Date
2016-06-23

Classification
UNCLASSIFIED

Subject

Security Target – Sensor for digital tachograph LESIKAR TACH2

Contents

Figures

Tables

1 ST Introduction

1.1 ST Reference

Title:	Security Target – Sensor for digital tachograph LESIKAR TACH2
Version:	2.5
Date:	2016-06-23
Editors:	Daniel Poignant and Anders Staaf

1.2 TOE Reference

Target of Evaluation:	Sensor for digital tachograph LESIKAR TACH2 Models: M071, M071.1, M072, M073, M074, M075 and M076.
Version:	HW version 04, SW version 02
Developer:	Lesikar

1.3 Document Overview

This is the Security Target for the Lesikar motion sensor. This Security Target (ST) has been developed to outline the IT security requirements as defined in the EU Commission Regulation 1360/2002, Annex I(B) [Annex1B], Appendix 10 (ITSEC) [Annex1B_App10] (Motion Sensor Generic Security Target) in the Common Criteria (CC) language and format (CC version 3.1, Revision 4 [CC]). This ST is using some interpretations from the Protection Profile ‘Digital Tachograph – Vehicle Unit (VU PP) developed by BSI, Germany [VU-PP]. The VU PP has been approved by the governmental IT security certification bodies organised within the Joint Interpretation Working Group (JIWG) which is supporting the mutual recognition of certificates under the umbrella of the European SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates). The VU PP is also recognised under CCRA. The VU PP and this ST uses the interpretations from the Joint Interpretation Library “Security Evaluation and Certification of Digital Tachographs” [JIL].

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.

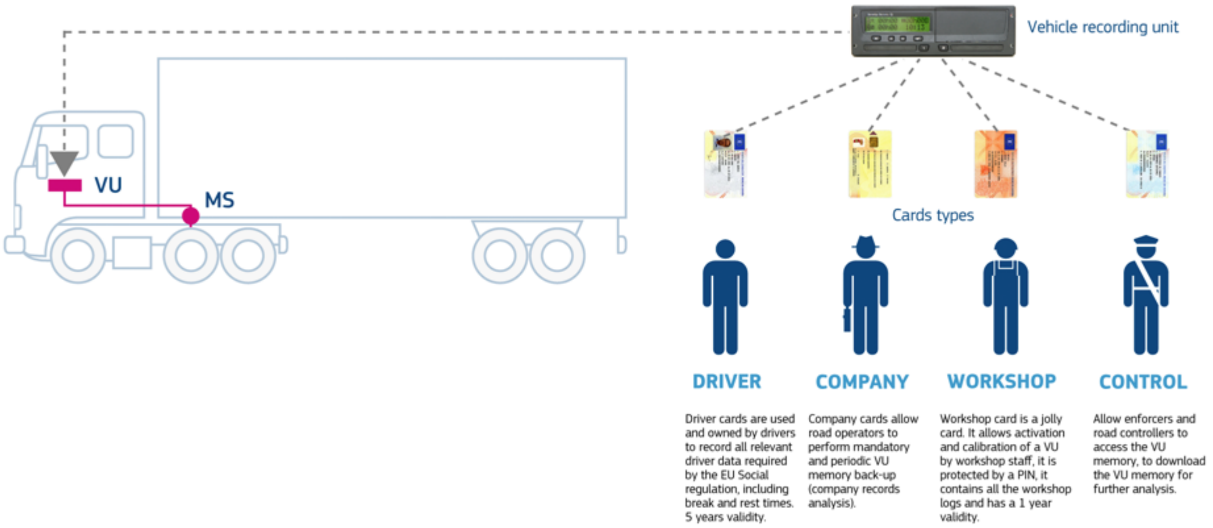
In chapter 6 the IT security functional and assurance requirements are stated for the TOE. These requirements are a selected subset of the requirements of part 2 and 3 of the Common Criteria standard.

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

1.4 TOE Overview

1.4.1 Digital Tachograph – System Overview

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



Driver cards are used and owned by drivers to record all relevant driver data required by the EU Social regulation, including break and rest times. 5 years validity.

Company cards allow road operators to perform mandatory and periodic VU memory back-up (company records analysis).

Workshop card is a jolly card. It allows activation and calibration of a VU by workshop staff, it is protected by a PIN, it contains all the workshop logs and has a 1 year validity.

Allow enforcers and road controllers to access the VU memory, to download the VU memory for further analysis.

Figure 1, The digital tachograph as described on the European Commission web site – VU, MS and card types

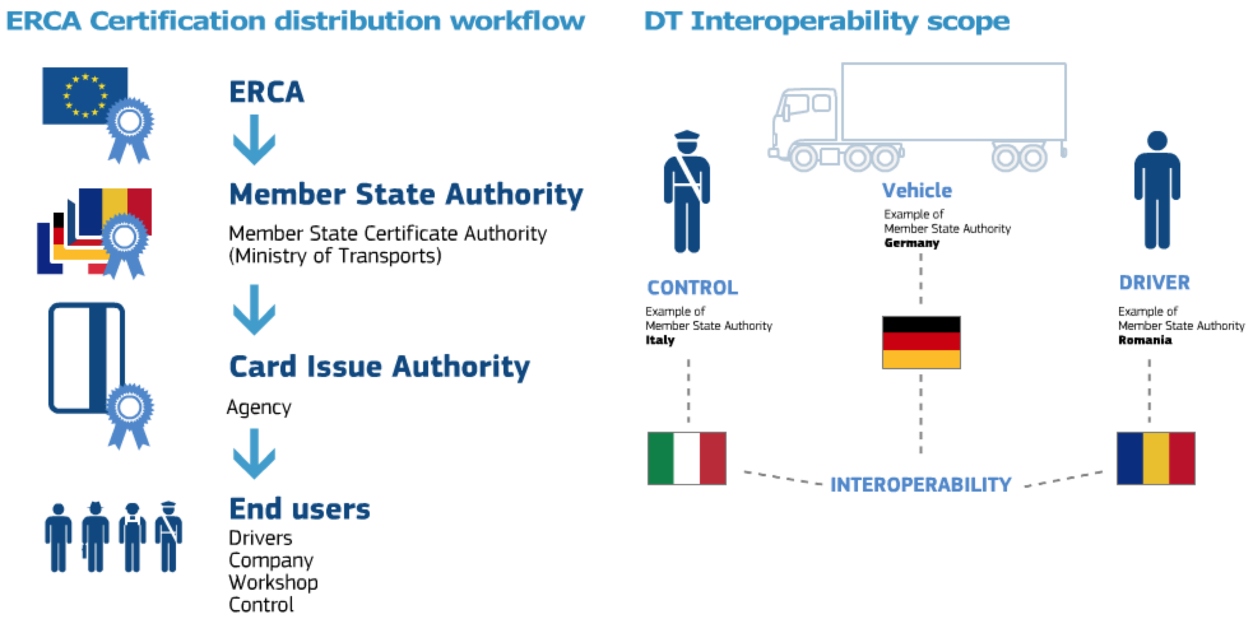


Figure 2, The digital tachograph as described on the European Commission web site – ERCA

Scope:

The 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.

1.4.2 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 [ISO16844-3]. This channel is used to respond to VU requests.

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 3.2.1) and TDES encryption/decryption in accordance with the interface specification [ISO16844-3], and described in the ST, section 1.5.2 “The cryptographic security model establishing the root of trust”. No PKI, certificates or asymmetric keys are used for this authentication.

1.4.3 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 [Regulation_2013] (Annex 1B 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.

For the TOE to operate securely and in accordance with the regulations the following security objectives for the operational environment of the TOE must be achieved:

OE.Approved_Workshops: Installation, calibration and repair of recording equipment shall be carried by trusted and approved fitters or workshops.

OE.Controls: Law enforcement controls shall be performed regularly and randomly, and must include security audits.

OE.Regular_Inspection: Recording equipment shall be periodically inspected and calibrated.

OE.Seal: A security seal shall be 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.

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 1.4.7.2. Also common security assurance requirements of the claimed EAL regarding product development, e.g. ADV and ALC, need to be fulfilled.

