**) during security data generation or transport or storage in the equipment, thereby allowing an **Other Device** to be connected.

T.SOFTWARE: Attack on software - An **Attacker** could modify motion sensor software (**TOE design and software code (TDS)**) during operation, and thereby compromise the integrity, availability or authenticity of **Motion data (MOD)**.

T.TESTS: Invalid test modes - The use by an **Attacker** of non-invalidated test modes or of existing back doors could permit manipulation of **Motion data (MOD)**.

T.POWER_SUPPLY: Interference with power supply – An **Attacker** could vary the power supply to the motion sensor, and thereby compromise the integrity or availability of **Motion data (MOD)**.

T.MECHANICAL: Interference with mechanical interface – An **Attacker** could manipulate the motion sensor input, for example, by disconnecting the sensor from the gearbox, such that **Motion data (MOD)** does not accurately reflect the vehicle's motion.

3.4 Organizational Security Policies

The organizational Security policies are defined as follows.

P.CRYPTO: The cryptographic algorithms and keys described in [CIR-EU-2016/799] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

3.5 Assumptions

The assumptions when using the TOE are the following:

A.APPROVED_WORKSHOPS: Approved Workshops - The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, checks, inspections and repairs.

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

A.TYPE_APPROVED: Type Approved VU - The motion sensor will only be operated together with a vehicle unit being type approved according to [CIR-EU-2016/799] Annex 1C.5

4 Security Objectives

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These consist of:

- the security objectives for the operational environment.
- the security objectives for the TOE

4.1 Security objectives for the TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in enforcing the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

O.SENSOR_MAIN: Accuracy, integrity and authenticity of data - The authentic motion data transmitted by the TOE must be provided to the vehicle unit, to allow the vehicle unit to accurately determine the movement of the vehicle in terms of speed and distance travelled.

O.ACCESS: Access – The TOE must control access to functions and data.

O.AUDIT: Audit - The TOE must audit attempts to undermine its security.

O.AUTHENTICATION: Authenticated access - The TOE must authenticate a connected user (vehicle unit) before allowing access to data and functions.

O.PROCESSING: Motion data derivation – The TOE must ensure that processing of input to derive motion data is accurate.

O.RELIABILITY: Reliable service - The TOE must provide a reliable service.

O.PHYSICAL: Physical protection - The TOE must resist attempts to access TSF software, and must ensure that physical tampering attacks on the TOE hardware can be detected.

O.SECURE_COMMUNICATION: Secure data exchange – The TOE must secure data exchanges with the vehicle unit.

O.CRYPTO_IMPLEMENT: Cryptographic operation – The cryptographic functions must be implemented within the TOE as required by [CIR-EU-2016/799] Annex 1C, Appendix 11.

O.SOFTWARE_UPDATE: Software updates - Where updates to TOE software are possible, the TOE must accept only those that are authorised.

Application Note: TOE software updates are not possible. This feature is not implemented by the TOE, as it is defined as optional, according to footnote 6 of **[BSI-CC-PP-0093]**. Therefore, no iterations for FCS components related to software updates are added in this ST.

4.2 Security objectives for the operational environment

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

OE.DEVELOPMENT: Responsible development - Developers must ensure that the assignment of responsibilities during TOE development is done in a manner which maintains IT security.

OE.MANUFACTURING: Protection during manufacture - Manufacturers must ensure that the assignment of responsibilities during manufacturing of the TOE is done in a manner that maintains IT security, and that during the manufacturing process the TOE is protected from physical attacks that might compromise IT security.

OE.DATA_GENERATION: Data generation - Security data generation algorithms must be accessible to authorised and trusted persons only.

OE.DATA_TRANSPORT: Handling of security data - Security data must be generated, transported, and inserted into the TOE in such a way as to preserve its appropriate confidentiality and integrity.

OE.DELIVERY: Protection during delivery – Manufacturers of the TOE, vehicle manufacturers and fitters or workshops must ensure that handling of the TOE is done in a manner that maintains IT security. Fitters and workshops shall particularly be informed of their responsibility related to proper sealing of the mechanical interface.

OE.DATA_STRONG: Strong crypto - Security data inserted into the TOE must be as cryptographically strong as required by [CIR-EU-2016/799] Annex 1C, Appendix 11.

OE.TEST_POINTS: Disabled test points - All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE must be disabled or removed before the end of the manufacturing process.

OE.APPROVED_WORKSHOPS: Use of approved workshops – Installation, calibration and repair of the TOE must be carried by trusted and approved fitters or workshops.

OE.CORRECT_PAIRING: Correct pairing - Approved fitters and workshops must correctly pair the TOE with a vehicle unit during the installation phase.

OE.MECHANICAL: Protection of interface – A means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)

OE.REGULAR_INSPECTION: Regular inspections - The TOE must be periodically inspected.

OE.CONTROLS: Law enforcement checks - Law enforcement controls must be performed regularly and randomly, and must include security audits.

OE.CRYPTO_ADMIN: Implementation of cryptography – All requirements from [CIR-EU-2016/799] Annex 1C concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.

OE.TYPE_APPROVED_VU: Type approved vehicle unit – The vehicle unit to which the TOE is connected must be type approved.

OE.EOL: End of life – When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric cryptographic keys has to be safeguarded.

4.3 Security Objectives Rationale

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs and the security objectives for the operational environment uphold all assumptions.

	O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update	OE.Development	OE.Manufacturing	OE.Data_Generation	OE.Data_Transport	OE.Delivery	OE.Data_Strong	OE.Test_Points	OE.Approved_Workshops	OE.Correct_Pairing	OE.Mechanical	OE.Regular_Inspection	OE.Controls	OE.Crypto_Admin	OE.Type_Approved_VU	OE.EOL
T.Access		X		X				X									X								
T.Design							X				X	X	X	X	X		X	X							
T.Environment	X		X		X	X	X													X	X	X			
T.Hardware	X					X	X				X	X			X			X			X	X			
T.Motion_Data	X		X	X	X		X	X											X						
T.Security_Data			X	X		X	X	X					X	X				X							X
T.Software	X		X	X		X	X	X		X	X	X			X						X				
T.Tests						X						X					X								
T.Power_Supply	X					X	X														X	X			
T.Mechanical	X																			X	X	X			

	O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update	OE.Development	OE.Manufacturing	OE.Data_Generation	OE.Data_Transport	OE.Delivery	OE.Data_Strong	OE.Test_Points	OE.Approved_Workshops	OE.Correct_Pairing	OE.Mechanical	OE.Regular_Inspection	OE.Controls	OE.Crypto_Admin	OE.Type_Approved_VU	OE.EOL
P.Crypto									X							X							X		
A.Approved_Workshops																		X							
A.Controls																					X	X			
A.Type_Approved																								X	

