DTMS-2 SECURITY TARGET LITE

Common Criteria version 3.1 revision 5 Assurance Level EAL 4+ ATE_DPT.2 and AVA_VAN.5

Version 1.0

Edition date 10.09.2025

This page intentionally left blank.

CONTENTS

Terms

AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
CC	Common Criteria
DES	Data Encryption Standard (see FIPS PUB 46-3)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EGF	External GNSS Facility
GNSS	Global Navigation Satellite System
HMS	Hall Motion Sensor
MAC	Message Authentication Code
MS	Motion Sensor
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VU	Vehicle Unit

1. Introduction

1.1. ST Reference

This ST is identified by the following unique reference:

ST Title	DTMS-2 Security Target
ST Version	v.1.7
ST Date	2025-09-10
ST Author	CB Electronics

1.2. TOE Reference

This TOE is identified by the following unique reference:

TOE Name	DTMS-2
TOE Version	v.2.0
Evaluation Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, version 3.1, revision 5, April 2017.
Evaluation Assurance Level	EAL 4+
TOE Developer	CB Electronics
TOE Sponsor	CB Electronics
Evaluation Facility	ITSEF NIT, Poland
Certification Authority	NASK – National Research Institute, Standardisation and Certification Centre, Poland
Certification ID	[2022-1]

1.3. TOE Overview

The TOE is a second generation tachograph motion sensor compliant with Protection Profile [BSI-CC-PP-0093[5]] in the sense of [6] Annex 1C, intended to be used in the digital tachograph system. The Digital Tachograph system additionally contains a VU, tachograph cards, an external GNSS module (if applicable) and remote early detection communication readers.

The motion sensor is mounted directly into the gearbox and collects the motion data that accurately reflects the vehicle's speed and distance travelled.

In the operational phase the motion sensor is connected to a VU and this data is captured from the rotating wheels inside the gearbox via a sensor and transmitted in an encrypted form and plain analog form to the authenticated VU of the Digital Tachograph system.

A motion sensor can be paired and used with second generation VU's and with first generation VU's as well [BSI-CC-PP-0093[5]]. The functional requirements for a Motion Sensor are specified in [6] Annex 1C, Chapter 3.2, and the common security mechanisms are specified in Appendix 11. Aspects of the electrical interface between the motion sensor and VU are described in ISO 16844-3 [7].

In case of failure in self-tests or during pairing and normal operation, the TOE generates and stores the audit record, to be read by the VU o its request.
The accuracy of motion data is checked by functional tests during the development and after its production.
The reliability of the TOE service is provided by sending motion data to the VU via 2 independent channels –analogue line (the electric pulses) and data line (number of pulses sent on analogue line-encrypted), which are compared by the VU. In case of difference the audit record is generated by VU, hence the motion data manipulation is detected.
The simplified block scheme of typical motion sensor is described in the Figure 1.

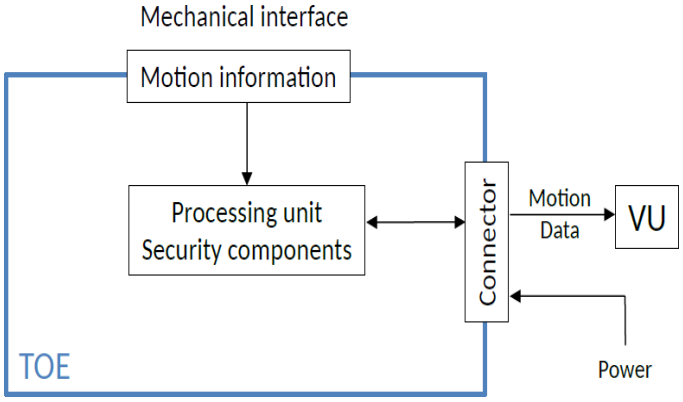

Figure 1. Motion sensor

The TOE physically consists of the following elements (see figure 2):

- A Hall Motion Sensor (HMS) that converts magnetic field changes of the rotating element of the gear into electrical pulses that allow the VU to derive speed and distance.
- A microcontroller processes the electrical pulses from the sensor in real-time and transmits the real time speed analog pulses to the VU and encrypted and authenticated motion data only to the authenticated VU.
- A Security Module (EAL 6+ certified [8]) stores key material and encrypts/decrypts data transmitted to and from the VU.
- Elements such as voltage regulator and buffers are required such that the TOE can fulfill its function according to [7]).

A schematic overview of the TOE is shown in Figure 2. The connector (1) connects the motion sensor with the cable to the VU. It also contains the interface to the VU (data interface) and the power supply. The crimping (2) links the connector with the body (3). Inside the body the Printed Circuit Board PCB (4) performs the logical security functions of the TOE (described below). It is connected with the Hall Motion Sensor (HMS) for motion detection (speed signal interface, 5).

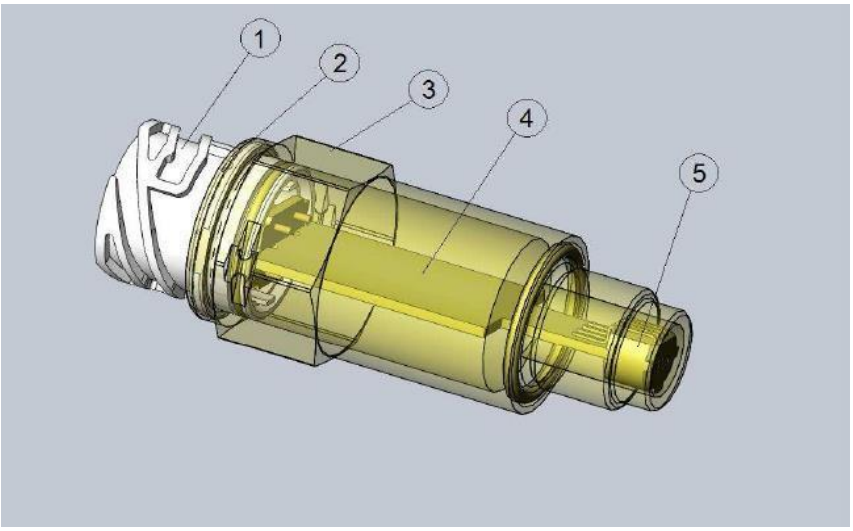

Figure 2. Schematic TOE overview (proximity type)

Figure 2 shows a motion sensor proximity type DTMS-2 distinguishes models with different lengths, see Table 1 for details of the identification system) which has an aluminum body and a socket (connector) for the cable (see Figure 3,right). The motion sensor rotary type DTMS-2 is equipped with a rotating element inside the body (see Figure 3, left).

Figure 3. From left to right: DTMS-2 – Rotary, DTMS-2 – Proximity

1.3.1. TOE Type

The TOE is a motion sensor in accordance with [6] Annex 1C, and Appendix 11 of that document.