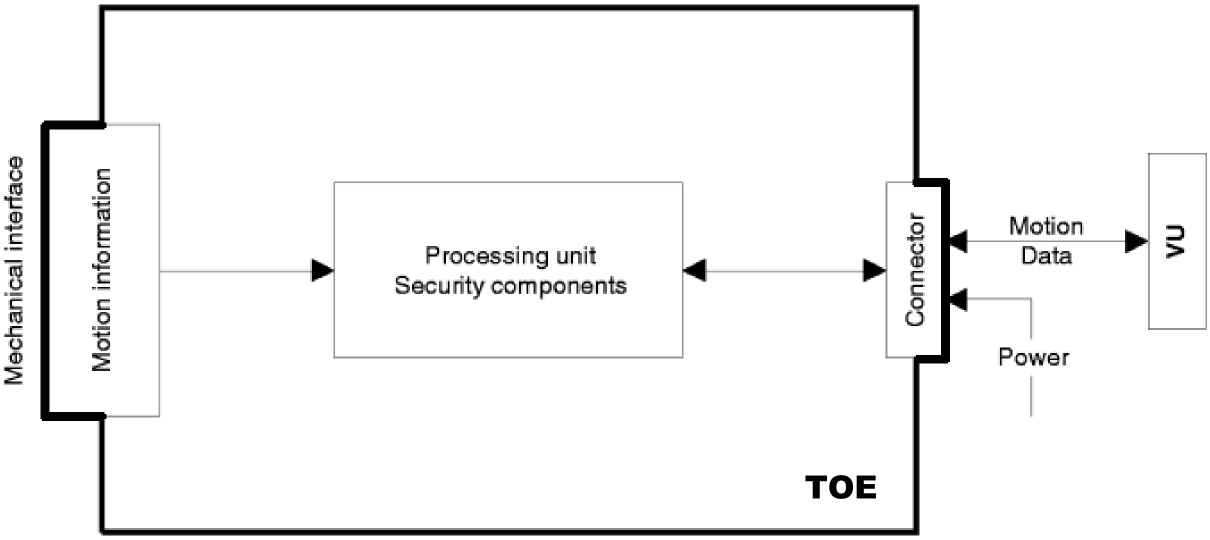


Figure 3, The schematics for a typical motion sensor

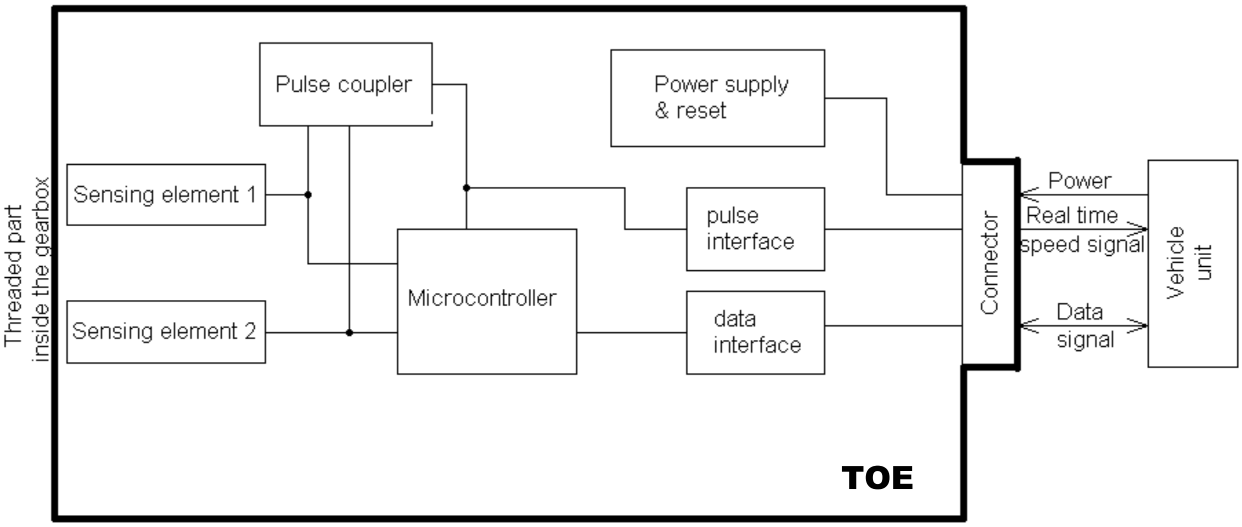


Figure 4, The schematics for the Sensor for digital tachograph LESIKAR TACH2

1.4.4 Major security features

As specified in [Annex1B_App10]; the main security objective of the digital tachograph system – motion sensor (the TOE) + vehicle unit (VU) + smartcard – is: “The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed” (O.Main). Therefore the security objective of the motion sensor, contributing to the global security objective, is: “The data transmitted by the motion sensor must be available to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance travelled” (O.Sensor_Main).

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 (OE.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 3.2.1, see also section 6.1.

1.4.4.1 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 3.2.1) and TDES encryption/decryption in accordance with the interface specification [ISO16844-3], and described in the ST, section 1.5.2 “The cryptographic security model establishing the root of trust”. No PKI, certificates or asymmetric keys are used for this authentication.

1.4.4.1.1 The authentication of the VU to the MS during pairing

The VU is authenticated to the MS during pairing as described in [ISO16844-3], sections 7.4.3 and 7.4.4; and in the ST, Figure 10:

- 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 [ISO16844-3], section 7.4.4.3.

1.4.4.1.2 The authentication of the MS to the VU during pairing

The MS is authenticated to the VU during pairing as described in [ISO16844-3], sections 7.4.4.3, 7.4.5, 7.4.6 and 7.4.7; and in the ST, Figure 10:

- 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, **$^{e}Km(K_P)$.**
- 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 $^{e}Km(K_P)$,** 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.**

1.4.4.2 Data integrity

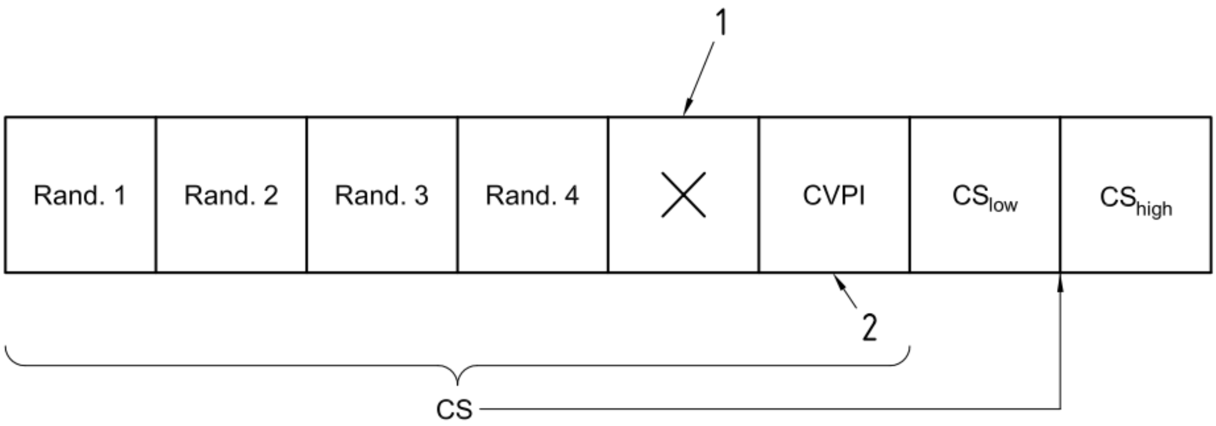
The data integrity as specified in [ISO16844-3], sections 7.1, 7.5 and 7.6; uses parity bits, LRC, checksums, counters and TDES encryption:

- 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 [ISO16844-3] 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, ${}^{e}K_S(D_A)$. **D_A = 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 7. 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.

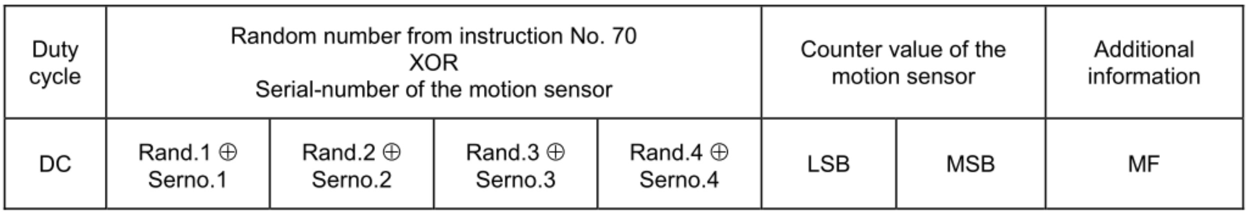
2 CheckSumlow of the previous instruction (instruction No. 10 or No 70) XORed with the low byte of the actually latched counter value.

Figure 5, Structure of authentication data after decryption, D_A

- The motion sensor have 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, ${}^{e}K_S(D_S)$. **D_S = 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, D_S

- The motion sensor responds to instruction 10 by submitting the data of the requested file encrypted with the session key, ${}^{e}K_S(D_{FS})$. D_{FS} = 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 [ISO16844-3], section 7.6.3.3.

1.4.5 TOE type

The TOE type is the Motion Sensor Unit in the sense of [Annex1B].

1.4.6 Required 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 [Annex1B], 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 1.5.2. 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 3.2.1.

1.4.7 Motion sensor life cycle

1.4.7.1 The life-cycle for a typical motion sensor

The typical life cycle of the motion sensor is described in the following figure from [Annex1B_App10]:

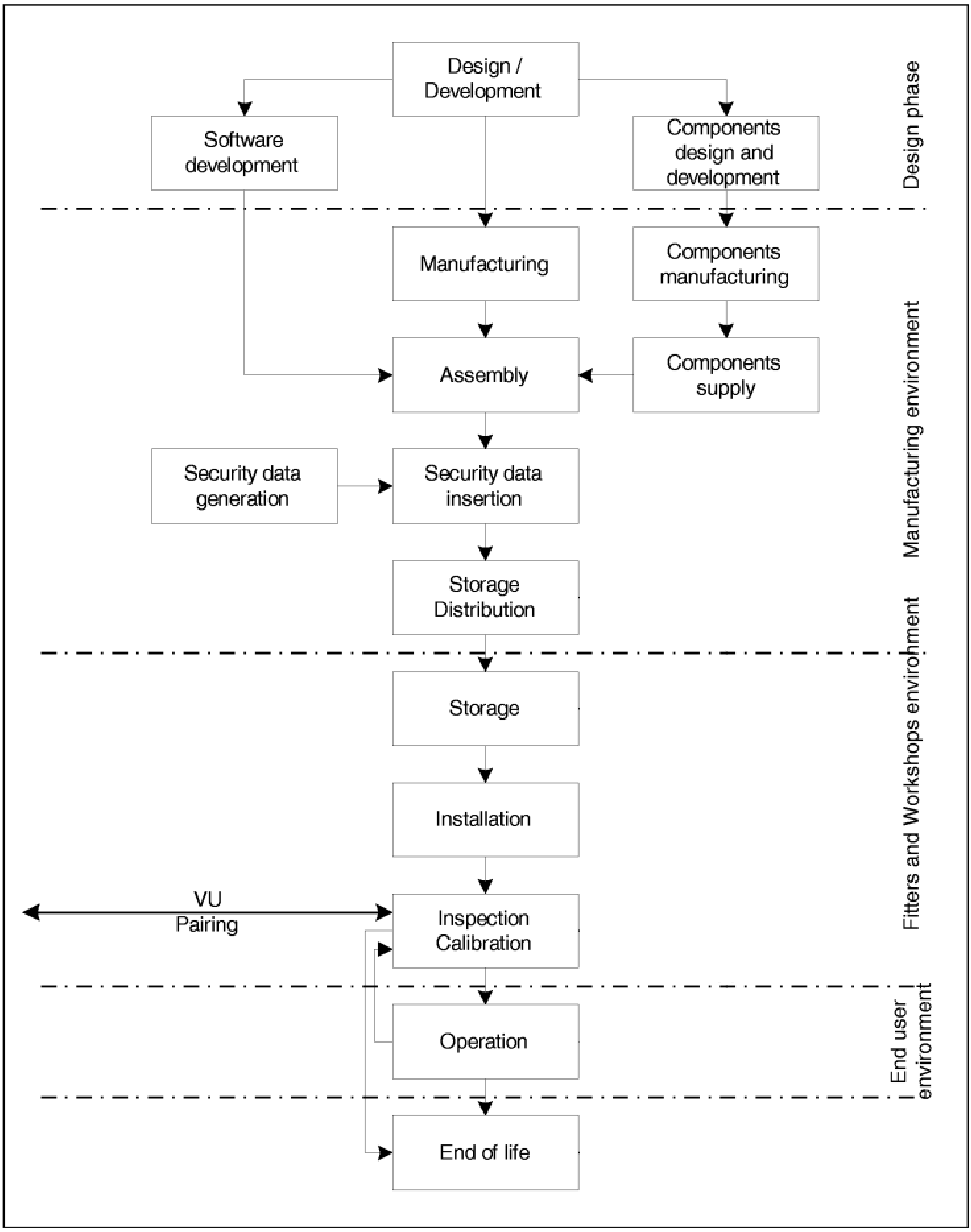


Figure 7, The life-cycle for a typical motion sensor

Note: The TOE as described in this ST is considered to be the product in the operational stage ready for pairing. In previous stages the TSF data needed for the cryptographic operations (cryptographic keys) is stored in the TOE (TOE personalisation and insertion of security data). Before use, the TOE first needs to be installed in the vehicle by an approved and trusted fitter or workshop. After installation the approved workshop attach a security seal (OE.Seal) according to regulations. During pairing with a VU, mutual authentication occurs and the TOE also gets a session key from the VU that is used to encrypt the communication between the TOE and the VU. See section 1.5.2. Also, the Sensor for digital tachograph LESIKAR TACH2, is not possible to repair. It must be replaced, if needed.