Table 1 *Security Objectives vs Security Problem Definition*

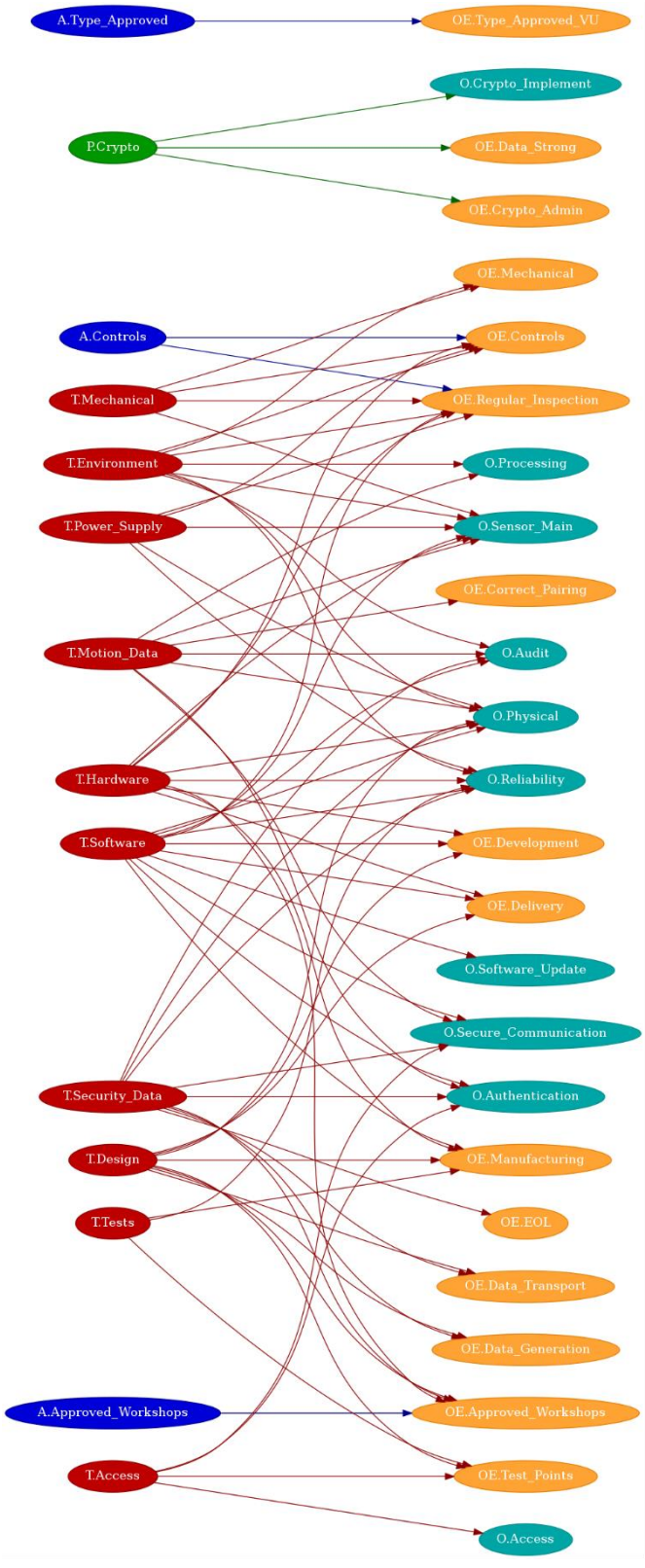


Figure 10 *Mapping of Security Problem Definition to Security Objectives*

4.3.1 Threats

T.ACCESS: T.Access is addressed directly by **O.Access**, which requires the TOE to control access to functions and data. This is supported by **O.Authentication**, which allows access only to an authenticated vehicle unit. **O.Secure_Communication** provides protection to the data channel. **OE.Test_Points** helps to ensure there are no test facilities in the delivered TOE that could be used to bypass the access controls.

T.DESIGN: T.Design is addressed by **O.Physical**, which would allow any unauthorised physical access to the TOE during operation to be detected. **OE.Development**, **OE.Manufacturing**, **OE.Data_Generation**, **OE.Data_Transport** and **OE.Delivery** all contribute to the protection of sensitive information about the TOE before it comes into operation. **OE.Approved_Workshops** ensures that the TOE is correctly installed under controlled conditions. **OE.Test_Points** helps to ensure that no access to modes that may disclose design information are available during operation.

T.ENVIRONMENT: T.Environment is addressed by **O.Sensor_Main**, which requires that motion data must be available to the VU, by **O.Reliability**, which requires a reliable service, and by **O.Processing**, which requires accurate processing of input data. **O.Physical** addresses the need to resist physical attacks, and **OE.Mechanical**, **OE.Controls** and **OE.Regular_Inspection** help to detect signs of interference with TOE hardware. **O.Audit** aims to record attempted attacks.

T.HARDWARE: T.Hardware is addressed by **O.Sensor_Main**, which requires that motion data must be available to the VU, and by **O.Reliability**, which requires a reliable service. **O.Physical** addresses the need to resist physical attacks. **OE.Regular_Inspection** and **OE.Controls** help to detect signs of interference with TOE hardware. Interference with TOE hardware during development, manufacturing, delivery, installation and repair is addressed by **OE.Development**, **OE.Manufacturing**, **OE.Delivery** and **OE.Approved_Workshops**.

T.MOTION_DATA: T.Motion_Data is addressed by **O.Sensor_Main**, which requires that motion data must be available to the VU. **O.Processing** requires that processing of inputs to derive the motion data is accurate. **O.Authentication** and **OE.Correct_Pairing** control the ability to connect to the TOE and to retrieve data, helping to protect against unauthorised access and tampering. **O.Secure_Communication** addresses security of the data transfer, helping to detect any modification or attempt to replay. **O.Physical** aims to detect physical interference, and **O.Audit** aims to record attempted attacks.

T.SECURITY_DATA: T.Security_Data is addressed by **O.Reliability**, which requires a reliable service. **O.Authentication** and **O.Secure_Communication** restrict the ability of a connected entity to access this data. **OE.Data_Generation**, **OE.Data_Transport** and **OE.Approved_Workshops** aim to protect the confidentiality and integrity of the security data before the TOE is brought into operational use, or during maintenance. **OE.EOL** requires that the TOE is disposed of securely when it no longer in service. **O.Physical** aims to detect physical interference, and **O.Audit** aims to record attempted attacks.

T.SOFTWARE: T.Software is addressed by **O.Sensor_Main**, which requires that motion data must be available to the VU, and by **O.Reliability**, which requires a reliable service. **O.Authentication**, **O.Secure_Communication** and **O.Software_Update** aim to prevent unauthorised connections to the TOE that could attempt to modify software during operation. **O.Physical** deals with attempts to modify the software by means of a physical attack on the TOE, and **O.Audit** aims to record attempted attacks. **OE.Development**, **OE.Manufacturing** and **OE.Delivery** address the prevention of software

modification prior to installation. **OE.Regular_Inspection** helps to detect signs of interference with TOE software.