The typical motion sensor product life-cycle is composed of 5 phases as follows:

a) Phase 1: Design
b) Phase 2: Manufacturing
c) Phase 3: Installation
d) Phase 4: Operational
e) Phase 5: End of life

Figure 4 shows the typical motion sensor life cycle as defined in [BSI-CC-PP-0093[5]].
In the case of this TOE is not designed to be repaired, therefore, if functioning problems are found during periodic inspections, installation or operation phases, the TOE will need to be replaced.

The CC does not prescribe any specific life-cycle model. However, in order to define the application of the assurance classes, the CC assumes the following implicit life-cycle model consisting of three phases:

a) TOE development
b) TOE delivery
c) TOE operational use

For the Sensor DTMS-2:

- "Design phase" and "Manufacturing phase" are part of the TOE development (ALC & ADV classes) in the sense of the CC.
- The "Design phase" covers all the activities related to the development of the TOE: design of software, hardware, mechanical parts, PCB, testing and implementation representation preparation.
- The "Manufacturing phase" contains the TOE manufacturing, its personalization and cryptographic keys injection and final testing. Independently all the components are mounted on PCB and software uploaded and on the other hand the case and mechanical parts are manufactured. Then final assembly and software upload take place.
    - The generation of personalization data unique to each MS (i.e. extended serial number N_s and pairing key K_P) is done in a secure environment approved during audits. The data is forwarded to the State Authority (SA).
    - SA performs encryption and returns data according to [EU-2016/799 [6]]. Data to/from SA is transferred according to SA procedures.
    - Data from SA is uploaded to MS personalization system in secure environment approved during audits.
    - Personalization data is transferred personalization system to MS in a secure environment approved during audits.
    - MS personalization is a unique and irreversible process. Once the process of uploading data to the MS is correctly completed, its unique data is deleted from the personalization system.
- The "Installation phase" belongs to the TOE delivery phase in the sense of the CC. During installation phase, the TOE is installed in the vehicle by an approved and trusted workshop. Once the TOE has been installed in the vehicle and the security seal has been attached, the TOE is paired with the VU. During pairing with a VU, mutual authentication occurs and the TOE also gets a session key from the VU that is used to encrypt the communication between the TOE and the VU.
    - The pairing process and the installation of a mechanical seal according to EN16882 [9] belong to the TOE operational use in the sense of the CC.
- The "End of life": If TOE is defected (i.e. functioning problems are found during periodic inspections, installation or operation phases) - it is disposed and replaced by new TOE.

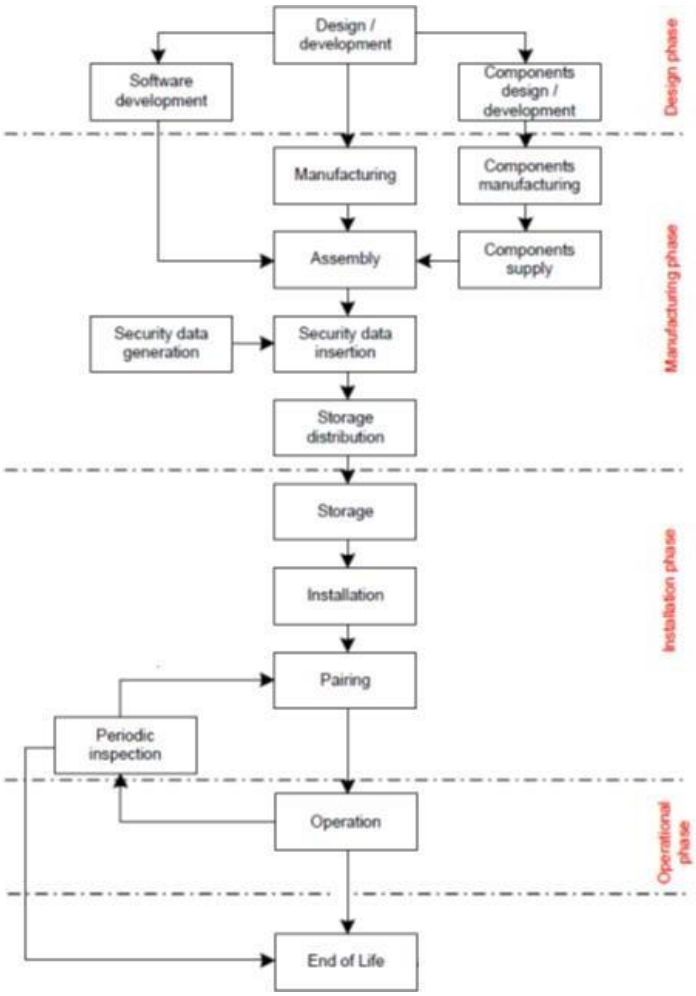

Figure 4. TOE life cycle

1.3.2. TOE Usage & Major Security Functions

The motion sensor aims to protect data that is stored and transferred in such a way as to prevent unauthorized access to and manipulation of the data, and to detect and report any such attempts.

The main security features of the TOE are as follows:

a) To maintain the integrity of motion data supplied to the VU;
b) To demonstrate its authenticity to the VU through an authenticated pairing process;
c) To detect physical tampering;
d) To audit security relevant events and send these to the VU;
e) To provide a secure communication channel between itself and the VU.

The main security features stated above are provided by the following major security services:

a) VU identification and authentication;
b) Access control to functions and stored data, according to [10];
c) Alerting of events and faults;
d) Integrity of stored data;
e) Reliability of services, including self-testing, physical protection, control of executable code, resource management, and secure handling of events;

f) Data exchange with a VU;
g) Cryptographic support for VU to motion sensor mutual authentication and secure messaging according to [6] Annex 1C, Appendix 11.

In this ST all cryptographic mechanisms for communications with first or second-generation VU's, including algorithms and the length of corresponding keys, are implemented exactly as required and defined in [6] Annex 1C, Appendix 11, Parts A and B, respectively.

1.3.3. Required non-TOE Hardware/Software/Firmware

The TOE is the Motion Sensor. It is an independent product, and does not need any additional hardware/software/firmware to ensure the security of the TOE.

In order to be able to supply motion data, the TOE must be paired with a VU, and must be installed in a motor vehicle.

1.4. TOE Description

The TOE is a second generation tachograph motion sensor compliant with Protection Profile [BSI-CC-PP-0093[5]] in the sense of [6] Annex 1C, intended to be used in the digital tachograph system.
The motion sensor (TOE) is mounted directly into the gearbox and collects the data that represents the vehicle speed and distance. In the operational phase the motion sensor is connected to a VU and this data is captured from the rotating wheels inside the gearbox via a sensor and transmitted in an encrypted form and plain analog form to the authenticated VU of the Digital Tachograph system.