Note: Some of the requirements in the ITSEC Security Target of [Annex1B_App10] apply to the manufacturing phase of the product and the development environment. These requirements are covered by the security assurance requirements of EAL4+ ATE_DPT.2 and AVA_VAN.4 – not by SFRs.

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

- Insertion of security data: During the manufacturing the personalisation is performed and all MS identification data and all MS initial security data are installed. The steps required becoming ready for pairing regarding the cryptographic security model and the establishment of trust is described in section 1.5.2. The TOE as described in this ST is considered to be in this phase: “The TOE ready for installation and pairing”. This is how the motion sensor is delivered, see Figure 7 and section 3.2.1.
    - Personalisation – insertion of MS identification data and MS initial 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 production. 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, ${}^{e}Km(K_P)$. 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: The TOE is installed in a vehicle and sealed according to regulation by an approved fitter or workshop (OE.Seal), see Figure 7.
- Pairing: After installation and sealing the TOE is paired with the VU. Pairing is performed by an approved fitter or workshop, see Figure 7 and Figure 10.
- Operation: After pairing the TOE is installed as part of a digital tachograph system. This is the end-user operational phase, see Figure 7.

1.5 TOE Description

1.5.1 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.

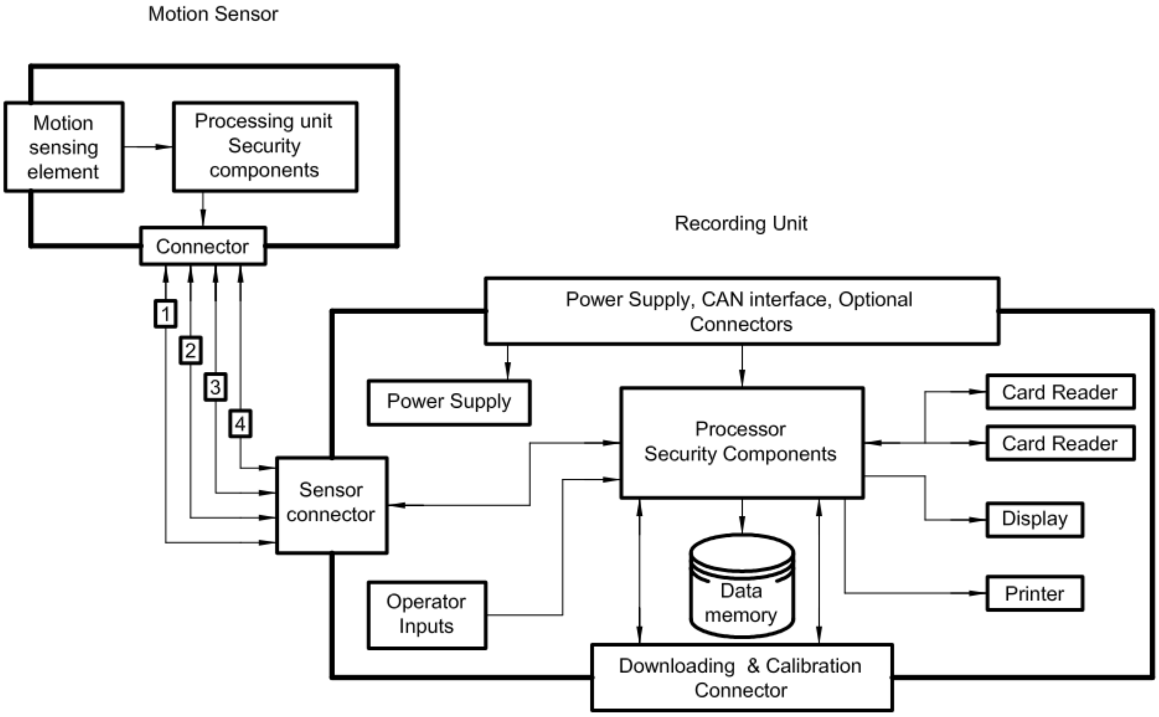
The interface between the motion sensor and the vehicle unit (physical, electrical and protocol levels) is designed to be compliant with ISO 16844-3:2004, Cor 1:2006 [ISO16844-3]. Input / Output signals and power are exchanged through an ISO 15170-1 4 pin connector [ISO15170-1].

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 1.5.2. 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 8, A typical tachograph system

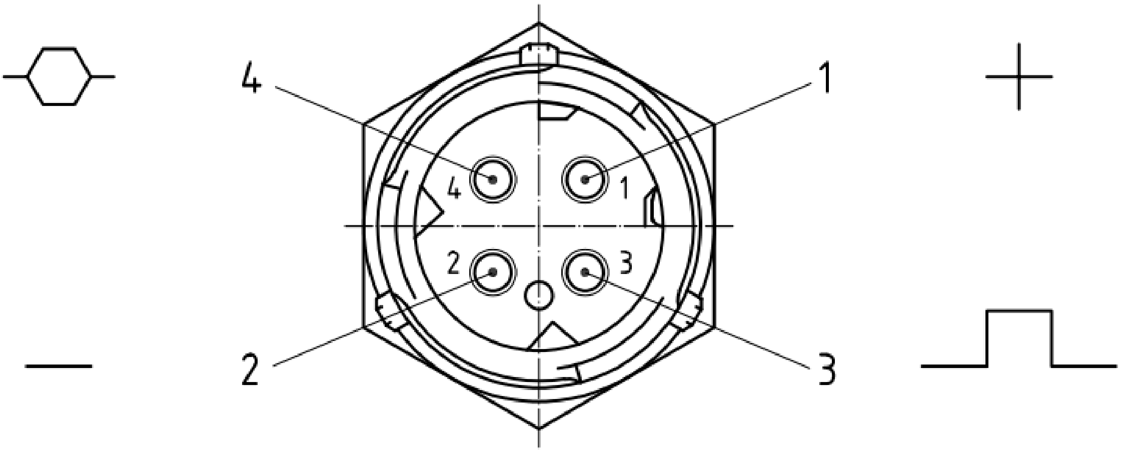


Figure 9, The ISO 15170-1 4 pin connector

1.5.2 The cryptographic security model establishing the root of trust

The cryptographic operations dictated in [Annex1B] and [ISO16844-3] for mutual authentication and data encryption between the motion sensor (MS) and the vehicle unit (VU):

- 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, N_S, 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 $(N_S||N_S)$
        - $n_{4\text{ byte}}$ is a 4 byte-long random number generated by the vehicle unit.
        - $P_D = {}^eK'_P[(n_{4\text{ byte}})||(\text{date of pairing})||(\text{VU type approval number})||(\text{VU serial number})]$

The sequence of instructions for pairing, see [ISO16844-3], 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 10, The sequence of instructions for pairing

1.5.3 Physical Scope

The physical scope of the TOE includes the following; see also Figure 4, The schematics for the Sensor for digital tachograph LESIKAR TACH2.

- TOE hardware:
  - The whole motion sensor including the casing.
    - Sensor for digital tachograph LESIKAR TACH2, models: M071, M071.1, M072, M073, M074, M075 and M076.
  - 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 (i.e. firmware):
  - The motion sensor software (i.e. firmware)
  - User data
  - TSF data (security data)
- The TOE documentation
  - The TOE operational guidance
  - The TOE preparative procedures

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 [ISO16844-3].

1.5.4 Logical Scope of the TOE

The 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

1.5.5 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 (OE.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.

1.5.6 Interfaces

- Mechanical interface between the sensor element and the gear box.
- The ISO 15170-1 connector to the VU and the power according to ISO 16844-3. Four pins:
  - 1: Positive supply
  - 2: Battery minus
  - 3: Speed signal, real-time (no integrity protection or authentication)
  - 4: Data signal, in/out

1.5.7 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 1.4.7.2.
    - 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 1.5.2. 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 (OE.Seal) 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 1.4.7.2. See also Figure 7.

1.5.8 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.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target is conformant to Common Criteria version 3.1, revision 4 [CC]

- Part 1: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-001
- Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
- Part 3: Security Assurance Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003

As follows, this ST is CC Part 2 conformant, and CC Part 3 conformant.

The guidance from ISO/IEC TR 15446 2nd edition *Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets* has been used when developing this Security Target [ISO-TR15446].

Also, the Common Methodology for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004, has been taken into account [CEM].

2.2 PP Conformance Claims

This Security Target does not claim conformance with any Protection Profile.

2.3 Package Conformance Claims

This Security Target claims conformance to assurance requirement package EAL4 augmented by ATE_DPT.2 and AVA_VAN.4.

Note: Although there is no PP to which the current ST is claimed to be conformant, this ST covers all requirements of the motion sensor generic ITSEC ST as contained in [Annex1B_App10].

Note: The European Regulation [Annex1B] requires for a motion sensor the assurance level ITSEC E3, high as specified in [Annex1B_App10], chap. 6 and 7. [JIL] defines an assurance package called E3hAP declaring assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. 2.1) certification (in conjunction with the Digital Tachograph System). The current official CCMB version of Common Criteria is Version 3.1, Revision 4. This version defines in its part 3 assurance requirements components partially differing from the respective requirements of CC v2.x. The assurance package requirements of this ST (EAL4+ ATE_DPT.2 and AVA_VAN.4) are chosen to relate to the latest interpretation of the [Annex1B] and [JIL] requirements from the BSI VU PP (E3hCC31_AP) [VU-PP]. The AVA_VAN.4 component is chosen, in front of AVA_VAN.5 stated in [VU-PP], to reflect the differences in attack potential resistance required, comparing the motion sensor with the vehicle unit, VU.

The [VU-PP] is certified by BSI (Germany), which is a member of SOG-IS and also participated in the [JIL] interpretation. Hence, this interpretation should also be recognised by SOG-IS.