T.TESTS: T.Tests is addressed by **O.Reliability**, **OE.Manufacturing** and **OE.Test_Points**. If the TOE provides a reliable service as required by **O.Reliability**, if its security cannot be compromised during the manufacturing process (**OE.Manufacturing**) and if all test points are disabled, the TOE can neither enter any non-invalidated test mode nor have any back door. Hence, the related threat will be mitigated.

T.POWER_SUPPLY: T.Power_Supply is addressed through **O.Reliability**, which requires that the TOE should operate reliably and predictably, and through **O.Sensor_Main**, which requires a supply of authentic data. **O.Physical** requires that physical attacks that attempt to modify motion data can be detected. Within the operational environment regular workshop inspections (**OE.Regular_Inspection**) and law enforcement controls (**OE.Controls**) will help to detect any interference.

T.MECHANICAL: T.Mechanical is addressed by **O.Sensor_Main**, which requires that authentic motion data must be available to the VU. **OE.Mechanical**, **OE.Regular_Inspection** and **OE.Controls** help to detect signs of interference with TOE hardware and its connection to the vehicle.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.Access	O.Access O.Authentication O.Secure_Communication OE.Test_Points
T.Design	O.Physical OE.Development OE.Manufacturing OE.Data_Generation OE.Data_Transport OE.Delivery OE.Approved_Workshops OE.Test_Points
T.Environment	O.Sensor_Main O.Reliability O.Processing O.Physical

Threats	Security Objectives
	O.Audit OE.Mechanical OE.Controls OE.Regular_Inspection
T.Hardware	O.Sensor_Main O.Reliability O.Physical OE.Regular_Inspection OE.Controls OE.Development OE.Manufacturing OE.Delivery OE.Approved_Workshops
T.Motion_Data	O.Sensor_Main O.Processing O.Authentication O.Secure_Communication O.Physical O.Audit OE.Correct_Pairing
T.Security_Data	O.Reliability O.Authentication O.Secure_Communication O.Physical O.Audit OE.Data_Generation OE.Data_Transport OE.Approved_Workshops

Threats	Security Objectives
	OE.EOL
T.Software	O.Sensor_Main O.Reliability O.Authentication O.Secure_Communication O.Software_Update O.Physical O.Audit OE.Development OE.Manufacturing OE.Delivery OE.Regular_Inspection
T.Tests	O.Reliability OE.Manufacturing OE.Test_Points
T.Power_Supply	O.Reliability O.Sensor_Main O.Physical OE.Regular_Inspection OE.Controls
T.Mechanical	O.Sensor_Main OE.Mechanical OE.Regular_Inspection OE.Controls

Table 2 Threats vs Security Objectives

4.3.2 Organizational Security Policies

P.CRYPTO: P.Crypto is supported by **O.Crypto_Implement**, which calls for the correct cryptographic functions to be implemented in the TOE. **OE.Data_Strong** calls for correct cryptographic material to be loaded into the TOE before operation, and **OE.Crypto_Admin** addresses the handling and operation of cryptographic material to be done in accordance with requirements.

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.Crypto	O.Crypto_Implement OE.Data_Strong OE.Crypto_Admin

Table 3 OSPs vs Security Objectives

4.3.3 Assumptions

A.APPROVED_WORKSHOPS: A.Approved_Workshops is supported by **OE.Approved_Workshops**, which requires the use of approved workshops for installation, pairing and repair of the TOE.

A.CONTROLS: A.Controls is supported by **OE.Controls**, which requires regular and random enforcement checks on the motion sensor, and by **OE.Regular_Inspection** which requires regular inspection of the motion sensor.

A.TYPE_APPROVED: A.Type_Approved is supported by **OE.Type_Approved_VU**, which requires that the vehicle unit that is coupled with the TOE is type approved.

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.Approved_Workshops	OE.Approved_Workshops
A.Controls	OE.Controls OE.Regular_Inspection
A.Type_Approved	OE.Type_Approved_VU

Table 4 Assumptions vs Security Objectives for the Operational Environment

5 Extended Components Definition

No extended components have been defined.

6 Security Requirements

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word “assignment” is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Selections. They appear between square brackets. The word “selection” is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Iterations. It includes “/” and an “identifier” following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.
- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 Security Functional Requirements

6.1.1 FAU: Security audit

6.1.1.1 FAU_GEN.1: Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[selection: not specified]*** level of audit; and

c) ***[assignment: The following events:***
i)Error in non-volatile memory
ii)Error in controller RAM
iii)Error in controller instruction
iv)Error in communication
v)Error in authentication] .

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[assignment: none]***.

Application Note

In sensor done according to Application note from PP **[BSI-CC-PP-0093]**: The occurrence of an auditable event on the motion sensor is flagged to the vehicle unit, which can then request a transfer of the event data for storage in the vehicle unit. The minimum list of events available from the motion sensor is specified in **[ISO 16844-3:2004]**. The vehicle unit itself generates and stores motion sensor related events as defined by Chapters 3.9, 3.12.8 and 3.12.9 and Appendix 1 of **[CIR-EU-2016/799]**. The motion sensor itself has no date/time source, and the paired vehicle unit adds a date/time stamp to the records.

6.1.1.2 FAU_STG.1: Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to ***[selection: prevent]*** unauthorised modifications to the stored audit records in the audit trail.

6.1.1.3 FAU_STG.4: Prevention of audit data loss

FAU_STG.4.1 The TSF shall ***[selection: ``overwrite the oldest stored audit records'']*** and ***[assignment: none]*** if the audit trail is full.

6.1.2 FCS: Cryptographic support

6.1.2.1 FCS_CKM.4/1: Cryptographic key destruction

FCS_CKM.4.1/1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: key destruction method in table 15 of [BSI-CC-PP-0093]]*** that meets the following: ***[assignment: -Requirements in table 15 of [BSI-CC-PP-0093]***
-Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means

-[assignment: none]] .

6.1.2.2 FCS_CKM.4/2: Cryptographic key destruction

FCS_CKM.4.1/2 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: key destruction method in table 14 of [BSI-CC-PP-0093]]*** that meets the following: ***[assignment: - Requirements in table 14 of [BSI-CC-PP-0093]***
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means.
-[assignment: none]] .

6.1.2.3 FCS_COP.1/1: AES: Cryptographic operation

FCS_COP.1.1/1: AES The TSF shall perform ***[assignment: encryption/decryption to support confidentiality, authenticity and integrity of data exchanged between a vehicle unit and a motion sensor]*** in accordance with a specified cryptographic algorithm ***[assignment: AES]*** and cryptographic key sizes ***[assignment: 128, 192, 256 bits]*** that meet the following: ***[assignment: FIPS PUB 197: Advanced Encryption Standard, and [CIR-EU-2016/799] Appendix 11, Part B]*** .

6.1.2.4 FCS_COP.1/2: TDES: Cryptographic operation

FCS_COP.1.1/2: TDES The TSF shall perform ***[assignment: encryption/decryption to support confidentiality, authenticity and integrity of data exchanged between a vehicle unit and a motion sensor]*** in accordance with a specified cryptographic algorithm ***[assignment: Triple DES in CBC mode]*** and cryptographic key sizes ***[assignment: 112 bits]*** that meet the following: ***[assignment: [CIR-EU-2016/799] Annex 1C, Appendix 11 Part A, Chapter 3]*** .