[1]. The TOE 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 VU 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[11]].

To enable security (authentication and data integrity) a data channel is used in accordance with the interface specification [ISO 16844-3:2004[7]]. This channel is used to respond to VU requests.
The TOE supports communication with second generation and first-generation VU's. according to [BSI-CC-PP-0093[5]].
The TOE is supported by VU, tachograph cards, an external GNSS module (if applicable) and remote early detection communication readers, i.e. other parts of the Digital Tachograph system.
.

1.4.1. Physical Scope of the TOE

The physical scope of the TOE is presented on Figure 2. Physically TOE consists of:

- the connector (connecting the motion sensor with the cable to the VU and contains the data interface to the VU and the power supply);
- the crimping (linking the connector with the body);
- the body containing the Printed Circuit Board PCB with microcontroller;
- the Hall sensor (HMS) for motion detection (speed signal interface),

The physical boundary of the TOE is defined by the MS casing, the mechanical interface with the gearbox and the 4-pin connector [ISO15170-1[11]].

Only the data signal in/out (pin 4) has integrity authenticity and confidentiality protection by the use of cryptographic support. The real-time analogue signal (pin 3) has not.

The different models of the motion sensor only differ by their length (to be able to fit in different kinds of vehicles) and the nature of operation (see Table 1 below).

The identification system for appropriate variants of motion sensors is as follows:

1. First digit indicates the motion sensor type: (0-Rotary; 2 - Proximity; 3-Sprinter).

2. Depending on the type of motion sensor:
    a. Applicable for the Rotary or Proximity types of motion sensors:
        i. Second digit indicates the connector type,
        ii. Third digit indicates the thread type,
    b. Applicable for the Sprinter type of motion sensor:
        i. All consecutive digits express the cable length in millimetres,
    c. Applicable for the proximity type of motion sensors:
        i. Next digits represent the motion sensor length expressed in tenth of millimetres.

No.	*Description*	*Variant*	*Length*	*Images*
1.	Digital Motion Sensor MS TYPE Proximity Standard ISO 15170 connector M 18x1,5	DTMS-2 20018000	18,0 mm	
		DTMS-2 20018600	18,6 mm	
		DTMS-2 20019800	19,8 mm	
		DTMS-2 20023800	23,8 mm	
		DTMS-2 20025000	25,0 mm	
		DTMS-2 20033800	33,8 mm	
		DTMS-2 20035000	35,0 mm	
		DTMS-2 20062000	62,0 mm	
		DTMS-2 20063200	63,2 mm	
		DTMS-2 20088800	88,8 mm	
		DTMS-2 20090000	90,0 mm	
		DTMS-2 20011300	113,8 mm	
		DTMS-2 20011500	115,0 mm	
		DTMS-2 20013700	136,8 mm	

2.	Digital Motion Sensor MS TYPE Rotary Standard ISO 15170 connector Internal thread M22x1,5 Right	DTMS-2 001	Not applicable	
3.	Digital Motion Sensor MS TYPE Sprinter Sensor with proximity detector and armored cable	DTMS-2 3224	Cable length 224 mm	
		DTMS-2 3230	Cable length 230 mm	
		DTMS-2 3410	Cable length 410 mm	

Table 1. Different models of DTMS-2

The TOE guidance documentation is the following:

- AGD_PRE EAL4+ for Digital Motion Sensor (DTMS-2), version 1.6, 07.04.2025,

- AGD_OPE EAL4+ for DTMS-2, version 1.6, 07.04.2025.

1.4.1.1. Delivery of the TOE

The TOE ready for pairing (software embedded in the hardware with user data and security data) is delivered to the thrusted Workshop by courier delivery. The TOE documentation (Installation Manual and Operational Guidance) is delivered by signed pdf file by e-mail.

1.4.2. Logical Scope of the TOE

The TOE measures the motion data that accurately reflects the vehicle's speed and distance travelled and passes this information along to the VU. 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 [7]), and the digital motion data (pin 4 [7]). The following actions are performed. [6]

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

The TOE provides the security features described in 1.3.2. In the context of the TOE logical scope, these security features are as follows:

- Maintenance the integrity of motion data supplied to the VU;
- Demonstration of the TOE authenticity to the VU through an authenticated pairing process;
- Preserving audit data for security relevant events and send these to the VU;
- Detecting physical tampering;
- Providing the secure communication channel between itself and the VU.

1.4.2.1. Secure initialization

When the MS ready for pairing is installed and coupled with gearbox according to the Installation Manual and Operational Guidance, the process of pairing (including generation and storage of appropriate session key) is performed in an authorized trusted workshop. Before pairing appropriate protective seals are mounted according to regulation [EN 16882:2016[10]]. The pairing is performed according to [ISO 16844-3:2004[7]] and [EU-2016/799[6]], Annex 1C, Appendix 11. In that way, the integrity and authenticity of motion data when supplied to the authenticated (paired) VU is preserved.

1.4.2.2. Audit

The TOE records security events. This event includes:

- all errors i.e. non-volatile memory, communication and authentication, etc.
- communication interruption,
- breach of security measures (e.g. as a result of tampering detection),

Each audit entry is protected to prevent changes, entries are protected against deletion (their integrity is ensured). The TOE is able to store audit records in its own memory. The access to this data is to be controlled (access to this data is possible only after prior authentication).

1.4.2.3. Using cryptography for trusted communications

The trusted communication between TOE and VU is performed by using appropriate cryptographic mechanisms according to [ISO 16844-3:2004[7]] and [EU-2016/799[6], Annex 1C, Appendix 11, Parts A and B, with first or second-generation Vehicle Units, respectively.

2. Conformance Claims

2.1. CC Conformance Claim

This security target claims conformance to Common Criteria version 3.1 revision 5.

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [1].

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [3].

as follows:

Part 2 conformant,

Part 3 conformant (EAL4 augmented by ATE_DPT.2 and AVA_VAN.5).

2.2. PP Conformance Claim

This security target claims strict conformance to:

- Digital Tachograph – Motion Sensor [BSI-CC-PP-0093], Version 1.0, 9 May 2017 – compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C).

2.3. Package claim

This [ST] claims conformance to the assurance package defined in [6] Annex 1C, Appendix 10, as follows:“SEC_006 The assurance level for each Protection Profile shall be EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5”.

2.4. Conformance claim rationale

This security target claims strict conformance to the BSI-CC-PP-0093 [5] Protection Profile.

The Security Problem Definition (Section 3) of this ST includes the assets, the subjects, the assumptions, the threats and the organizational security policies as defined in the BSI-CC-PP-0093 [5].

The Security Objectives (Section 4) of this ST includes the security objectives as defined in the BSI-CC-PP-0093 [5].