3 Security Problem Definition

3.1 Introduction

The security problem definition described below includes threats, organisational security policies and security usage assumptions.

3.2 Threats

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

3.2.1 Assets

The user data assets and TSF data assets are part of the TOE Software (i.e. firmware). The terminology used are specified in [Regulation_2013] (Annex 1B, II, requirements 077-079, 099, 214; Appendix 1, sections 2.92-2.100 (ASN.1)) and [ISO16844-3] (sections 7.2, 7.6.9, 7.6.10). The “operating system identifier” is in the Toe implemented as the TOE firmware version.

User data:

- **Sensor data, D_S** (to be exported on pin 4 – sent when requested, see Figure 6)
- **Motion sensor identification data – stored in MS during manufacturing:**
  - the extended serial-number of the motion sensor in plain text, N_S (not a secret value), including:
    - serial number
    - motion sensor type in plain text
    - date of production of the motion sensor in plain text
    - name of the motion sensor manufacturer in plain text
  - operating system identifier of the motion sensor in plain text (i.e the TOE firmware version)
  - security identifier of the motion sensor (type of processor used) in plain text
  - type approval number of the motion sensor in plain text

TSF data:

- **Motion sensor initial security data – stored in MS during manufacturing:**
  - 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 master key, $^{e}Km(K_P)$

- **Motion sensor pairing security data – stored in MS during pairing:**
  - Session key, K_S
  - Pairing data, P_D (motion sensor installation data, pairing information):
    - first pairing with a VU (date, time, VU approval number, VU serial number)
    - last pairing with a VU (date, time, VU approval number, VU serial number)

Note:

As described in section 1.4.7.2; N_S and K_P are generated by Lesikar, $^eK_{ID}(N_S)$ and $^eKm(K_P)$ are received from Transportstyrelsen. All motion sensor identification data and all motion sensor initial security data are stored in the motion sensor during production (personalisation) and are always present in the TOE.

"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, see also section 6.1. No MS data can be accessed directly by external entities, e.g. the authenticated VU. External entities can only access the data through the available functions, see [ISO16844-3] (called instructions). Therefore, access control is only considered for the functions, not the data. The flow of data is controlled by information flow control policies.

"Sensor data", D_S, is the digital sensor data exported on pin 4 to provide data integrity for the real-time speed signal (enabling the VU to compare trusted pin 4 data with real-time pin 3 data).

3.2.2 Threat Agents

The threat agents that are identified for the TOE are described below.

The threat agent "Malicious user" is any user aiming for compromising the security of the tachograph system. The attack potential of the malicious users may vary from basic attack potential to high attack potential.

The threat agent "Malfunction" is the cause of any fault in hardware or software. Since it is not a conscious threat agent, the attack potential would be related to the consequences of the adverse action.

3.2.3 Threats

The threats against the TOE according to Table 1 are identified. All the threats in the ST are taken unmodified from the ITSEC ST of the regulation [Annex1B_App10]. The design related threats “T.Tests” and “T.Design” are not included in this ST since they do not describe threats against the operational TOE, but threats related to security measures that should be taken during the TOE development. These measures are handled by the security assurance requirements of EAL4. The Threat “T.Magnetic_Fields” is added because of an updated regulation, [Regulation_2013], requirement 161a, amendment M15. The terminology comes from the [Regulation_2013] and the [ISO16844-3] interface specification, e.g. “functions” equals the functions specified in [ISO16844-3], called “instructions”.

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

Table 1, Threats against the TOE

3.3 Organisational Security Policies

Organisational security policies, OSPs, for the TOE are stated according to Table 2. All IT Security Objectives from the ITSEC ST of the regulation [Annex1B_App10] are present as Security Objectives in this Security Target, section 4. These two objectives that could not fully trace back to threats are present also here for clarity, as OSPs.

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

Table 2, Organisational Security Policies for the TOE

3.4 Assumptions

Assumptions on the operational environment of the TOE are made according to Table 3. A.Approved_Workshops is identical with OE.Approved_Workshops (but rephrased as an assumption), which is identical with M.Approved_Workshops in [Annex1B_App10]. A.Controls is identical with OE.Controls (but rephrased as an assumption), which is identical with M.Controls. A.Regular_Inspection is identical with OE.Regular_Inspection (but rephrased as an assumption), which is identical with M.Regular_Inspection. A.Seal is identical with OE.Seal (but rephrased as an assumption), which is a clarification of M.Mechanical_Interface, that the seal is part of the operational environment of the TOE. See section 4.3. 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].

Name	Assumptions on the operational environment of the TOE
A.Approved_Workshops	The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections and repairs.
A.Controls	Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated.

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

Table 3, Assumptions on the operational environment of the TOE

4 Security Objectives

4.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its operational environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.

- The security objectives for the operational environment of the TOE shall be clearly stated and traced back to aspects of identified threats countered by the operational environment of the TOE, organisational security policies or assumptions.

4.2 Security Objectives for the TOE

The following security objectives for the TOE are defined. All IT Security Objectives from the ITSEC ST of the regulation [Annex1B_App10] are present here, as security objectives. The security objective “O.Magnetic_Fields” is added because of an updated regulation [Regulation_2013], requirement 161a, amendment M15. The terminology comes from the [Regulation_2013] and the [ISO16844-3] interface specification, e.g. “functions” equals the functions specified in [ISO16844-3], called “instructions”. The security objective “O.Phys_Protection” is added to clarify the requirement of a TOE casing capable of being sealed in [Regulation_2013], Annex I, Chapter III (a) 7.2 and Annex I B, RLB_106. 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].

Security Objective	Description
O.Access	The motion sensor must control connected entities’ access to functions and data.
O.Audit	The motion sensor must audit attempts to undermine its security and should trace them to associated entities.
O.Authentication	The motion sensor must authenticate connected entities.
O.Processing	The motion sensor must ensure that processing of input to derive motion data is accurate.

Security Objective	Description
O.Reliability	The motion sensor must provide a reliable service.
O.Secured_Data_Exchange	The motion sensor must secure data exchanges with the VU.
O.Phys_Protection	The TOE shall have a casing capable of being sealed and thereby make physical tampering attempts detectable by visual inspection.
O.Magnetic_Fields	The TOE must have a sensing element that is protected from, or immune to, magnetic fields.
O.Software	The TOE must prevent all users from modifying the TOE software (no software debug or software update functionality allowed).

Table 4, Security objectives for the TOE

4.3 Security Objectives for the Operational Environment of the TOE

The following security objectives for the operational environment of the TOE are defined. In the ITSEC ST of the regulation [Annex1B_App10], section 3.6 "Physical, personnel or procedural means", different categories of security means are described: *Equipment design* – M.Development, M.Manufacturing (ADV, ALC); *Equipment delivery* – M.Delivery (ALC); *Security data generation and delivery* – M.Sec_Data_Generation, M.Sec_Data_Transport (out-of-scope for this ST. The TOE is the MS ready for pairing. Personalisation is done prior to that in accordance with the regulation); *Recording equipment installation, calibration, and inspection* – M.Approved_Workshops, M.Mechanical_Interface, M.Regular_Inpections; *Law enforcement control* – M.Controls; *Software upgrades* – M.Software_Upgrade (O.Software prevents software upgrades or manipulation).

OE.Approved_Workshops is identical with M.Approved_Workshops. OE.Controls is identical with M.Controls. OE.Regular_Inspection is identical with M.Regular_Inspection. OE.Seal is a clarification of M.Mechanical_Interface, that the seal is part of the operational environment of the TOE. 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].

Security Objective	Description
OE.Approved_Workshops	Installation, calibration and repair of recording equipment shall be carried by trusted and approved fitters or workshops.
OE.Controls	Law enforcement controls shall be performed regularly and randomly, and must include security audits.

Security Objective	Description
OE.Regular_Inspection	Recording equipment shall be periodically inspected and calibrated.
OE.Seal	A security seal shall be used to seal the TOE and thereby its mechanical interface, to the gearbox. The security seal is applied during installation of the motion sensor in the vehicle. The security seal used to seal the TOE cannot be broken or removed and re-attached without the user or the inspector being able to detect the manipulation; and thereby provides the means of detecting physical tampering with the mechanical interface.

Table 5, Security objectives for the operational environment of the TOE

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

	T.Access	T.Faults	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	T.Magnetic_Fields	OSP.Audit	OSP.Processing	A.Approved_Workshops	A.Controls	A.Regular_Inspections	A.Seal
O.Access	x							x		x							
O.Audit	x									x		x					
O.Authentication	x							x		x							
O.Processing										x			x				
O.Reliability		x	x				x			x	x						
O.Secured_Data_Exchange						x		x									
O.Phys_Protection			x	x	x			x	x	x	x						
O.Magnetic_Fields			x		x						x						
O.Software		x							x								
OE.Approved_Workshops			x		x						x			x			
OE.Controls			x	x	x		x				x				x		
OE.Regular_Inspection			x	x	x		x				x					x	
OE.Seal			x	x	x			x	x	x	x						x

Table 6, Security objectives coverage

4.4.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives for the TOE are suitable to cover each individual threat to the TOE or organisational security policy; and that each security objective for the TOE traces back to a threat or an organisational security policy. The rationale also provides justification that the security objectives for the operational environment of the TOE are suitable to cover each individual threat to the TOE, organisational security policy or assumption about the operational environment of the TOE; and that each security objective for the operational environment of the TOE traces back to a threat, an organisational security policy or an assumption about the operational environment of the TOE.

Threat/OSP/Assumption	Objective	Rationale
T.Access	**O.Access** **O.Audit** **O.Authentication**	T.Access is addressed by the O.Authentication objective to ensure the identification of the user, the O.Access objective to control access of the user to functions and the O.Audit objective to trace attempts of unauthorised accesses.
T.Faults	**O.Reliability** **O.Software**	T.Faults is addressed by the O.Reliability objective by providing a fault tolerant design. The O.Software objective contributes to address the threat by preventing software upgrades or manipulation.
T.Environment	**O.Phys_Protection** **OE.Seal** **O.Reliability** **O.Magnetic_Fields** **OE.Approved_Workshops** **OE.Controls** **OE.Regular_Inspection**	T.Environment is addressed by the O.Phys_Protection and the OE.Seal objectives to ensure that direct attacks cannot be made inside the equipment. The O.Magnetic_Fields objective handles tampering by the use of magnetic fields. The O.Reliability objective contributes to address the threat by providing a failure tolerant design. The objectives for the operational environment of the TOE OE.Approved_Workshops, OE.Controls and OE.Regular_Inspection also contributes by trusted calibration, control and inspections.