6.1.3 FDP: User data protection

6.1.3.1 FDP_ACC.1: Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***[assignment: access control SFP]*** on ***[assignment:***

Subjects:
- Vehicle unit
- Other device
Objects
-TOE symmetric keys (see Table 14 and Table 15 of [BSI-CC-PP-0093])
-Encrypted KP (with KM) and encrypted motion sensor serial number (with KID)
-TOE executable code
-TOE file system
-Motion sensor identification data
-Pairing data from first pairing
-Motion data
-Commands, actions, or test points, specific to the testing needs of the manufacturing phase
Operations
Read, write, modify, delete] .

6.1.3.2 FDP_ACF.1: Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to objects based on the following: ***[assignment: Subjects:***
-Vehicle unit
- Other device
Objects
-TSF secret keys (see Table 14 of [BSI-CC-PP-0093] and Table 15 of [BSI-CC-PP-0093])
-Encrypted K_P (with K_M) and encrypted motion sensor serial number (with K_{ID})
-TOE executable code
-TOE file system
-Motion sensor identification data

-Pairing data from first pairing
-Motion data
-Commands, actions, or test points, specific to the testing needs of the manufacturing phase] .

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[assignment: a)The send data and pairing functions of the TOE are only accessible to an authenticated vehicle unit, according to [ISO 16844-3:2004];***
b) Identification data, encrypted KP, encrypted motion sensor serial number and pairing data from first pairing shall be written once only;
c) Secret keys shall not be externally readable;
d) The TOE file system and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion;
e)All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase, and it shall not be possible to restore them for later use;
f) Unauthenticated inputs from external sources shall not be accepted as executable code ;
g) The TSF shall export motion data to the vehicle unit such that the vehicle unit can verify its integrity and authenticity;
h)Motion data shall only be processed and derived from the TOE's mechanical input] .

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***[assignment: none]***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***[assignment: none]***.

6.1.3.3 FDP_ETC.1: Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

Application Note

FDP_ETC.1 covers the requirement to send motion data, including audit records, to the VU.

6.1.3.4 FDP_ETC.2: Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: ***[assignment: none]***.

6.1.3.5 FDP_ITC.1: Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***[assignment: cryptographic session keys will only be accepted from a VU that has been successfully paired with the TOE]***.

Application Note

FDP_ITC.1 covers the import of the motion sensor session key from the VU during pairing.

6.1.3.6 FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for ***[assignment: integrity errors]*** on all objects, based on the following attributes: ***[assignment: data checksum]***.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall ***[assignment: generate an audit record]***.

6.1.4 FIA: Identification and authentication

6.1.4.1 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***[assignment: 20]*** unsuccessful authentication attempts occur related to ***[assignment: pairing of a vehicle unit]***.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[selection: met, surpassed]***, the TSF shall ***[assignment: a) generate an audit record of the event;***
b) continue to export motion data in a non-secured mode (speed pulses only)].

6.1.4.2 FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: ***[assignment: Pairing data from***
a) first pairing with a VU;
b) last pairing with a VU.].

6.1.4.3 FIA_UAU.2/1: User authentication before any action

FIA_UAU.2.1/1 The TSF shall require each user to be successfully authenticated ***using the method described in [CIR-EU-2016/799] Annex 1C, Appendix 11, Part A, Chapter 12*** before allowing any other TSF-mediated actions on behalf of that user.

Application Note

In the case of a motion sensor authentication (pairing) can be done only in the presence of a workshop card.

6.1.4.4 FIA_UAU.2/2: User authentication before any action

FIA_UAU.2.1/2 The TSF shall require each user to be successfully authenticated ***using the method described in [CIR-EU-2016/799] Annex 1C, Appendix 11, Part A, Chapter 3*** before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.5 FIA_UAU.3: Unforgeable authentication

FIA_UAU.3.1 The TSF shall ***[selection: detect, prevent]*** use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall ***[selection: detect, prevent]*** use of authentication data that has been copied from any other user of the TSF.

Application Note

"User" in FIA_UAU.3 includes any attacker.

6.1.4.6 FIA_UID.2: User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note

The identification of the user is achieved during pairing of the motion sensor and the vehicle unit.

6.1.5 FPT: Protection of the TSF

6.1.5.1 FPT_FLS.1: Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: ***[assignment: a)Reset;***
b)Power supply cut-off;
c)Deviation from the specified values of the power supply;
d)Transaction stopped before completion] .

6.1.5.2 FPT_PHP.2: Notification of physical attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For ***[assignment: motion sensor case opening]***, the TSF shall monitor the devices and elements and notify ***[assignment: a paired VU]*** when physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note

Option from the PP **[BSI-CC-PP-0093]** application note is used: If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected and FPT_PHP.2.3 is not relevant (penetration of the case by other means is addressed by FPT_PHP.2.2). – The sensor is sealed to the gearbox; the seal consists of a wire which is put through the hole on the sensor's connector made for this purpose and through the hole on the gearbox side. Both ends of the wire are sealed with a seal stamp. Therefore, any attempt to open it is easily visible and detectable from the outside.

6.1.5.3 FPT_PHP.3/1: Resistance to physical attack

FPT_PHP.3.1/1 The TSF shall resist ***[assignment: use of magnetic fields to disturb vehicle motion detection]*** to the ***[assignment: TOE components implementing the TSF]*** by responding automatically such that the SFRs are always enforced.

Application Note

FPT_PHP.3/1, according to the application note #9 in **[BSI-CC-PP-0093],** this requirement is addressed by being immune to magnetic fields, thanks to the usage of the two sensing elements (according to EU patent no. 29650931). At least one sensing element always stays functional.

6.1.5.4 FPT_PHP.3/2: Resistance to physical attack

FPT_PHP.3.1/2 The TSF shall resist ***[assignment: physical tampering attacks]*** to the ***[assignment: TSF software and TSF data]*** by responding automatically such that the SFRs are always enforced.

6.1.5.5 FPT_TDC.1/1: Inter-TSF basic TSF data consistency

FPT_TDC.1.1/1 The TSF shall provide the capability to consistently interpret ***[assignment: secure messaging attributes as defined by [CIR-EU-2016/799] Annex 1C, Appendix 11 Part B]]*** when shared between the TSF and ~~***another trusted IT product.***~~ ***a vehicle unit.***

FPT_TDC.1.2/1 The TSF shall use ***[assignment: the interpretation rules (communication protocols) as defined by [CIR-EU-2016/799] Annex 1C, Appendix 11 Part B]*** when interpreting the TSF data from ~~***another trusted IT product.***~~ ***a vehicle unit.***

6.1.5.6 FPT_TDC.1/2: Inter-TSF basic TSF data consistency

FPT_TDC.1.1/2 The TSF shall provide the capability to consistently interpret ***[assignment: secure messaging attributes as defined by [CIR-EU-2016/799] Annex 1C, Appendix 11 Part A, Chapter 5]*** when shared between the TSF and ~~***another trusted IT product.***~~ ***a vehicle unit.***

FPT_TDC.1.2/2 The TSF shall use ***[assignment: the interpretation rules (communication protocols) as defined by [CIR-EU-2016/799] Annex 1C, Appendix 11 Part A, Chapter 5]*** when interpreting the TSF data from ~~***another trusted IT product.***~~ ***a vehicle unit.***

6.1.5.7 FPT_TST.1: TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests ***[selection: during initial start-up, periodically during normal operation]*** to demonstrate the correct operation of ***[selection: [assignment: the TSF]]***.