The Security Functional Requirements section (6.2) of this ST include all SFRs presented in the BSI-CC-PP-0093 [5]. Iterations and changes to the SFRs introduced in this ST, with respect to the BSI-CC-PP-0093 [5], do not lower TOE security.

The Security Assurance Requirements section (6.3) of this ST claims conformance to EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5”. This is the package of security assurance requirement allowed for conformance to the BSI-CC-PP-0093 [5].

3. Security Problem Definition

3.1. Assets

The TOE has the following assets, which are to be protected in integrity and some of them in confidentiality and authenticity as described below.

Motion data (MOD) -Data sent from the motion sensor to the paired VU, reflecting the vehicle's speed and distance travelled. There are two aspects of motion data: real time speed pulses sent from a motion sensor; and secure data communications between a motion sensor and a VU.

Audit data (AUD): Details of events.

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

Keys to protect data (SDK): Enduring secret keys and session keys used to protect security and user data held within and transmitted by the TOE, and as a means of authentication.
Design and software code (TDS): Design information and source code (uncompiled or reverse engineered) for the TOE that could facilitate an attack.

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

3.2. Subjects and external entities

This following list of subjects interact with the TOE:

[1]. **Vehicle Unit (VU)**[1] is the vehicle unit (authenticated), to which the motion sensor is paired. The term "user" is also used within this ST to refer to a VU.

[2]. **Other Device** Other device (not authenticated)[2] to which the motion sensor is may be connected. This includes an unauthenticated vehicle unit.

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

Application Note 1

Defined subjects in the sense of [1] which can be recognised by the TOE independently of their nature (human or external IT entity). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entities except the Attacker and the Other Device, – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not distinguish between "subjects" and "external entities".

3.3. Threats

The following threats are defined for the TOE.

T.Access: Access control – a VU or other device (under control of an attacker) could try to use functions not allowed to them, and thereby compromise the integrity or authenticity of motion data (MOD).

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

---

[1] The sensors DTMS-2 may be paired with 2nd generation VU's, and optionally 1st generation VU's.

[2] The sensors DTMS-2 does not have any provisions for the connection of any management devices. However, in the case of a management device, it shall be possible to read the serial number of the device.

T.Environment: Environmental attacks – an attacker could compromise the integrity or authenticity of motion data (MOD) through physical attacks on the motion sensor (thermal, electromagnetic, optical, chemical, mechanical).
T.Hardware: Modification of hardware -An attacker could modify the motion sensor hardware (THW), and thereby compromise the integrity or authenticity of motion data (MOD).
T.Mechanical: Interference with mechanical interface –an attacker could manipulate the motion sensor input, for example, by disconnecting the sensor from the gearbox, such that motion data (MOD) does not accurately reflect the vehicle's motion.
T.Motion_Data: Interference with motion data - an attacker could add to, modify, delete or replay the vehicle's motion data, and thereby compromise the integrity or authenticity of motion data (MOD).
T.Security_Data: Access to security data - an attacker could gain illicit knowledge of secret cryptographic keys (SDK) during security data generation or transport or storage in the equipment, thereby allowing an Other Device to be connected.
T.Software: Attack on software -an attacker could modify motion sensor software (TDS) during operation, and thereby compromise the integrity, availability or authenticity of motion data (MOD).
T.Test: an attacker use of non-invalidated test modes or of existing back doors could permit manipulation of motion data (MOD).
T.Power_Supply: Invalid test modes -an attacker could vary the power supply to the motion sensor, and thereby compromise the integrity or availability of motion data (MOD).

3.4 Assumptions

This section describes the assumptions that are made about the operational environment in order to be able to provide the security functionality.

A.Approved_Workshops: It is assumed that the Authority States (Member State) approve, regularly control and certify trusted fitters and workshops to carry out installations, checks, inspections and repairs.

A.Controls : It is assumed that the law enforcement controls of the TOE will be performed regularly and randomly, and must include security audits (as well as visual inspection of the TOE).

A.Type Approved: It is assumed that the motion sensor will only be operated together with a VU being type approved according to [6] Annex 1C[3].

3.5 Organisational security policies

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.Crypto: The cryptographic algorithms and keys described in [6] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

[3] Type approval requirements include Common Criteria certification against the relevant digital tachograph protection profile

4. Security Objectives

4.1. General

This section identifies and defines the security objectives for the TOE and its operational environment. These security objectives reflect the stated intent, counter the identified threats, and take into account the assumptions.

4.2 Security objectives for the TOE

The following security objectives describe security functions to be provided by the TOE.

OT.Sensor_Main: The authentic motion data transmitted by the TOE must be provided to the VU, to allow the VU to accurately determine the movement of the vehicle in terms of speed and distance travelled.

OT.Access: The TOE must control access to functions and data.

OT.Audit: The TOE must audit attempts to undermine its security.

OT.Authentication: The TOE must authenticate a connected user (VU) before allowing access to data and functions.

OT.Processing: The TOE must ensure that processing of input to derive motion data is accurate.

OT.Reliability: The TOE must provide a reliable service.

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

OT.Secure_Communication: The TOE must secure data exchanges with the VU.

OT.Crypto_Implement: The cryptographic functions must be implemented within the TOE as required by [6] Annex 1C, Appendix 11.

OT.Software_Update: Where updates to TOE software are possible, the TOE must accept only those that are authorised[4].

Application refinement note 2:

OT.Software_Update is not considered in this document.

4.3 Security objectives for the operational environment

The following security objectives for the operational environment describe security functions to be provided by the TOE.

Design phase

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

Manufacturing phase

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

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

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

OE.Delivery: Manufacturers of the TOE, vehicle manufacturers and fitters or workshops must ensure that handling of the TOE is done in a manner that maintains IT security. Fitters and workshops shall particularly be informed of

[4] Implementation of a software update facility is optional for developers (according to footnote 6 of [BSI-CC-PP-0093[5]], but the sensor DTMS-2 does not implement any possibility to update the software.

their responsibility related to proper sealing of the mechanical interface.

OE.Data_Strong: Security data inserted into the TOE must be as cryptographically strong as required by [6] Annex 1C, Appendix 11.

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

Application note 3

Additional motion sensor manufacturer instruction required during manufacturing phase for the adjustment of pulses coefficient value stored in the TOE's non-volatile memory could be sent to the TOE, but the pairing of VU and TOE have to be done just after the TOE's response.

Installation phase

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

OE.Correct_Pairing: Approved fitters and workshops must correctly pair the TOE with a VU during the installation phase.

Operational phase

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

OE.Regular_Inspection: The TOE must be periodically inspected.

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

OE.Crypto_Admin: All requirements from [6] Annex 1C concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.

OE.Type_Approved_VU: The VU to which the TOE is connected must be type approved.

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

4.3.1. Security Problem Definition & Security Objectives

The following tables map security objectives with the security problem definition.