Threat/OSP/Assumption	Objective	Rationale
T.Hardware	**O.Phys_Protection** **OE.Seal** **OE.Controls** **OE.Regular_Inspection**	T.Hardware is addressed by the O.Phys_Protection and the OE.Seal objectives. The OE.Controls and OE.Regular_Inspection help addressing the threat through visual inspection of the installation.
T.Mechanical_Origin	**O.Phys_Protection** **OE.Seal** **O.Magnetic_Fields** **OE.Controls** **OE.Regular_Inspection** **OE.Approved_Workshops**	T.Mechanical_Origin is addressed by the O.Phys_Protection and the OE.Seal objectives. The OE.Seal objective contributes by ensuring that a security seal seals the mechanical interface of the TOE to the gearbox. The security seal is applied during installation of the motion sensor in the vehicle. And the OE.Seal objective also contributes by ensuring that the seal 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. The O.Magnetic_Fields objective handles tampering by the use of magnetic fields. The OE.Controls and OE.Regular_Inspection objectives contribute to addressing the threat by revealing attempts to manipulate the MS input; the OE.Approved_Workshops objective contributes also by ensuring the TOE will be and remain properly sealed during installation and normal use.
T.Motion_Data	**O.Secured_Data_Exchange**	T.Motion_Data is addressed by the O.Secured_Data_Exchange objective by securing data exchanges.

Threat/OSP/Assumption	Objective	Rationale
T.Power_Supply	**O.Reliability** **OE.Controls** **OE.Regular_Inspection**	T.Power_Supply is addressed by the O.Reliability objective by ensuring a reliabile service regardless of power deviations. Also OE.Controls and OE.Regular_Inspection supports by allowing checking of the TOE power supply.
T.Security_Data	**O.Access** **O.Phys_Protection** **OE.Seal** **O.Authentication** **O.Secured_Data_Exchange**	The O.Access, O.Phys_Protection an OE.Seal objectives ensures appropriate protection of security data while stored in the TOE. Most security data generation and transport are performed before the operational state of the TOE and therefore out of scope (handled by assurance requirements, e.g. ALC, ADV). The confidentiality and integrity of the security data exchanged between the MS and the VU during pairing (pairing key, session key and pairing information) is addressed by O.Authentication and O.Secured_Data_Exchange.
T.Software	**O.Phys_Protection** **OE.Seal** **O.Software**	T.Software is addressed by the O.Phys_Protection and OE.Seal objectives to prevent physical tampering with the code. And the O.Software objective to prevent software analysis, debugging or update in the field.
T.Stored_Data	**O.Access** **O.Audit** **O.Processing** **O.Reliability** **O.Phys_Protection** **OE.Seal** **O.Authentication**	T.Stored_Data is addressed by the objectives O.Access and O.Audit that ensures access control and security audit. The O.Processing and O.Reliability objectives contribute also to address the threat. The O.Phys_Protection and OE.Seal objectives provide means to prevent physical attacks, which protects stored data.

Threat/OSP/Assumption	Objective	Rationale
		O.Authentication handles the authentication of external entities so that no external users other than authenticated Vus can connect to the MS.
T.Magnetic_Fields	**O.Magnetic_Fields** **O.Phys_Protection** **OE.Seal** **O.Reliability** **OE.Approved_Workshops** **OE.Controls** **OE.Regular_Inspection**	T.Magnetic_Fields is addressed by the O.Magnetic_Fields objective that ensures that the TOE has a sensing element that is protected from, or immune to, magnetic fields. Also the O.Phys_Protection and the OE.Seal objectives contribute to protect the TOE from tampering by e.g. magnetic fields. And the O.Reliability objective contributes to address the threat by providing a failure tolerant design. The objectives for the operational environment of the TOE OE.Approved_Workshops, OE.Controls and OE.Regular_Inspection also contributes by trusted calibration, control and inspections.
OSP.Audit	**O.Audit**	OSP.Audit is addressed by the O.Audit objective that ensures that auditing is implemented.
OSP.Processing	**O.Processing**	OSP.Processing is addressed by the O.Processing objective that ensures that processing of input to derive motion data is accurate.
A.Approved_Workshops	**OE.Approved_Workshops**	A.Approved_Workshops is addressed by the objective OE.Approved_Workshops for the operational environment of the TOE that ensures that installation, calibration and repair of recording equipment are to be carried out by trusted and approved fitters or workshops.

Threat/OSP/Assumption	Objective	Rationale
A.Controls	**OE.Controls**	A.Controls is addressed by the objective OE.Controls for the operational environment of the TOE that ensures that law enforcement controls are to be performed regularly and randomly, and includes security audits.
A.Regular_Inspections	**OE.Regular_Inspections**	A.Regular_Inspections is addressed by the objective OE.Regular_Inspections for the operational environment of the TOE that ensures that recording equipment is to be periodically inspected and calibrated.
A.Seal	**OE.Seal**	A.Seal is addressed by the objective OE.Seal for the operational environment of the TOE ensuring that a security seal seals the mechanical interface of the TOE to the gearbox. The security seal is applied during installation of the motion sensor in the vehicle. And the OE.Seal objective also contributes by ensuring that the seal 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.

Table 7, Security objectives sufficiency

5 Extended Components Definition

No extended components are defined.

6 Security Requirements

6.1 Security Functional Policies and Terminology

Three Security Functional Policies are defined in this ST:

- Function access control SFP (FDP_ACC.2, FDP_ACF.1): To control access to the TOE functions available through the [ISO16844-3] interface, called instructions.
- MS data import information flow control SFP (FDP_ITC.1, FDP_IFC.1a, FDP_IFF.1a): To control the import of data to the TOE. The import of the session key is also expressed by FCS_CKM.2a.
- MS data export information flow control SFP (FDP_ETC.1, FDP_IFC.1b, FDP_IFF.1b): To control the export of data from the TOE. The export of the pairing key is also expressed by FCS_CKM.2b.

"function number" is a security attribute for the object *"MS function"* referring to the [ISO16844-3] function, called instruction. Available values for function number: 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 (instruction 11 or 80).

"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 3.2.1.

"MS data type" is a security attribute used in the SFRs to differentiate between data types – which kind of data that is referred to.

Available values for MS data type, see the asset list in section 3.2.1:

- MS sensor data
- MS identification data
- MS identification data::serial number (N_S)
- Motion sensor initial security data
- Session key
- Pairing data – first pairing
- Pairing data – last pairing

"user category" is a security attribute for the subject/external entity *"user"* used in the SFRs to differentiate whether the user is an authenticated VU.

Available values for user category (both are external entities):

- Authenticated VU
- Unauthenticated VU

"Pairing mode" is a security attribute for the information MS data (the pairing data) used in the SFRs to differentiate whether pairing is occurring at the moment, and if so, if this is the first pairing or not.

Available values for Pairing mode:

- First pairing
- Last pairing
- No pairing

"First pairing" is only the first pairing. *"Last pairing"* is the current pairing if the current pairing is not the first pairing. *"during pairing"* refers to both "First pairing" and "Last pairing". *"No pairing"* means that the current instruction is not related to pairing (and therefore the TOE shall not allow the import of pairing data for this instruction).

"Sensor data", D_S, is the digital sensor data exported on pin 4 to provide data integrity for the real-time speed signal (enabling the VU to compare trusted pin 4 data with real-time pin 3 data).

"Motion data" is the raw data about the vehicle's motion that the sensor imports (processes and derives) to the TOE from the MS mechanical interface. This data is processed to become *"Sensor data"*, D_S, see above.

6.2 Security Functional Requirements

The following table presents the SFRs used.

Assignment and selection operations are marked with **bold**; refinements with **<u>bold underlined</u>**. If an assignment or selection operation uses several lines square brackets ("**[**" and "**]**") are used as well.

Class	Family	Component
FAU: Security audit	FAU_GEN: Security audit data generation	FAU_GEN.1: Audit data generation
FCS : Cryptographic support	FCS_CKM: Cryptographic key management	FCS_CKM.2b: Cryptographic key distribution FCS_CKM.2a: Cryptographic key import FCS_CKM.4: Cryptographic key destruction
	FCS_COP: Cryptographic operation	FCS_COP.1a: Cryptographic operation, encryption of data FCS_COP.1b: Cryptographic operation, decryption of data
FDP: User data protection	FDP_ACC: Access control policy	FDP_ACC.2: Complete access control
	FDP_ACF: Access control functions	FDP_ACF.1: Security attribute based access control

Class	Family	Component
	FDP_ETC: Export from the TOE	FDP_ETC.1: Export of user data without security attributes
	FDP_ITC: Import from outside of the TOE	FDP_ITC.1: Import of user data without security attributes
	FDP_IFC Information flow control policy	FDP_IFC.1a: Subset information flow control, MS data import FDP_IFC.1b: Subset information flow control, MS data export
	FDP_IFF: Information flow control functions	FDP_IFF.1a: Simple security attributes, , MS data import FDP_IFF.1b: Subset information flow control, MS data export
	FDP_SDI: Stored data integrity	FDP_SDI.1: Stored data integrity monitoring
	FDP_UIT: Inter-TSF user data integrity transfer protection	FDP_UIT.1a: Data exchange integrity, import FDP_UIT.1b: Data exchange integrity, export
FIA: Identification and authentication	FIA_AFL: Authentication failures	FIA_AFL.1: Authentication failure handling
	FIA_UAU: User authentication	FIA_UAU.2: User authentication before any action FIA_UAU.3: Unforgeable authentication
	FIA_UID: User identification	FIA_UID.2: User identification before any action
FPT: Protection of the TSF	FPT_FLS: Fail secure	FPT_FLS.1: Failure with preservation of secure state
	FPT_PHP: TSF physical protection	FPT_PHP.1 – Passive detection of physical attack FPT_PHP.3 – Resistance to physical attack
	FPT_TST: TSF self test	FPT_TST.1: TSF testing
FTP: Trusted path/channels	FTP_ITC: Inter-TSF trusted channel	FTP_ITC.1: Inter-TSF trusted channel

Table 8, Security Functional Requirements

6.2.1 Class FAU – Security audit

6.2.1.1 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 **not specified** level of audit; and

c)

Event type [1]	**Event**	**SFR**	**Class of error reported** [2]
Security breach attempts	Authentication failure	FIA_AFL.1 FIA_UAU.2 FIA_UAU.3 FIA_UID.2	24, Authentication
	Stored data integrity error	FDP_SDI.1	20, Non-volatile memory
Sensor faults	TSF self-test failure	FPT_TST.1	20, Non-volatile memory

1) – According to [Annex1B_App10], AUD_102
2) – According to [ISO16844-3], section 7.6.9.2 Structure of error messages

Figure 11, Audit events

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**~~ **connected external entity** 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 ST, **no other audit relevant information**

Application note: *In accordance with (AUD_103) and (AUD_104) [Annex1B_App10], the audit record is sent to the VU, which will time stamp the event. The Motion sensor itself will not provide a reliable time stamp, hence no FPT_STM.1. The only identifiable user of the TOE is the identity of the authenticated VU (external entity). Furthermore, the audit review functionality is also achieved by the VU.*

The VU handles the logging (e.g. auditing date and time and Start-up and shutdown of the audit functions). The motion sensor only generates the audit event, signals its presence with the NARA (New Audit Record Available) flag and waits for the VU to request the audit event.