FPT_TST.1.2 The TSF shall ~~***provide authorised users with the capability***~~ ***run a suite of self tests*** to verify the integrity of ***[selection: TSF data]*** .

FPT_TST.1.3 The TSF shall ~~***provide authorised users with the capability***~~ ***run a suite of self tests*** to verify the integrity of ***[selection: TSF software]***.

Application Note

The periodicity of self-tests and the justification of the appropriateness of this strategy is provided in the TOE Summary Specification of this Security Target, (section 7.6 SF.Integrity).

6.1.6 FRU: Resource utilisation

6.1.6.1 FRU_PRS.1: Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to ***[assignment: information processed in the motion sensor needed for pairing and correct functioning]*** shall be mediated on the basis of the subjects assigned priority.

Application Note

Controlled resources are information which are processed in sensor and they concern information needed for pairing and correct functioning - motion data transmission. The priority is given by a preset instruction sequence which is defined both for the sensor and VU in specification **[ISO 16844-3:2004]**. Additional details are provided in TOE Summary Specification, section 7.5 (SF.Access).

6.1.7 FTP: Trusted path/channels

6.1.7.1 FTP_ITC.1: Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~***another trusted IT product***~~ ***the vehicle unit*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[selection: another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[assignment: all communications with the vehicle unit]***.

6.2 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL4 + ATE_DPT.2 + AVA_VAN.5**

The following table shows the assurance requirements by reference the individual components in [CC31R5P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_TSS.1: TOE summary specification ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_SPD.1: Security problem definition
ALC: Life-cycle support	ALC_CMC.4: Production support, acceptance procedures and automation ALC_CMS.4: Problem tracking CM coverage ALC_DEL.1: Delivery procedures ALC_DVS.1: Identification of security measures ALC_LCD.1: Developer defined life-cycle model ALC_TAT.1: Well-defined development tools
ADV: Development	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
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_COV.2: Analysis of coverage ATE_FUN.1: Functional testing ATE_IND.2: Independent testing - sample ATE_DPT.2: Testing: security enforcing modules
AVA: Vulnerability assessment	AVA_VAN.5: Advanced methodical vulnerability analysis

Table 5 Security Assurance Requirements

6.3 Security Requirements Rationale

6.3.1 Necessity and sufficiency analysis

SFR / TOE Security Objective	O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update
FAU_GEN.1			X				X			
FAU_STG.1			X							
FAU_STG.4			X							
FDP_ACC.1		X		X		X				X
FDP_ACF.1		X		X		X				X
FDP_ETC.1	X		X							
FDP_ETC.2	X									
FDP_ITC.1				X				X	X	
FDP_SDI.2	X				X	X				
FIA_AFL.1				X						
FIA_ATD.1				X						
FIA_UAU.3	X	X		X				X		
FIA_UID.2	X	X		X				X		
FPT_FLS.1						X				
FPT_PHP.2	X					X	X			
FPT_PHP.3/1	X					X	X			

SFR / TOE Security Objective	O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update
FPT_PHP.3/2	X					X	X			
FPT_TST.1	X				X	X				
FRU_PRS.1					X	X				
FTP_ITC.1	X							X		
FCS_CKM.4/1				X				X	X	
FCS_COP.1/1: AES				X				X	X	
FIA_UAU.2/1	X	X		X				X		
FPT_TDC.1/1	X				X	X				
FCS_CKM.4/2				X				X	X	
FCS_COP.1/2: TDES				X				X	X	
FIA_UAU.2/2	X	X		X				X		
FPT_TDC.1/2	X				X	X				

Table 6 SFRs / TOE Security Objectives coverage

Figure 11 *Mapping of SFRs to TOE Security Objectives*

6.3.2 Security Requirement Sufficiency

O.Sensor_Main: **FDP_ETC.1**. Addresses the export of motion data in compliance with policy.

FDP_ETC.2. The motion sensor serial number is exported to support verification of motion data authenticity.

FDP_SDI.2. Requires the TOE to monitor stored data for integrity errors.

FIA_UAU.2/1, **FIA_UAU.2/2**, **FIA_UAU.3** & **FIA_UID.2**. These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
FPT_PHP.2. Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
FPT_PHP.3/1 & **FPT_PHP.3/2** require resistance to or reaction to magnetic physical attack that may interfere with motion data supply and they also require resistance to physical attacks designed to access TSF software.
FPT_TST.1. Self-tests help to ensure that the TOE is operating correctly.
FTP_ITC.1. Requires use of a secure channel for communication with the VU.
FPT_TDC.1/1 & **FPT_TDC.1/2** require a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.

O.Access: **FDP_ACC.1** & **FDP_ACF.1**. Defines the access control policy for the TOE.
FIA_UAU.2/1, **FIA_UAU.2/2**, **FIA_UAU.3** & **FIA_UID.2**. These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.

O.Audit: **FAU_GEN.1**. Specifies what must be audited.
FAU_STG.1. Requires that the audit records are protected against unauthorised deletion while held on the TOE.
FAU_STG.4. Specifies the actions to be taken when the available storage for audit records on the TOE is full.
FDP_ETC.1. Requires that recorded audit records are transmitted to the vehicle unit for storage.

O.Authentication: **FDP_ACC.1FDP_ACF.1**. Defines policy for protection of TOE identification data.

FDP_ITC.1. Provides for the import of cryptographic session keys from the VU.
FIA_ATD.1, **FIA_UAU.2/1**, **FIA_UAU.2/2**, **FIA_UAU.3** & **FIA_UID.2**. These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
FIA_AFL.1. Defines the actions to be taken when there is an authentication failure with the VU.
FCS_CKM.4/1, **FCS_CKM.4/2**, **FCS_COP.1/1: AES** & **FCS_COP.1/2: TDES**. Define the required cryptography to be used by the TOE for authentication.

O.Processing: **FDP_SDI.2**. Requires the TOE to monitor stored data for integrity errors.
FPT_TST.1. Self-tests help to ensure that the TOE is operating correctly.
FPT_TDC.1/1 & **FPT_TDC.1/2**. Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.
FRU_PRS.1. Ensuring that access to resources is correctly prioritised assists in ensuring that the TOE processes motion data correctly.

O.Reliability: **FDP_ACC.1FDP_ACF.1**. Requires that testing commands, actions and test points are disabled to prevent their use by an attacker.