	OT.Sensor_Main	OT.Access	OT.Audit	OT.Authentication	OT.Processing	OT.Reliability	OT.Physical	OT.Secure_Communication	OT.Crypto_Implement
Threats									
T.Access		**X**		**X**				**X**	
T.Design							**X**		
T.Environment	**X**		**X**		**X**	**X**	**X**		
T.Hardware	**X**					**X**	**X**		
T.Mechanical	**X**								
T.Motion_Data	**X**			**X**	**X**		**X**	**X**	
T.Security_Data			**X**	**X**		**X**	**X**	**X**	
T.Software	**X**		**X**	**X**		**X**	**X**	**X**	

T.Test						**X**			
T.Power_Supply	**X**					**X**	**X**		
Organizational Security Policies									
OSP.Crypto									**X**

Table 4.1 TOE Security objectives & (Threats, Organizational Security Policies)

	OE.Development	OE.Manufacturing	OE.Data_Generation	OE.Data_Transport	OE.Delivery	OE.Data_Strong	OE.Test_Points	OE.Approved_Workshops	OE.Correct_Pairing	OE.Mechanical	OE.Regular_Inspection	OE.Controls	OE.Crypto_Admin	OE.Type_Approved_VU	OE.EOL
Threats															
T.Access							X								
T.Design	X	X	X	X	X		X	X							
T.Environment										X	X	X			
T.Hardware	X	X			X			X			X	X			
T.Mechanical										X	X	X			
T.Motion_Data									X						
T.Security_Data			X	X				X							X
T.Software	X	X			X						X				
T.Test		X					X								
T.Power_Supply											X	X			
Organizational Security Policies															
OSP.Crypto						X							X		

Table 4.2 Security Objectives for the Operational Environment & (Threats, Organizational Security Policies)

	OE.Development	OE.Manufacturing	OE.Data_Generation	OE.Data_Transport	OE.Delivery	OE.Data_Strong	OE.Test_Points	OE.Approved_Workshops	OE.Correct_Pairing	OE.Mechanical	OE.Regular_Inspection	OE.Controls	OE.Crypto_Admin	OE.Type_Approved_VU	OE.EOL
Assumptions															
A.Approved_Workschops								X							
A.Controls											X	X			
A.Type_Approved														X	

Table 4.3 Assumptions and Security Objectives for the environment

4.3.2. Rationale for the Security Objectives

This section provides a rationale objective that covers each threat, organizational security policy and assumption.

4.3.2.1. Threats & Objectives

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

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

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

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

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

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

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

T.Software is addressed by OT.Sensor_Main, which requires that motion data must be available to the VU, and by OT.Reliablility, which requires a reliable service. OT.Authentication and OT.Secure_Communication aim to prevent unauthorised connections to the TOE. OT.Physical deals with attempts to modify the software by means of a physical attack on the TOE, and OT.Audit aims to record attempted attacks. OE.Development, OE.Manufacturing and OE.Delivery address the prevention of software modification prior to installation. OE.Regular_Inspection helps to detect signs of interference with TOE software.

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

T.Power_Supply is addressed through OT.Reliability, which requires that the TOE should operate reliably and predictably, and through OT.Sensor_Main, which requires a supply of authentic data. OT.Physical requires that physical attacks that attempt to modify motion data can be detected. Within the operational environment regular workshop

inspections (OE.Regular_Inspections) and law enforcement controls (OE.Controls) will help to detect any interference.

4.3.2.2. Organizational Security Policies & Objectives

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

4.3.2.3. Assumptions & Objectives

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

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

A.Type_Approved is supported by OE.Type_Approved_VU, which requires that the VU that is coupled with the TOE is type approved.

5 Extended Components Definition

This security target does not use any components defined as extensions to Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2].

6. TOE Security Requirements

6.1. Typographical Conventions

The following conventions are used in the definitions of the SFRs:

- Selections made in this ST are written in **bold text and double underlined**, and the original text is indicated in a footnote.
- Assignments made in this ST are written in **italics and underlined**, and the original text is indicated in a footnote.
- Iterations are denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator.
- Refinement operations are indicated by striking out the original content of relevant part of the SFR as defined in [CC31p2] and expressing refined parameter in bold.
-

6.2 Security functional requirements

This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications.

6.2.1 Security functional requirements for the Motion Sensor

6.2.1.1 Class FAU Security Audit

6.2.1.1.1 FAU_GEN.1 Security 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[5];

b) All auditable events for the ***not specified***[6] level of audit; and

c) [***The following events*****[7]:**

I. ***Error in non-volatile memory***

II. ***Error in controller RAM***

III. ***Error in controller instruction***

IV. ***Error in communication***

V. ***Error in authentication***

VI. ***Error in sensor element***

VII. ***None***[8][9]

[5] Since audit functions on the TOE are always enabled this requirement can be considered satisfied
[6] [selection, choose one of: minimum, basic, detailed, not specified]
[7] Of the events optional, TOE only takes into account the Error in sensor element
[8] If the TOE casing is designed to be opened then an audit event shall be generated when that is done. [ST Authors: it is related to the [Case opening (optional] assignment, and the footnote is kept for preserving compatibility with the PP]
[9] [assignment: other specifically defined auditable events]

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

a) Date and time of event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event[10], and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***none***[11]].

Application note 4: The occurrence of an auditable event on the motion sensor is flagged to the VU, which can then request a transfer of the event data for storage in the VU. The minimum list of events available from the motion sensor is specified in [7].

The VU itself generates and stores motion sensor related events as defined by [6] Chapters 3.9, 3.12.8 and 3.12.9 and Appendix 1. The motion sensor itself has no date/time source, and the paired VU adds a date/time stamp to the records.

6.2.1.1.2 FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to [**prevent**[12]] unauthorized modifications to the stored audit records in the audit trail.

6.2.1.1.3 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [**overwrite the oldest storage record**[13]] and ***none***[14] if the audit trail is full.

6.2.1.2. Class FDP User data protection

6.2.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***access control SFP[15]*** on [

Subjects:

- ***VU***
- ***Other device***

Objects

- ***TOE symmetric keys (see Table 6.2 and Table 6.1)***
- ***Encrypted KP (with K_M) and encrypted motion sensor serial number (with K_{ID})***
- ***TOE executable code***
- ***TOE file system***
- ***Motion sensor identification data***
- ***Pairing data from first pairing***
- ***Motion data***

---

[10] When required data is not available an appropriate default indication shall be given (to be defined by manufacturer
[11] [assignment: other audit relevant information]
[12] [selection, choose one of: *prevent, detect*]
[13] [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]
[14] [assignment: other actions to be taken in case of audit storage failure]
[15] [assignment: access control SFP]

- ***Commands, actions, or test points, specific to the testing needs of the manufacturing phase***

Operations

Read, write, modify, delete][16].