The SFRs generating auditable events are: 6.2.3.9 FDP_SDI.1 – Stored data integrity monitoring; 6.2.4.1 FIA_AFL.1 – Authentication failure handling; 6.2.4.2 FIA_UAU.2 – User authentication before any action; 6.2.4.3 FIA_UAU.3 – Unforgeable authentication; 6.2.4.4 FIA_UID.2 – User identification before any action; and 6.2.5.4 FPT_TST.1 – TSF testing.

6.2.2 Class FCS – Cryptographic support

6.2.2.1 FCS_CKM.2 – Cryptographic key distribution

FCS_CKM.2a – import of session key

FCS_CKM.2a.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **import of session key K_S during instruction 42 of the pairing** that meets the following: **ISO 16844-3:2004, Cor 1:2006, 7.4.5.2 and Table 6.**

Application note: See also FDP_ITC.1, section 6.2.3.3.

FCS_CKM.2b – export of pairing key

FCS_CKM.2b.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **export of pairing key K_P during instruction 41 of the pairing** that meets the following: **ISO 16844-3:2004, Cor 1:2006, 7.4.4.3 and Table 6**.

Application note: See also FDP_ETC.1, section 6.2.3.4.

6.2.2.2 FCS_CKM.4 – Cryptographic key destruction

FCS_CKM.4 – destruction of session key

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **replace the old session key with the new session key** that meets the following: **ISO 16844-3:2004, Cor 1:2006, 7.4.5.2 and Table 6.**

6.2.2.3 FCS_COP.1 – Cryptographic operation

FCS_COP.1a – encryption of data

FCS_COP.1a.1 The TSF shall perform **encryption of data** accordance with a specified cryptographic algorithm **two key triple DES** and cryptographic key sizes **112 bits** that meet the following: **Protocol: ISO 16844-3:2004, Cor 1:2006; Algorithm: TDEA in TCBC and TECB mode of operation in accordance with FIPS PUB 46-3 (TDES), ANSI X9.52 (TCBC, null vector as Initial Value block and TECB).**

FCS_COP.1b – decryption of data

FCS_COP.1b.1 The TSF shall perform **decryption of data** accordance with a specified cryptographic algorithm **two key triple DES** and cryptographic key sizes **112 bits** that meet the following: **Protocol: ISO 16844-3:2004, Cor 1:2006; Algorithm: TDEA in TCBC and TECB mode of operation in accordance with FIPS PUB 46-3 (TDES), ANSI X9.52 (TCBC, null vector as Initial Value block and TECB).**

Application note: *TCBC mode is used for encryption/decryption during pairing, TECB mode is used elsewhere.*

6.2.3 Class FDP – User data protection

6.2.3.1 FDP_ACC.2 – Function – Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Function access control SFP** on **[**

- **Subjects/external entities: user**
- **Objects: MS function]**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application note: *See section 6.1, Security Functional Policies and Terminology.*

6.2.3.2 FDP_ACF.1 – Function – Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Function access control SFP** to objects based on the following: **[**

- **user: user category**
- **MS function: function number].**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

- **Authorise access to MS Function only if**
  - **function number = 40 or if**
  - **user category = authenticated VU].**

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

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

Application Note: *Function number 40 is the instruction to initialise pairing between the MS and the unauthenticated VU. Authentication is performed during pairing. All other functions shall be restricted to authenticated VUs. See section 6.1, Security Functional Policies and Terminology.*

6.2.3.3 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **MS data import information flow 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: **none.**

6.2.3.4 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the **MS data export information flow 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

6.2.3.5 FDP_IFC.1a – MS data import – Subset information flow control

FDP_IFC.1a.1 The TSF shall enforce the **MS data import information flow control SFP** on **[**

- **Subjects/external entities: user**
- **Information: MS data**
- **Operation: MS data import].**

Application note: *See section 6.1, Security Functional Policies and Terminology.*

6.2.3.6 FDP_IFF.1a – MS data import – Simple security attributes

FDP_IFF.1a.1 The TSF shall enforce the **MS data import information flow control SFP** based on the following types of subject and information security attributes: **[**

- **user: user category**
- **MS data: MS data type, Pairing mode].**

FDP_IFF.1a.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

- **Motion data may only be imported (processed and derived) to the TOE from the MS mechanical interface**

- **Session key may only be imported**
  - **during pairing from**
    - **An authenticated VU**
- **Pairing data – first pairing may only be imported**
  - **during first pairing from**
    - **An authenticated VU**
- **Pairing data – last pairing may only be imported**
  - **during last pairing from**
    - **An authenticated VU].**

FDP_IFF.1a.3 The TSF shall enforce the **no additional rules.**

FDP_IFF.1a.4 The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1a.5 The TSF shall explicitly deny an information flow based on the following rules: **none.**

Application note: *See section 6.1, Security Functional Policies and Terminology.*

6.2.3.7 FDP_IFC.1b – MS data export – Subset information flow control

FDP_IFC.1b.1 The TSF shall enforce the **MS data export information flow control SFP** on **[**

- **Subjects/external entities: user**
- **Information: MS data**
- **Operation: MS data export].**

Application note: *See section 6.1, Security Functional Policies and Terminology.*

6.2.3.8 FDP_IFF.1b – MS data export – Simple security attributes

FDP_IFF.1b.1 The TSF shall enforce the **MS data export information flow control SFP** based on the following types of subject and information security attributes: **[**

- **User/external entity: user category**
- **MS data: MS data type, Pairing mode].**

FDP_IFF.1b.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

- **Sensor data may only be exported from the TOE through:**
  - **the data signal in/out (pin 4) interface to**

        - **an authenticated VU**
            - **in accordance with ISO 16844-3:2004, Cor 1:2006, providing integrity and authenticity.**
- **MS initial security data may only be exported:**
    - **during pairing to**
        - **an authenticated VU**
            - **in accordance with ISO 16844-3:2004, Cor 1:2006, providing authentication, confidentiality and integrity.**
- **MS identification data::serial number (N_S) may only be exported to:**
    - **An authenticated VU or**
    - **An unauthenticated VU**
- **MS identification data may only be exported to**
    - **An authenticated VU].**

FDP_IFF.1b.3 The TSF shall enforce the **no additional rules.**

FDP_IFF.1b.4 The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1b.5 The TSF shall explicitly deny an information flow based on the following rules: **none.**

Application note: *See section 6.1, Security Functional Policies and Terminology.*

6.2.3.9 FDP_SDI.1 – Stored data integrity monitoring

FDP_SDI.1 **Audit events:**

a) Minimal: **Stored data integrity error**

FDP_SDI.1.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **data checksum.**

Application note: *The following stored data assets have data integrity monitoring by checksum verification, see also 3.2.1 Assets:*

- ***Motion sensor identification data – stored in MS during manufacturing:***
    - *the extended serial-number of the motion sensor in plain text, N_S (not a secret value), including:*
        - *serial number*

        - *motion sensor type in plain text*
        - *date of production of the motion sensor in plain text*
        - *name of the motion sensor manufacturer in plain text*
    - *operating system identifier of the motion sensor in plain text*
    - *security identifier of the motion sensor (type of processor used) in plain text*
    - *type approval number of the motion sensor in plain text*
- ***Motion sensor initial security data – stored in MS during manufacturing:***
    - *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 master key, $^{e}Km(K_P)$*
- ***Motion sensor pairing security data – stored in MS during pairing:***
    - Session key, K_S
    - Pairing data, P_D (motion sensor installation data, pairing information):
        - first pairing with a VU (date, time, VU approval number, VU serial number)
        - last pairing with a VU (date, time, VU approval number, VU serial number)

6.2.3.10 FDP_UIT.1a – import – Data exchange integrity

FDP_UIT.1a.1 The TSF shall enforce the **MS data import information flow control SFP** to **receive** user data in a manner protected from **modification, deletion, insertion, replay** errors.

FDP_UIT.1a.2 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay** has occurred.

6.2.3.11 FDP_UIT.1b – export – Data exchange integrity

FDP_UIT.1b.1 The TSF shall enforce the **MS data export information flow control SFP** to **transmit** user data in a manner protected from **modification, deletion, insertion, replay** errors.

FDP_UIT.1b.2 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay** has occurred.

6.2.4 Class FIA – Identification and authentication

6.2.4.1 FIA_AFL.1 – Authentication failure handling

FIA_AFL.1 **Audit events:**

a) Minimal: **the reaching of the threshold for the unsuccessful authentication attempts.**

FIA_AFL.1.1 The TSF shall detect when **at most 20 consecutive** unsuccessful authentication attempts occur related to **VU authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall:

- **Generate an audit record of the event,**
- **Warn the entity,**
- **Continue to export motion data to the VU in a non-secured mode (real-time speed signal).**

6.2.4.2 FIA_UAU.2 – User authentication before any action

FIA_UAU.2 **Audit events:**

a) Minimal: **Unsuccessful use of the authentication mechanism.**

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

6.2.4.3 FIA_UAU.3 – Unforgeable authentication

FIA_UAU.3 **Audit events:**

a) Minimal: **Detection of fraudulent authentication data.**

FIA_UAU.3.1 The TSF shall **prevent** use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **prevent** use of authentication data that has been copied from any other user of the TSF.

6.2.4.4 FIA_UID.2 – User identification before any action

FIA_UID.2 **Audit events:**

a) Minimal: **Unsuccessful use of the user identification mechanism, including the user identity provided**

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.

6.2.5 Class FPT – Protection of the TSF

6.2.5.1 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:

- **TSF self-test failure at startup**
- **TSF self-test failure during operation**
- **Power supply deviation**

Application note: *Implementing RLB_109: The motion sensor shall preserve a secure state during power supply cut-off or variations. And RLB_110: In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the motion sensor shall be reset cleanly.*

6.2.5.2 FPT_PHP.1 – Passive detection of physical attack

FPT_PHP.1.1 The TSF shall **have a casing capable of being sealed that together with the security seal (OE.Seal)** provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall **have a casing capable of being sealed that together with the security seal (OE.Seal)** provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.5.3 FPT_PHP.3 – Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical tampering by the use of magnetic fields up to 400 mT** to the **MS mechanical interface** by responding automatically such that the SFRs are always enforced.