FDP_SDI.2. Requires the TOE to monitor stored data for integrity errors.
FPT_FLS.1. Requires the TOE to preserve a secure state in the event of certain failure events.
FPT_PHP.2. Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
FPT_PHP.3/1 & **FPT_PHP.3/2** require resistance to or reaction to magnetic physical attack that may interfere with motion data supply and they also require resistance to physical attacks designed to access TSF software.

FPT_TDC.1/1 & **FPT_TDC.1/2**. Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.

FPT_TST.1. Self-tests help to ensure that the TOE is operating correctly.

FRU_PRS.1. Ensuring that access to resources is correctly prioritised assists in ensuring that the TOE operates reliably.

O.Physical: **FAU_GEN.1**. Audit records are stored when attempted physical tampering is detected.

FPT_PHP.2. Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
FPT_PHP.3/1 & **FPT_PHP.3/2** require resistance to or reaction to magnetic physical attack that may interfere with motion data supply and they also require resistance to physical attacks designed to access TSF software.

O.Secure_Communication: **FCS_CKM.4/1**, **FCS_CKM.4/2**, **FCS_COP.1/1: AES** & **FCS_COP.1/2: TDES**. Define the required cryptography to be used by the TOE for authentication and data protection.

FDP_ITC.1. Provides for the import of cryptographic session keys from the VU.
FIA_UAU.2/1, **FIA_UAU.2/2**, **FIA_UAU.3** & **FIA_UID.2**, These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
FTP_ITC.1. Requires use of a secure channel for communication with the VU.

O.Crypto_Implement: **FCS_CKM.4/1**, **FCS_CKM.4/2**, **FCS_COP.1/1: AES** & **FCS_COP.1/2: TDES**. These requirements define the required cryptography to be used by the TOE for authentication and data protection.
FDP_ITC.1. Provides for the import of cryptographic session keys from the VU.

O.Software_Update: **FDP_ACC.1** & **FDP_ACF.1**. Require that unauthenticated software is not accepted.

6.3.3 SFR Dependency Rationale

6.3.3.1 Table of SFR dependencies

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FAU_GEN.1	FPT_STM.1	None	FPT_STM.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1	FMT_MSA.3
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1	None
FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1	None
FDP_ITC.1	FMT_MSA.3, [FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1	FMT_MSA.3
FDP_SDI.2	None	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2/1 (h.a. FIA_UAU.1), FIA_UAU.2/2 (h.a. FIA_UAU.1)	None
FIA_ATD.1	None	None	None
FIA_UAU.3	None	None	None
FIA_UID.2	None	None	None
FPT_FLS.1	None	None	None
FPT_PHP.2	FMT_MOF.1	None	FMT_MOF.1
FPT_PHP.3/1	None	None	None
FPT_PHP.3/2	None	None	None
FPT_TST.1	None	None	None
FRU_PRS.1	None	None	None
FTP_ITC.1	None	None	None
FCS_CKM.4/1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1	None
FCS_COP.1/1: AES	FCS_CKM.4, [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.4/1, FDP_ITC.1	None
FIA_UAU.2/1	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FPT_TDC.1/1	None	None	None
FCS_CKM.4/2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1	None
FCS_COP.1/2: TDES	FCS_CKM.4, [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.4/2, FDP_ITC.1	None
FIA_UAU.2/2	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FPT_TDC.1/2	None	None	None

Table 7 SFR Dependencies

6.3.3.2 Justification for missing dependencies

FAU_GEN.1 dependency on FPT_STM.1

Audit records are indicated to the vehicle unit as soon as they are available. The audit records are then transferred to the vehicle unit, which itself generates and stores motion sensor related events as defined by [CIR-EU-2016/799] Chapters 3.9, 3.12.8 and 3.12.9 and Appendix 1. Time stamping of these events is based on the vehicle unit internal clock. The requirement for the TOE to provide reliable time stamps is therefore not needed.

FDP_ACF.1 dependency on FMT_MSA.3

The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Manufacturing Phase, and are fixed over the whole life time of the TOE. No management of default values for these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during the fitters and workshops phase, or within the usage phase of the TOE.

FDP_ITC.1 dependency on FMT_MSA.3

There is no requirement for management of default values for the key values that are imported, and no concept of restrictive or permissive values for the cryptographic keys. The dependency on FMT_MSA.3 is not relevant in this case.

FPT_PHP.2 dependency on FMT_MOF.1

CC Part 2 paragraph 1220 states that the use of FMT_MOF.1 should be considered to specify who can make use of the capability, and how they can make use of the capability. Since the capability, if implemented, is always enabled use of FMT_MOF.1 is not relevant.

6.3.4 SAR Rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by **[CIR-EU-2016/799]** Annex 1C, Appendix 10.

This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects, entry 'Attacker' of **[BSI-CC-PP-0093]**). This decision represents a part of the conscious security policy for the recording equipment required by the regulations and reflected by **[BSI-CC-PP-0093]** Protection Profile.
The set of assurance requirements being part of EAL4 fulfills all dependencies a priori.
The augmentation of EAL4 chosen comprises the following assurance components:
– ATE_DPT.2 and
– AVA_VAN.5.
For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package.

Component	Dependencies required by CC Part 3	Dependency satisfied by
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

6.3.5 SAR Dependency Rationale

6.3.5.1 Table of SAR dependencies

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2 (hierarchically above ASE_REQ.1)	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (hierarchically above ASE_REQ.1), ADV_FSP.4 (hierarchically above ADV_FSP.1)	None
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	ALC_CMS.4 (hierarchically above ALC_CMS.1), ALC_DVS.1, ALC_LCD.1	None
ALC_CMS.4	None	None	None
ADV_FSP.4	ADV_TDS.1	ADV_TDS.3 (hierarchically above ADV_TDS.1)	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.4 (hierarchically above ADV_FSP.1)	None
AGD_PRE.1	None	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.4 (hierarchically above ADV_FSP.2), AGD_OPE.1, AGD_PRE.1, ATE_COV.2 (hierarchically above ATE_COV.1), ATE_FUN.1	None
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2 (hierarchically above ATE_DPT.1)	None
ASE_SPD.1	None	None	None
ALC_DEL.1	None	None	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.4 (hierarchically above ADV_FSP.1), ADV_TDS.3 (hierarchically above ADV_TDS.1)	None
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_TDS.3, ALC_TAT.1	None

SAR	Required	Fulfilled	Missing
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4	None
ALC_DVS.1	None	None	None
ALC_LCD.1	None	None	None
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1	None
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.4 (hierarchically above ADV_FSP.2), ATE_FUN.1	None
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.2 (hierarchically above ATE_COV.1)	None

Table 8 SAR dependencies

7 TOE Summary Specification

Each of the security requirements and the associated descriptions correspond to security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. The TSF protects itself from interference and logical tampering from untrusted subjects or external entities by the use of SF.Authentication, SF.Audit, SF.Crypto, SF.Flow, SF.Access and SF.Integrity. The TSF protects itself from physical tampering by the use of SF.Casing and SF.Magnetic_Fields (**FPT_PHP.2**, **FPT_PHP.3/1** and **FPT_PHP.3/2**). The TSF prevents the bypass of security enforcement functionality by the use of SF.Authentication, SF.Audit, SF.Crypto, SF.Flow, SF.Access, SF.Integrity, SF.Casing and SF.Magnetic_Fields.