6.2.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Access Control SFP*** [17]to objects based on the following: [

Subjects:

- ***VU***
- ***Other device***

Objects

- ***TSF secret keys (see Table 6.2 and Table 6.1)***
- ***Encrypted K_P (with K_M) and encrypted motion sensor serial number (with K_{ID})***
- ***TOE executable code***
- ***TOE file system***
- ***Motion sensor identification data***
- ***Pairing data from first pairing***
- ***Motion data***
- ***Commands, actions, or test points, specific to the testing needs of the manufacturing phase][18].***

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

a) The send data and pairing functions of the TOE are only accessible to an authenticated VU, according to [7];

b) Identification data, encrypted K_P, encrypted motion sensor serial number and pairing data from first pairing shall be written once only;

c) Secret keys shall not be externally readable;

d) The TOE file system and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion;

e) All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase, and it shall not be possible to restore them for later use;

f) Unauthenticated inputs from external sources shall not be accepted as executable code;

g) The TSF shall export motion data to the VU such that the VU can verify its integrity and authenticity;

h) Motion data shall only be processed and derived from the TOE's mechanical input][19].

---

[16] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[17] [assignment: access control SFP]

[18] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[19] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***none***][20].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***][21].

6.2.1.3.3 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [***Access Control SFP***][22] when exporting user data controlled under the SFP(s), outside the TOE.

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

Application note 5: FDP_ETC.1 covers the requirement to send motion data, including audit records, to the VU.

6.2.1.3.4 FDP_ETC.2 Export of user data with security attributes[23]

FDP_ETC.2.1 The TSF shall enforce the [***Access Control SFP***][24] when exporting user data controlled under the SFP(s), outside the TOE.

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

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

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [***none***][25].

6.2.1.3.5 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [***Access Control SFP***][26] when importing user data controlled under the SFP, from outside the TOE.

FDP_ITC.1.2 The TSF shall ignore any 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: [***cryptographic session keys will only be accepted from a VU that has been successfully paired with the TOE***][27].

Application note 6: FDP_ITC.1 covers the import of the motion sensor session key from the VU during pairing.

6.2.1.3.6 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in the TOE's data memory containers controlled by the TSF for ***data checksum/CRC errors***[28] on all objects, based on the following attributes: ***data checksum/CRC***[29].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall ***generate an audit record***[30].

---

[20] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[21] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[22] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[23] The motion sensor sends data to the VU accompanied by attributes that serve to authenticate the data.
[24] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[25] [assignment: additional exportation control rules]
[26] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[27] [assignment: *additional importation control rules*]
[28] [assignment: integrity errors]
[29] [assignment: user data attributes]
[30] [assignment: *action to be taken*]

6.2.1.3 Class FIA Identification and authentication

6.2.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **1**[31] unsuccessful authentication attempts occur related to ***pairing of a VU***[32].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met or surpassed**[33], the TSF shall [

a) generate an audit record of the event;

b) ***continue to export motion data in a non-secured mode (speed pulses only)]***[34].

6.2.1.3.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of attributes belonging to individual users: [

Pairing data from

a) first pairing with a VU;

b) ***last pairing with a VU]***[35].

6.2.1.3.3 FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall **detect and prevent**[36] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **detect and prevent**[37] use of authentication data that has been copied from any other user of the TSF.

Application note 7: "User" in FIA_UAU.3 includes any attacker.

6.2.1.3.4 FIA_UID.2 User identification before any action

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

Application note 8: The identification of the user is achieved during pairing of the motion sensor and the VU.

6.2.1.4 Class FPT Protection of the TSF

6.2.1.4.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state[38] when the following types of failures occur [

a) Reset;

b) Power supply cut-off;

c) Deviation from the specified values of the power supply;

---

[31] [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*]
[32] [assignment: *list of authentication events*]
[33] [selection: *met, surpassed*]
[34] [assignment: *list of actions*]
[35] [assignment: *list of security attributes*]
[36] [selection: *detect, prevent*]
[37] [selection: *detect, prevent*]
[38] A secure state is defined here as one in which all security data is protected.

d) ***Transaction stopped before completion[39]***[40].

6.2.1.4.2 FPT_PHP.2 Notification of physical attack

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

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

FPT_PHP.2.3 For [***motion sensor case opening***[41]**]**, the TSF shall monitor the devices and elements and notify [***a paired VU***[42]] when physical tampering with the TSF's devices or TSF's elements has occurred.

Application note 9: If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of 6 months. It is acceptable that the audit record is stored after power supply reconnection. If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection), and FPT_PHP.2.3 is not relevant (penetration of the case by other means is addressed by FPT_PHP.2.2).

6.2.1.4.3 FPT_PHP.3 Resistance to physical attack (1)

FPT_PHP.3.1 (1) The TSF shall resist ***use of magnetic fields to disturb vehicle motion detection***[43] to the ***TOE components implementing the TSF***[44] by responding automatically such that the SFRs are always enforced.

Application note 10: The TSF shall detect such interference and provide means to the VU to record a sensor fault. The detection of external magnetic field is carried out by measuring the operating point of the HMS. If the external magnetic field is so intensive that the operating point of the HMS is outside the assumed range an error is reported and an audit record is generated.

6.2.1.4.4 FPT_PHP.3 Resistance to physical attack (2)

FPT_PHP.3.1 (2) The TSF shall resist ***physical tampering attacks***[45] to the ***TSF software and TSF data***[46] by responding automatically such that the SFRs are always enforced.

6.2.1.4.5 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up and periodically during normal operation**[47] to demonstrate the correct operation of **the TSF**[48].

FPT_TST.1.2 The TSF shall ~~**provide authorized users with the capability**~~ **run a suite of self tests** to verify the integrity of **TSF data**[49].

FPT_TST.1.3 The TSF shall ~~**provide authorized users with the capability**~~ **run a suite of self tests** to verify the integrity of **TSF software**[50].

---

[39] Transaction stopped" here means an incomplete request received from the VU, or the incomplete transmission of a response to the VU.
[40] [assignment: *list of types of failures in the TSF*]
[41] [assignment: *list of TSF devices/elements for which active detection is required*]
[42] [assignment: *a designated user or role*]
[43] [assignment: *physical tampering scenarios*]
[44] [assignment: *list of TSF devices/elements*]
[45] [assignment: *physical tampering scenarios*]
[46] [assignment: *list of TSF devices/elements*]
[47] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]*]
[48] [selection: *[assignment: parts of TSF], the TSF*]
[49] [selection: *[assignment: parts of TSF data], TSF data*]
[50] [selection: *[assignment: parts of TSF], TSF*].

Application note 11: The strategy for running self-tests is specified and justified appropriately in the TOE summary specification.