Application note: *The TOE uses a patent pending solution that has two sensors mounted in a way that makes the TOE resistant to physical tampering by the use of magnetic fields. This has been tested up to 400 mT since it is hard to get hold of stronger magnets; but it may work with even stronger magnets. If magnetic fields tampering attempts occur, the TOE is able to process this and provide the correct real-time speed signal and Sensor data, D_S, anyway.*

6.2.5.4 FPT_TST.1 – TSF testing

FPT_TST.1 **Audit events:**

a) Minimal: **Failure of the TSF self-tests (TOE internal fault).**

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

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **none**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **none**.

Application note: *Implementing RLB_102: The motion sensor shall run self-tests, during initial start-up, and during normal operation to verify its correct operation. The motion sensor self-tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).*

The self-test run is a checksum verification of the data integrity of the TSF (i.e. the firmware itself).

There are no users on the TOE; therefore there are no users with the capability to verify integrity of the TSF or the TSF data. The only user is the authenticated VU which is an external entity that only can access the TOE by the available functions, i.e. the [ISO16844-3] instructions. The authenticated VU will however be able to retrieve audit records in accordance with [ISO16844-3]. The TSF will use the self-tests to preserve a secure state, see FPT_FLS.1 in section 6.2.5.1.

6.2.6 Class FTP – Trusted path/channels

6.2.6.1 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 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 **the VU** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for: **none**.

Application note: *The cryptographic operations needed by the trusted channel are defined by FCS_CKM and FCS_COP.*

6.3 Security Assurance Requirements

The security assurance requirements according to Table 9 have been chosen. They comprise EAL4 augmented by ATE_DPT.2 and AVA_VAN.4.

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

Table 9, Security Assurance Requirements

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Dependencies

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FAU_GEN.1	FPT_STM.1 Reliable time stamps	No	In accordance with (AUD_103) and (AUD_104) [Annex1B_App10], the audit record is sent to the VU, which will time stamp the event. The Motion sensor itself will not provide a reliable time stamp, hence no FPT_STM.1.
FCS_CKM.2a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Yes, FDP_ITC.1 and FCS_CKM.4	
FCS_CKM.2b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	No	The pairing key that gets exported to the VU is not generated by the TOE or imported by the TOE. It is imported to the product during the manufacturing phase. The pairing key is never destructed.
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Yes, FDP_ITC.1	Session key import by FCS_CKM.2a

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Yes, FDP_ITC.1 and FCS_CKM.4	Session key import by FCS_CKM.2a
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Yes, FDP_ITC.1 and FCS_CKM.4	Session key import by FCS_CKM.2a
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	Yes, FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Yes, FDP_ACC.2. No, FMT_MSA.3.	There is no way to initialise or change the values of the security attributes. The security attribute “user category” can be “authenticated VU” or “Unauthenticated VU” the user will only be considered to belong to the category “authenticated VU” if authenticated as a VU. The “function number” for the different functions are hard-coded in the software, in the TSF.

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Yes, FDP_IFC.1a No, FMT_MSA.3.	There is no way to initialise or change the values of the security attributes. The security attribute “user category” can be “authenticated VU” or “Unauthenticated VU” the user will only be considered to belong to the category “authenticated VU” if authenticated as a VU. The “MS data type” for the MS data depends upon which data type the MS data belongs to. It is hard-coded in the software, in the TSF.
FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Yes, FDP_IFC.1b	The “MS data type” for the MS data depends upon which data type the MS data belongs to. It is hard-coded in the software, in the TSF. The “pairing mode” is determined by the software in the TSF (first pairing, last pairing or no pairing).
FDP_IFC.1a	FDP_IFF.1 Simple security attributes	Yes, FDP_IFF.1a	
FDP_IFC.1b	FDP_IFF.1 Simple security attributes	Yes, FDP_IFF.1b	
FDP_IFF.1a	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Yes, FDP_IFC.1a No, FMT_MSA.3.	There is no way to initialise or change the values of the security attributes. The security attribute “user category” can be “authenticated VU” or “Unauthenticated VU” the user will only be considered to belong to the category “authenticated VU” if authenticated as a VU. The “MS data type” for the MS data depends upon which data type the MS data belongs to. It is hard-coded in the software, in the TSF. The “pairing mode” is determined by the software in the TSF (first pairing, last pairing or no pairing).

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_IFF.1b	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Yes, FDP_IFC.1b No, FMT_MSA.3.	There is no way to initialise or change the values of the security attributes. The security attribute “user category” can be “authenticated VU” or “Unauthenticated VU” the user will only be considered to belong to the category “authenticated VU” if authenticated as a VU. The “MS data type” for the MS data depends upon which data type the MS data belongs to. It is hard-coded in the software, in the TSF. The “pairing mode” is determined by the software in the TSF (first pairing, last pairing or no pairing).
FDP_SDI.1	No dependencies.	Yes.	
FDP_UIT.1a	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Yes, FDP_IFC.1a and FTP_ITC.1	
FDP_UIT.1b	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Yes, FDP_IFC.1b and FTP_ITC.1	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Yes, FIA_UAU.2	
FIA_UAU.2	FIA_UID.1 Timing of identification	Yes, FIA_UID.2	
FIA_UAU.3	No dependencies.	Yes.	
FIA_UID.2	No dependencies.	Yes.	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FPT_FLS.1	No dependencies.	Yes.	
FPT_PHP.1	No dependencies.	Yes.	
FPT_PHP.3	No dependencies.	Yes.	
FPT_TST.1	No dependencies.	Yes.	
FTP_ITC.1	No dependencies.	Yes.	

Table 10, SFR dependencies

6.4.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level EAL4 augmented by ATE_DPT.2 and AVA_VAN.4. Since all dependencies are met internally by the EAL package only the augmented the assurance components dependencies are analysed.

Assurance Component	Dependencies	Met
ATE_DPT.2	ADV_ARC.1 Security architecture description ADV_TDS.3 Basic modular design ATE_FUN.1 Functional testing	Yes, the same dependencies as for EAL4.
AVA_VAN.4	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_TDS.3 Basic modular design ADV_IMP.1 Implementation representation of the TSF AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_DPT.1 Testing: basic design	Yes, the same dependencies as for EAL4.

Table 11, Security Assurance Dependencies Analysis

According to Table 11 all dependencies are met.

6.4.3 Security Functional Requirements Coverage

	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Phys_Protection	O.Magnetic_Fields	O.Software
FAU_GEN.1		x	x						
FCS_CKM.2b			x			x			
FCS_CKM.2a			x			x			
FCS_CKM.4			x			x			
FCS_COP.1a			x			x			
FCS_COP.1b			x			x			
FDP_ACC.2	x			x					x
FDP_ACF.1	x			x					x
FDP_ITC.1			x	x		x			x
FDP_ETC.1			x	x		x			
FDP_IFC.1a			x	x		x			x
FDP_IFC.1b			x	x		x			
FDP_IFF.1a			x	x		x			x
FDP_IFF.1b			x	x		x			
FDP_SDI.1		x							x
FDP_UIT.1a						x			
FDP_UIT.1b						x			
FIA_AFL.1		x	x						
FIA_UAU.2	x	x	x						
FIA_UAU.3	x	x	x						
FIA_UID.2	x	x	x						
FPT_FLS.1				x	x				x
FPT_PHP.1							x		x
FPT_PHP.3								x	
FPT_TST.1		x		x	x				x
FTP_ITC.1						x			

Table 12, Security Functional Requirements Coverage

6.4.4 Security Functional Requirements Sufficiency

Objective	SFR	Rationale
O.Access The motion sensor must control connected entities' access to functions and data.	**FDP_ACC.2** **FDP_ACF.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3**	Function access control is provided by FDP_ACC.2 and FDP_ACF.1. Identification and authentication are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3.
O.Audit The motion sensor must audit attempts to undermine its security and should trace them to associated entities.	**FAU_GEN.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3** **FDP_SDI.1** **FIA_AFL.1** **FPT_TST.1**	FAU_GEN.1 generates audit events. Identification and authentication, and related audit events, are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3. FDP_SDI.1 provides stored data integrity error events. FDP_AFL.1 provides authentication failure events. FPT_TST.1 provides TSF self-test failure events.
O.Authentication The motion sensor must authenticate connected entities.	**FAU_GEN.1** **FCS_CKM.2b** **FCS_CKM.2a** **FCS_CKM.4** **FCS_COP.1a** **FCS_COP.1b** **FDP_ITC.1** **FDP_ETC.1** **FDP_IFC.1a** **FDP_IFC.1b** **FDP_IFF.1a** **FDP_IFF.1b** **FIA_AFL.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3**	FAU_GEN.1 associates the audit events with the VU identity. FCS_CKM.2b exports the pairing key, which is part of the authentication during pairing. FCS_CKM.2a imports the session key, which is part of the authentication during pairing. FCS_CKM.4 replaces the old session key with the new session key, which is part of the authentication during pairing. FCS_COP.1a and FCS_COP.1b encrypts and decrypts data, which is part of the authentication during pairing. FDP_ITC.1, FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a and FDP_IFF.1b provides information flow control when importing and exporting data during the authentication and pairing. FIA_AFL.1 provides authentication failure handling. Identification and authentication are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3.
O.Processing The motion sensor must ensure that processing of input to derive motion data is accurate.	**FDP_ACC.2** **FDP_ACF.1** **FDP_ITC.1** **FDP_ETC.1** **FDP_IFC.1a** **FDP_IFC.1b**	Function access control is provided by FDP_ACC.2 and FDP_ACF.1. FDP_ITC.1, FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a, FDP_IFF.1b provides information flow control that ensures e.g. that motion sensor data must originate from the mechanical interface.