7.1 SF.Audit

This Security Function is related to the following SFRs of the TOE: **FAU_GEN.1**, **FIA_UID.2**, **FIA_UAU.2/1**, **FIA_UAU.2/2**, **FIA_UAU.3**, **FDP_SDI.2**, **FIA_AFL.1**, **FPT_TST.1**, **FAU_STG.1**, **FAU_STG.4** and **FDP_ETC.1**

FAU_GEN.1 generates audit events. Identification and authentication, and related audit events are provided by **FIA_UID.2, FIA_UAU.2/1**, **FIA_UAU.2/2** and **FIA_UAU.3**. **FDP_SDI.2** provides stored data integrity error events. **FIA_AFL.1** provides authentication failure events. **FPT_TST.1** provides TSF self-test failure events. A security audit record is generated when any type of security error in the MS occurs; e.g. data integrity error, authorization error, or communication error.

FAU_STG.1 provides protection to unauthorized deletion and/or modification to the protected audit storage. Additionally, **FAU_STG.4** specifies actions in case the audit trail is full (prevention of audit data loss).

FDP_ETC.1 allows the TOE to export audit records to the VU, enforcing access control policy, and exporting the data without associated security attributes.

7.2 SF.Authentication

This Security Function is related to the following SFRs of the TOE: **FAU_GEN.1**, **FCS_CKM.4/1**, **FCS_CKM.4/2**, **FCS_COP.1/1: AES**, **FCS_COP.1/2: TDES**, **FDP_ITC.1**, **FDP_ETC.1**, **FIA_AFL.1**, **FIA_UID.2**, **FIA_UAU.2/1**, **FIA_UAU.2/2**, **FIA_UAU.3 FDP_ETC.2** and **FIA_ATD.1**.

The following features related to authentication are implemented in the TOE:

- Mutual authentication between the MS and the VU during pairing.
    - Processed according to the **[ISO 16844-3:2004]**, section 7.4.2 and Annex 1C, Appendix 11, Part B, chapter 12 of **[CIR-EU-2016/799]**.
- Authentication failure handling.
    - After 20 unsuccessful authorization attempts the TOE generates an audit record (error message).

- After 20 unsuccessful authorisation attempts the MS also stops responding, until the authorised VU is connected: it blocks unauthorised key testing / hacking (notice that ACKs still are sent to incoming messages as required by the communication protocol as described in **[ISO 16844-3:2004],** but no additional response to the command is provided). The only exception is that the TOE continues to export motion data in a non-secured mode, by sending only speed pulses on pin 3.

- Unforgeable user identification and authentication before any action.

FAU_GEN.1 associates the audit events with the VU identity.

FCS_CKM.4/1 and **FCS_CKM.4/2** replace the old session key with the new session key, which is part of the authentication during pairing.

FCS_COP.1/1: AES and **FCS_COP.1/2: TDES** encrypt and decrypt data, which is part of the authentication during pairing.

FDP_ITC.1, **FDP_ETC.1** and **FDP_ETC.2** provide information flow control when importing and exporting data during the authentication and pairing. This information could also contain security attributes.

FIA_AFL.1 provides authentication failure handling.

FIA_ATD.1 provides user attribute definition. This SFR allows user security attributes for each user to be maintained individually.

Identification and authentication are provided by **FIA_UID.2**, **FIA_UAU.2/1**, **FIA_UAU.2/2** and **FIA_UAU.3**.

7.3 SF.Crypto

This Security Function is related to the following SFRs of the TOE: **FCS_CKM.4/1**, **FCS_CKM.4/2**, **FCS_COP.1/1: AES**, **FCS_COP.1/2: TDES**, **FPT_TDC.1/2**, **FPT_TDC.1/1**, and **FTP_ITC.1**.

SF.Crypto includes the implementation of Cryptographic key distribution, import and destruction; encryption and decryption; data exchange integrity related functionality:

- The import of a session key, KS, from the VU during pairing.
  - Processed according to the **[ISO 16844-3:2004]**, section 7.4.6.
- The export of a pairing key, KP, to the VU during pairing.
  - Processed according to the **[ISO 16844-3:2004]**, section 7.4.4.3.
- Destruction of old session key by replacement with a 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 16844-3:2004]**.

- Encryption and decryption of data, with the session key, for the transmission of data between the MS and the VU.
- Additional requirements for smart digital tachographs in Annex 1C, Appendix 11, Part B, chapter 12 of **[CIR-EU-2016/799]**.

To provide data integrity and data confidentiality protection during transmission between the MS and the VU, first mutual authentication is needed – which takes place during pairing and is handled by SF.Authentication. Secondly, they need to establish a common secret, a session key. Now secure data exchange in accordance with **[ISO 16844-3:2004]** can begin.

FCS_CKM.4/1 and **FCS_CKM.4/2** replace the old session key with the new session key, which is part of the authentication during pairing.

The TOE implements communication vehicle units (VU) according to the protocol defined by **[CIR-EU-2016/799]** Annex 1C, Appendix 11 Part B, including consistent interpretation of secure message attributes (**FPT_TDC.1/1**) and also according to the protocol defined by **[CIR-EU-2016/799]**, Annex 1C, Appendix 11 Part A, Chapter 5, including consistent interpretation of secure message attributes as well (**FPT_TDC.1/2**).

FCS_COP.1/1: AES and **FCS_COP.1/2: TDES** encrypt and decrypt data, which is part of the authentication during pairing and it is also how the data exchange is secured after pairing.

FTP_ITC.1 ensures the trusted channel between the MS and the VU which is provided by the security mechanism above.

7.4 SF.Flow

This Security Function is related to the following SFRs of the TOE: **FDP_ITC.1** and **FDP_ETC.1**.

FDP_ITC.1 and **FDP_ETC.1** provides information flow control when importing and exporting data during the authentication and pairing. The VU is always the communication master. The VU sends a request and the MS responds, if the VU is authorised.

7.5 SF.Access

This Security Function is related to the following SFRs of the TOE: **FDP_ACC.1**, **FDP_ACF.1**, **FIA_UID.2**, **FIA_UAU.2/1**, **FIA_UAU.2/2**, **FIA_UAU.3** and **FRU_PRS.1**. and provides functionality related to Access control to TOE functions.

Function access control is provided by **FDP_ACC.1** and **FDP_ACF.1**.
Identification and authentication are provided by **FIA_UID.2**, **FIA_UAU.2/1**, **FIA_UAU.2/2** and **FIA_UAU.3**.