6.2.1.5 Class FRU Resource utilization

6.2.1.5.1 FRU_PRS.1 Limited priority of service

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

FRU_PRS.1.2 The TSF shall ensure that each access to [***data processed in the motion sensor during pairing and and operation***][51] shall be mediated on the basis of the subjects assigned priority.

Application note 12: The list of the resources that are controlled and the basis of mediation are described in the TOE summary specification.

6.2.1.6 Class FTP Trusted path/channels

6.2.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communications channel between itself and ~~**another trusted IT product the**~~ **VU** 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 **another trusted IT product**[52] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***all communications with the VU***[53].

6.2.2 Security functional requirements for external communications (2nd Generation)

The security functional requirements in this section are required to support communications specifically with 2nd generation vehicle units.

6.2.2.1 Class FCS Cryptographic support

6.2.2.1.1 FCS_CKM.4 - Cryptographic key destruction (1)

FCS_CKM.4.1 (1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method (***see table 6.1***[54]) that meets the following [

- ***Requirements in table 6.1;***
- ***Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying***
- ***material so that it cannot be recovered by either physical or electronic means***[55]
- ***Java Card 3.0.1***][56].

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and time	Stored in

[51] [assignment: *controlled resources*]
[52] [selection: *the TSF, another trusted IT product*]
[53] [assignment: *list of functions for which a trusted channel is required*]
[54] [assignment: *cryptographic key destruction method*]
[55] Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.
[56] [assignment: *list of standards*]

K_S	Motion sensor session key[57]	Session key for confidentiality between a VU and the motion sensor in operational phase.	AES	Generated by the VU during pairing to the motion sensor.	Out of scope for this ST	Made unavailable when the motion sensor is paired to another (or the same) VU.	Motion sensor non-volatile memory (conditional, only if the motion sensor has been paired with a second- generation VU).
K_P	Motion sensor pairing key	Key used by a VU for encrypting the motion sensor session key when sending it to the motion sensor during pairing. Note (as explained in [5] Annex 1C, Appendix 11, section 9.2.1.2) that a motion sensor may contain up to 3 keys K_P, of consecutive generations.	AES	Generated by the motion sensor manufacturer; stored in motion sensor at the end of the manufacturing phase.	Out of scope for this ST	Made unavailable when the motion sensor has reached end of life.	Motion sensor non-volatile memory.

Table 6.1 – Second generation symmetric keys stored or used by a motion sensor

6.2.2.1.2 FCS_COP.1 - Cryptographic operation (1:AES)

FCS_COP.1.1 (1:AES) The TSF shall perform ***encryption/decryption to support confidentiality, authenticity and integrity of data exchanged between a VU and a motion sensor***[58] in accordance with a specified cryptographic algorithm ***AES***[59] and cryptographic key sizes [***128, 192, 256 bits***][60] that meet the following: [***FIPS PUB 197: Advanced Encryption Standard, and [5] Appendix 11, Part B***][61].

6.2.2.2 Class FIA Identification and authentication

6.2.2.2.1 FIA_UAU.2 - User authentication before any action (1)

FIA_UAU.2.1 (1) The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Part A, Chapter 12**[62] before allowing any other TSF-mediated actions on behalf of that user.

Application note 13: In the case of a motion sensor authentication (pairing) can be done only in the presence of a workshop card.

6.2.2.3 Class FTP Protection of TSF

6.2.2.3.1 FPT_TDC.1 - Inter-TSF basic TSF data consistency (1)

FPT_TDC.1.1 (1) The TSF shall provide the capability to consistently interpret ***secure messaging attributes as defined by [5] Annex 1C, Appendix 11 Part B***[63] when shared between the TSF and ~~another trusted IT product~~ **a VU**.

FPT_TDC.1.2 (1) The TSF shall use ***the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11 Part B***[64] when interpreting the TSF data from ~~another trusted IT product~~ **a VU** .

6.2.3 Security functional requirements for external communications (1st Generation)

The security functional requirements in this section are required to support communications specifically with 1st

[57] Note that a 'session' can last up to two years, until the next calibration of the VU in a workshop.
[58] [assignment: *list of cryptographic operations*]
[59] [assignment: *cryptographic algorithm*]
[60] [assignment: *cryptographic key sizes*]
[61] [assignment: *list of standards*]
[62] [refinement]
[63] [assignment: *list of TSF data types*]
[64] [assignment: *list of interpretation rules to be applied by the TSF*]

generation vehicle units.

6.2.3.1 Class FCS Cryptographic support

6.2.3.1.1 FCS_CKM.4 - Cryptographic key destruction (2)

FCS_CKM.4.1 (2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method (***see table 6.2***[65]) that meets the following [

- ***Requirements in table 6.2;***
- ***Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means***[66]***;***
- ***None]***[67].

Key Symbol	Description	*Purpose*	*Type*	Source	Generation Method	Destruction method and time	Stored in
K_S	Motion sensor session key[68]	Session key for confidentiality between a (first-generation) VU and the motion sensor in operational phase.	TDES	Generated by the VU during pairing to the motion sensor.	Out of scope for this ST	Made unavailable when the motion sensor is paired to another (or the same) VU.	Motion sensor non-volatile memory (conditional, only if the motion sensor has been paired with a first- generation VU).
K_P	Motion sensor pairing key	Key used by a (first-generation) VU for encrypting the motion sensor session key when sending it to the motion sensor during pairing.	TDES	Generated by the motion sensor manufacturer; stored in motion sensor at the end of the manufacturing phase.	Out of scope for this ST	Made unavailable when the motion sensor has reached end of life.	Motion sensor non-volatile memory (conditional, only if the motion sensor supports pairing to a first- generation VU).

Table 6.2 – First-generation symmetric keys stored or used by a motion sensor

6.2.3.1.2 FCS_COP.1 - Cryptographic operation (2:TDES)

FCS_COP.1.1 (2:TDES) The TSF shall perform ***encryption/decryption to support confidentiality, authenticity and integrity of data exchanged between a VU and a motion sensor***[69] in accordance with a specified cryptographic algorithm ***Triple DES in CBC mode***[70] and cryptographic key sizes ***112 bits***[71] that meet the following: [***[5] Annex 1C, Appendix 11 Part A, Chapter 3***][72].

6.2.3.2 Class FIA Identification and authentication

6.2.3.1.1 FIA_UAU.2 - User authentication before any action (2)

FIA_UAU.2.1 (2) The TSF shall require each user to be successfully authenticated **using the method described in [5]**

---

[65] [assignment: *cryptographic key destruction method*]

[66] Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

[67] [assignment: *list of standards*]

[68] Note that a 'session' can last up to two years, until the next calibration of the VU in a workshop.