Objective	SFR	Rationale
	FDP_IFF.1a **FDP_IFF.1b** **FPT_FLS.1** **FPT_TST.1**	FPT_TST.1 and FPT_FLS.1 provides TSF self-test and preservation of a secure state.
O.Reliability The motion sensor must provide a reliable service.	**FPT_FLS.1** **FPT_TST.1**	FPT_TST.1 and FPT_FLS.1 provides TSF self-test and preservation of a secure state (providing a fault tolerant design).
O.Secured_Data_Exchange The motion sensor must secure data exchanges with the VU.	**FCS_CKM.2b** **FCS_CKM.2a** **FCS_CKM.4** **FCS_COP.1a** **FCS_COP.1b** **FDP_UIT.1a** **FDP_UIT.1b** **FDP_ITC.1** **FDP_ETC.1** **FDP_IFC.1a** **FDP_IFC.1b** **FDP_IFF.1a** **FDP_IFF.1b** **FTP_ITC.1**	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 O.Authentication (see also section 1.5.2). Second they need to establish a common secret, a session key. Now secure data exchange in accordance with ISO 16844-3 can begin. FCS_CKM.2b exports the pairing key, which is part of the authentication during pairing. FCS_CKM.2a imports the session key, which is part of the authentication during pairing. FCS_CKM.4 replaces the old session key with the new session key, which is part of the authentication during pairing. FCS_COP.1a and FCS_COP.1b encrypts and decrypts data, which is part of the authentication during pairing and it is also how the data exchange is secured after pairing. FDP_UIT.1a and FDP_UIT.1b provides data exchange integrity for MS data import and export – enforces integrity protection for data using MS data import information flow control SFP and MS data export information flow control SFP. FDP_ITC.1, FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a and FDP_IFF.1b provides information flow control when importing and exporting data during the authentication and pairing. FTP_ITC.1 ensures the trusted channel between the MS and the VU which is provided by the security mechanism above.

Objective	SFR	Rationale
O.Phys_Protection The TOE shall have a casing capable of being sealed and thereby make physical tampering attempts detectable by visual inspection.	**FPT_PHP.1**	FPT_PHP.1 provides physical tampering detection by the use of a protective casing capable of being sealed.
O.Magnetic_Fields The TOE must have a sensing element that is protected from, or immune to, magnetic fields.	**FPT_PHP.3**	FPT_PHP.3 provides a sensing element that is protected from, or immune to, magnetic fields.
O.Software The TOE must prevent all users from modifying the TOE software (no software debug or software update functionality allowed).	**FDP_ACC.2** **FDP_ACF.1** **FDP_ITC.1,** **FDP_IFC.1a** **FDP_IFF.1a** **FDP_SDI.1** **FPT_TST.1** **FPT_FLS.1** **FPT_PHP.1**	No software update functionality is implemented. Function access control is provided by FDP_ACC.2 and FDP_ACF.1. FDP_ITC.1, FDP_IFC.1a and FDP_IFF.1a provides information flow control when importing data to the TOE. FDP_SDI.1 provides stored data integrity. FPT_TST.1 and FPT_FLS.1 provides TSF self-test and preservation of a secure state, providing a fault tolerant design against software attacks. FPT_PHP.1 provides physical tampering detection to protect against software attacks enabled by hardware attacks.

Table 13, Security Functional Requirements Sufficiency

7 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

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 rationalise that the security functions satisfy the necessary requirements. Table 14 lists the security functions and their associated SFRs.

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.1 and FPT_PHP.3).

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.

TOE Security Function	SFR	Description
SF.Audit	**FAU_GEN.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3** **FDP_SDI.1** **FIA_AFL.1** **FPT_TST.1**	Security audit data generation. SF.Audit helps achieving the security objective O.Audit. FAU_GEN.1 generates audit events. Identification and authentication, and related audit events, are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3. FDP_SDI.1 provides stored data integrity error events. FDP_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, authorisation error, or communication error. The data of the audit record is written to the MS NVRAM and the flag NARA (New Audit Record Available) is set in the next communication frame. When the VU detects that the NARA flag is set, it requests the new audit record.

TOE Security Function	SFR	Description
SF.Authentication	**FAU_GEN.1** **FCS_CKM.2b** **FCS_CKM.2a** **FCS_CKM.4** **FCS_COP.1a** **FCS_COP.1b** **FDP_ITC.1** **FDP_ETC.1** **FDP_IFC.1a** **FDP_IFC.1b** **FDP_IFF.1a** **FDP_IFF.1b** **FIA_AFL.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3**	SF.Authentication helps achieving the security objective O.Authentication. • Mutual authentication between the MS and the VU during pairing. o Processed according to the ISO 16844-3, section 7.4.2. • Authentication failure handling. o After 20 unsuccessful authorisation attempts the TOE generates an audit record (error message). It is stored in the sensor memory (NVRAM) until the MS is properly connected to the authorised VU and then the MS sends its error file to the VU. o After 20 unsuccessful authorisation attempts the MS also stops responding, until the authorised VU is connected (blocks unauthorised key testing / hacking). • Unforgeable user identification and authentication before any action. FAU_GEN.1 associates the audit events with the VU identity. FCS_CKM.2b exports the pairing key, which is part of the authentication during pairing. FCS_CKM.2a imports the session key, which is part of the authentication during pairing. FCS_CKM.4 replaces the old session key with the new session key, which is part of the authentication during pairing. FCS_COP.1a and FCS_COP.1b encrypts and decrypts data, which is part of the authentication during pairing. FDP_ITC.1, FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a and FDP_IFF.1b provides information flow control when importing and exporting data during the authentication and pairing. FIA_AFL.1 provides authentication failure handling. Identification and authentication are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3.
SF.Crypto	**FCS_CKM.2b** **FCS_CKM.2a** **FCS_CKM.4** **FCS_COP.1a** **FCS_COP.1b** **FDP_UIT.1a** **FDP_UIT.1b** **FTP_ITC.1**	Cryptographic key distribution, import and destruction; encryption and decryption; data exchange integrity. SF.Crypto helps achieving the security objectives O.Secured_Data_Exchange and O.Authentication. • The import of a session key, K_S, from the VU during pairing. o Processed according to the ISO 16844-3, section 7.4.6.

TOE Security Function	SFR	Description
		• The export of a pairing key, K_P, to the VU during pairing. o Processed according to the ISO 16844-3, section 7.4.4.3. • Destruction of old session key by replacement with new session key. o 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. o MS data that is exported is first checked for integrity of all the data, and then every frame sent has a checksum in accordance with the ISO 16844-3. • Encryption and decryption of data, with the session key, for the transmission of data between the MS and the VU. 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 (see also section 1.5.2). Second they need to establish a common secret, a session key. Now secure data exchange in accordance with ISO 16844-3 can begin. FCS_CKM.2b exports the pairing key, which is part of the authentication during pairing. FCS_CKM.2a imports the session key, which is part of the authentication during pairing. FCS_CKM.4 replaces the old session key with the new session key, which is part of the authentication during pairing. FCS_COP.1a and FCS_COP.1b encrypts and decrypts data, which is part of the authentication during pairing and it is also how the data exchange is secured after pairing. FDP_UIT.1a and FDP_UIT.1b provides data exchange integrity for MS data import and export – enforces integrity protection for data using MS data import information flow control SFP and MS data export information flow control SFP. FTP_ITC.1 ensures the trusted channel between the MS and the VU which is provided by the security mechanism above.
SF.Flow	**FDP_ITC.1** **FDP_ETC.1** **FDP_IFC.1a** **FDP_IFC.1b**	Information flow control for MS data import and export. SF.Flow helps achieving the security objectives O.Secured_Data_Exchange, O.Authentication, O.Processing and O.Software.

TOE Security Function	SFR	Description
	FDP_IFF.1a **FDP_IFF.1b**	FDP_ITC.1, FDP_ETC.1, FDP_IFC.1a, FDP_IFC.1b, FDP_IFF.1a and FDP_IFF.1b 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.
SF.Access	**FDP_ACC.2** **FDP_ACF.1** **FIA_UID.2** **FIA_UAU.2** **FIA_UAU.3**	Access control to TOE functions. SF.Access helps achieving the security objectives O.Access, O.Processing and O.Software. Function access control is provided by FDP_ACC.2 and FDP_ACF.1. Identification and authentication are provided by FIA_UID.2, FIA_UAU.2 and FIA_UAU.3.
SF.Integrity	**FPT_TST.1** **FPT_FLS.1** **FDP_SDI.1**	Integrity protection, checksums. SF.Integrity helps achieving the security objectives O.Processing, O.Reliability and O.Software. • Stored data integrity monitoring. o Stored data are checked for integrity during start-up and periodically during operation by the use of checksums. • TSF self-testing. o Stored data and software code are checked for integrity during start-up and periodically during operation by the use of checksums. • Failure with preservation of secure state. o 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.
SF.Magnetic_Fields	**FPT_PHP.3**	FPT_PHP.3 provides resistance to magnetic fields tampering using two sensor elements. SF.Magnetic_Fields helps achieving the security objective O.Magnetic_Fields
SF.Casing	**FPT_PHP.1**	The TSF provides physical tampering detection by the use of a protective casing capable of being sealed. SF.Casing helps achieving the security objectives O.Phys_Protection and O.Software. FPT_PHP.1 provides physical tampering detection by the use of a protective casing capable of being sealed.

Table 14, TOE Security Functions

A Appendix – Abbreviations and Acronyms

Acronym or Abbreviation	Explanation
TOE	Target of Evaluation
MS	Motion Sensor
VU	Vehicle Unit
SOG-IS	Senior Officials Group – Information Systems Security
MSCA	Member State Certification Authority (member of the European Union)
CA	Certification Authority

Table 15, Abbreviations and acronyms

B Appendix – Referenced Documents

[CC] Common Criteria:

- Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, Version 3.1, Revision 4, CCMB-2012-09-001, September 2012
- Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements, Version 3.1, Revision 4, CCMB-2012-09-002, September 2012
- Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements, Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

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

[ISO-TR15446] ISO/IEC TR 15446 2nd edition Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets

[Regulation_2013] Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (OJ L 370, 31.12.1985, p. 8), updated up until 2013 with these two latest updates “M15 Commission Regulation (EU) No 1266/2009 of 16 December 2009 in Official Journal L 339, page 3, 22.12.2009” and “M16 Council Regulation (EU) No 517/2013 of 13 May 2013 in Official Journal L 158, page 1, 10.6.2013”.

[Annex1B] Annex 1B of [Regulation_2013].

[Annex1B_App10] Appendix 10 of [Annex1B]

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

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

[JIL] Joint Interpretation Library – Security Evaluation and Certification of Digital Tachographs – JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1B.

[VU-PP] Digital Tachograph – Vehicle Unit (VU PP) - Compliant to EU Commission Regulation 1360/2002, Annex I(B), App. 10, Version 1.0, 13 July 2010, BSI-CC-PP-0057.

[DT-site] European Commission – Joint Research Center – Digital Tachograph http://dtc.jrc.ec.europa.eu/

[ERCA-Policy] European Commission, Joint Research Center – Digital Tachograph System, European Root Policy, Version 2.1, JRC 53429

[TFSF2013:1] TSFS 2013:1 – Transportstyrelsens föreskrifter om hantering av krypteringsnycklar och certifikat för tillverkning av digitala färdskrivare, 2012-12-13.