FRU_PRS.1 helps to provide priorities for a subject's use of the resources under the control of the TSF. Controlled resources are information which are processed in sensor and they concern information

needed for pairing and correct functioning - motion data transmission. The priority is given by a preset instruction sequence which is defined both for the sensor and VU in specification **[ISO 16844-3:2004]**.

7.6 SF.Integrity

This Security Function is related to the following SFRs of the TOE: **FPT_TST.1**, **FPT_FLS.1** and **FDP_SDI.2**, related to Integrity protection, checksums:

- Stored data integrity monitoring.
    - Stored data are checked for integrity during start-up and periodically during operation by the use of checksums. This is provided by **FDP_SDI.2**.
- TSF self-testing.
    - Stored data and software code are checked for integrity during start-up and periodically during operation by the use of checksums. This strategy is aims to check if the crucial data in Flash memory (including the keys) are not damaged. This is provided by **FPT_TST.1**.
- 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. This is provided by **FPT_FLS.1**.

7.7 SF.Magnetic_Fields

This Security Function is related to the following SFRs of the TOE: **FPT_PHP.3/1** and **FPT_PHP.3/2**

FPT_PHP.3/1 and **FPT_PHP.3/2** provide to the TOE the capability of resist the use of magnetic fields to disturb vehicle motion detection. Moreover, this Security Function offers resistance to physical tampering attacks by responding automatically such that the SFRs are always enforced.

7.8 SF.Casing

This Security Function is related to the following SFR of the TOE: **FPT_PHP.2**

FPT_PHP.2 provides physical tampering detection by the use of a protective casing capable of being sealed. Moreover, provides an automatic notification of tampering for an identified subset of physical penetrations. The motion sensor (MS) is connected and sealed to the gearbox during installation. The security seal used to seal the TOE cannot be broken or removed and re-attached without the user being able to detect the manipulation; and thereby provide the means of detecting physical tampering with the mechanical interface.

Automatic notification is not implemented as the case is not designed for opening – it is easily detectable if there was an attempt for physical tampering.

8 Acronyms

The following table shows the acronyms used in this Security Target

Acronym	Meaning
ST	Security Target
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
IT	Information Technology
OSP	Organizational Security Policy
EAL	Evaluation Assurance Level
TSC	TSF Scope of Control
TSS	TOE Summary Specification
AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
DES	Data Encryption Standard (see FIPS PUB 46-3)
EGF	External GNSS Facility
GNSS	Global Navigation Satellite System
MAC	Message Authentication Code
MS	Motion Sensor
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
TC	Tachograph Card
TDES	Triple-DES
TSP	TOE Security Policy
VU	Vehicle Unit

Table 9 Abbreviations

9 Glossary of Terms

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance
Application note	Informative part of the ST containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE.
Approved Workshops	Fitters and workshops installing, calibrating and (optionally) repairing motion sensors, and being approved to do so by an EU Member State, so that the assumption A.Approved_Workshops is fulfilled.
Attacker	A person, or a process acting on their behalf, trying to undermine the security policy defined by the current ST, especially to change properties of the assets that have to be maintained.
Authentication	A function intended to establish and verify a claimed identity.
Authentication data	Data used to support verification of the identity of an entity.
Authenticity	The property that information is coming from a party whose identity can be verified.
Calibration	Updating or confirming motion sensor parameters held in the data memory of a VU. Calibration of a VU requires the use of a workshop card.
Data memory	An electronic data storage device built into the motion sensor.
Digital Signature	Data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data.
Event	An abnormal operation detected by the motion sensor that may result from a fraud attempt.
Fault	An abnormal operation detected by the motion sensor that may arise from an equipment malfunction or failure.
Installation	The mounting of a motion sensor in a vehicle.
Integrity	The property of accuracy and completeness of information.

Term	Meaning
Interface	A facility between systems that provides the media through which they can connect and interact.
Manufacturer	The generic term for a manufacturer producing the motion sensor as the TOE.
Motion Sensor	A part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Motion sensor identification data	Data identifying the motion sensor: name of manufacturer, serial number, approval number, embedded security component identifier and operating system identifier. Motion sensor identification data are part of security data. These are stored in clear in the motion sensor's permanent memory.
Motion data	Data sent from the motion sensor to the paired vehicle unit, reflecting the vehicle's speed and distance travelled. There are two aspects of motion data: real time speed pulses sent from a motion sensor; and secure data communications between a motion sensor and a vehicle unit
Pairing	A process whereby, in the presence of a workshop card, a VU and a motion sensor mutually authenticate each other, and establish a session key to be used to protect the confidentiality and authenticity of motion data exchanged between them in operation.
Pairing Data	Pairing data contains encrypted information about the date of pairing, VU type approval number, and VU serial number of the vehicle unit with which the motion sensor was paired.
Personalisation	The process by which the equipment-individual data are stored in and unambiguously, inseparably associated with the related equipment.
Security Certification	Process to certify, by a Common Criteria certification body, that the TOE fulfils the security requirements defined in the relevant Protection Profile.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys and certificates).
Self Test	Tests run cyclically and automatically to detect faults.
Smart Tachograph System	The recording equipment, tachograph cards and the set of all directly or indirectly interacting equipment during their construction, installation, use, testing and control, such as cards, remote early detection communication readers and any other equipment for data downloading, data analysis, calibration, generating, managing or introducing security elements, etc.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1). In this ST TSF data the term security data is also used.
User	A legitimate user of the TOE, being a paired vehicle unit.
User data	Any data, other than security data, recorded or stored by the motion sensor. User data include motion sensor identification data and motion data. The CC gives the following generic definitions for user data:- Data

Term	Meaning
	created by and for the user that does NOT affect the operation of the TSF (CC part 1).- Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2).
Vehicle Unit	The tachograph excluding the motion sensor and the cables connecting the motion sensor.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
Workshop Card	A tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the user and allows for the testing, calibration and activation of tachographs, and/or downloading from them.

Table 10 *Glossary of terms*

10 Document References

The following table shows the documents referenced in this Security Target

Reference	Document
CC31R5P1	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
CC31R5P2	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
CC31R5P3	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
CEM31R5P3	Common Criteria Evaluation methodology, Version 3.1, Revision 5
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
CIR-EU-1360/2002	Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex I B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13 March 2004 (OJ L 71)
ISO 16844-3:2004	ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface, 1 November 2004
BSI-CC-PP-0093	BSI-CC-PP-0093
DT-site	European Commission – Joint Research Center – Digital Tachograph https://dtc.jrc.ec.europa.eu/dtc_smart_tachograph.php
ISO15170-1	ISO 15170-1:2001 Road vehicles – Four-pole electrical connectors with pins and twist lock – Part 1: Dimensions and classes of application.
TACH3-Catalogue	SENSOR FOR DIGITAL TACHOGRAPHS LESIKAR TACH3 (models M171, M171.1, M172, M173, M174, M175, M176, M193), Lesikar, a.s., product catalogue list
EN 16882:2016	Road vehicles. Security of the mechanical seals used on tachographs. Requirements and test procedures
CIR-EU-2018/502	COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

Table 11 *List of document references*