[69] [assignment: *list of cryptographic operations*]

[70] [assignment: *cryptographic algorithm*]

[71] [assignment: *cryptographic key sizes*]

[72] [assignment: *list of standards*]

Annex 1C, Appendix 11, Part A, Chapter 3[73] before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.3 Class FTP Protection of TSF

6.2.3.3.1 FPT_TDC.1 - Inter-TSF basic TSF data consistency (2)

FPT_TDC.1.1 (2) The TSF shall provide the capability to consistently interpret ***secure messaging attributes as defined by [5] Annex 1C, Appendix 11 Part A, Chapter 5***[74] when shared between the TSF ~~and another trusted IT product~~ **a VU**.

FPT_TDC.1.2 (2) The TSF shall use ***the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11 Part A, Chapter 5***[75] when interpreting the TSF data from ~~another trusted IT product~~ **a VU**.

[73] [refinement]
[74] [assignment: *list of TSF data types*]
[75] [assignment: *list of interpretation rules to be applied by the TSF*]

6.3. Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with ATE_DPT.2 and AVA_VAN.5. The assurance components are identified in the table below with the augmented item in bold.

Assurance Class	Assurance Components
Development (ADV)	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)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support (ALC)	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)
Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)

	Testing: security enforcing modules (ATE_DPT.2)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability assessment (AVA)	**Advanced methodical vulnerability analysis (AVA_VAN.5)**

Table 6.3. Security Assurance Requirements

7. Rationale

7.1 Security objectives rationale

The following table provides an overview for security objectives coverage (TOE and its operational environment), also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

7.1.1 Security functional requirements rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

	OT.Sensor_Main	OT.Access	OT.Audit	OT.Authentication	OT.Processing	OT.Reliability	OT.Physical	OT.Secure_Communications	OT.Crypto_Implement
FAU_GEN.1 - Security audit data generation			x				x		
FAU_STG.1 - Protected audit trail storage			x						
FAU_STG 4 - Prevention of audit data loss			x						
FDP_ACC.1 - Subset access control		x		x		x			
FDP_ACF.1 - Security attribute based access control		x		x		x			
FDP_ETC.1 - Export of user data without security attributes	x		x						
FDP_ETC.2 - Export of user data with security attributes	x								
FDP_ITC.1 - Import of user data without security attributes				x				x	x
FDP_SDI.2 - Stored data integrity monitoring and action	x				x	x			
FIA_AFL.1 - Authentication failure handling				x					
FIA_ATD.1 - User attribute definition				x					
FIA_UAU.3 - Unforgeable authentication	x	x		x				x	
FIA_UID.2 - User authentication before any action	x	x		x				x	
FPT_FLS.1 - Failure with preservation of secure state						x			
FPT_PHP.2 - Notification of physical attack	x					x	x		
FPT_PHP.3 - Resistance to physical attack (1)	x					x	x		
FPT_PHP.3 - Resistance to physical attack (2)	x					x	x		
FPT_TST.1 - TSF testing	x				x	x			
FRU_PRS.1 - Limited priority of service					x	x			
FTP_ITC.1 - Inter-TSF trusted channel	x							x	
Security functional requirements for external communications (2nd Generation)									
FCS_CKM.4 - Cryptographic key destruction (1)				x				x	x
FCS_COP.1 - Cryptographic operation (1:AES)				x				x	x

FIA_UAU.2 - User authentication before any action (1)	x	x		x				x	
FPT_TDC.1 - Inter-TSF basic TSF data consistency (1)	x				x	x			
Security functional requirements for external communications (1st Generation)									
FCS_CKM.4 - Cryptographic key destruction (2)				x				x	x
FCS_COP.1 - Cryptographic operation (2:TDES)				x				x	x
FIA_UAU.2 - User authentication before any action (2)	x	x		x				x	
FPT_TDC.1 - Inter-TSF basic TSF data consistency (2)	x				x	x			

Table 7.1 - Security requirement coverage

7.1.2. Rationale

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below:

OT.Sensor_Main is handled by FDP_ETC.1 which ensure the export of motion data in compliance with policy. The FDP_ETC.2 ensures the export the motion sensor serial number to support verification of motion data authenticity. The FDP_SDI.2 requires the TOE to monitor stored data for integrity errors. The FIA_UAU.2 (1&2), FIA_UAU.3 and FIA_UID.2 ensures that the credentials of entities using the secure channel are established and maintained. The FPT_PHP.2 requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated. The FPT_PHP.3 (1&2) requires resistance to or reaction to magnetic physical attack that may interfere with motion data supply, and requires resistance to physical attacks designed to access TSF software. The FPT_TST.1 help to ensure that the TOE is operating correctly. The FTP_ITC.1 requires use of a secure channel for communication with the VU, and the FTP_TDC.1 (1&2) requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.

OT.Access is handled by FDP_ACC.1 and FDP_ACF.1 which defines the access control policy for the TOE. The FIA_UAU.2 (1&2), FIA_UAU.3 and FIA_UID.2 ensures that the credentials of entities using the secure channel are established and maintained.

OT.Audit is handled by FAU_GEN.1 and FAU_STG.1 which requires that the specified audit event and its records are protected against unauthorised deletion while held on the TOE. The FAU_STG.4 specifies the actions to be taken when the available storage for audit records on the TOE is full. The FAU_ETC.1 requires that recorded audit records are transmitted to the VU for storage.

OT.Authentication is handled by FDP_ACC.1 and FDP_ACF.1 which defines policy for protection of TOE identification data. The FDP_ITC.1 provides for the import of cryptographic session keys from the VU. The FIA_ATD.1, FIA_UAU.2 (1&2), FIA_UAU.3 and FIA_UID.2 ensures that the credentials of entities using the secure channel are established and maintained. The FIA_AFL.1 defines the actions to be taken when there is an authentication failure with the VU, and the FCS_CKM.4 (1&2), FCS_COP.1 (1:AES&2:TDES) define the required cryptography to be used by the TOE for authentication.

OT.Processing is handled by FDP_SDI.2 which requires the TOE to monitor stored data for integrity errors. The FPT_TST.1 help to ensure that the TOE is operating correctly. The FPT_TDC (1&2) requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted. The FRU_PRS.1 ensures that the TOE processes motion data correctly based on correct prioritisation of access to resources.

OT.Reliability is handled by FDP_ACC.1 and FDP_ACF.1 which defines policy for protection of TOE identification data. The FDP_SDI.2 requires the TOE to monitor stored data for integrity errors. The FPT_FLS.1 requires the TOE to preserve a secure state in the case of certain failure events. The FPT_PHP.2 requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated. The FPT_PHP.3 (1&2) requires resistance to or reaction to magnetic physical attack that may interfere with motion data supply, and requires resistance to physical attacks designed to access TSF software. The FPT_TST.1 help to ensure that the TOE is operating correctly. The FTP_ITC.1 requires use of a secure channel for communication with the VU, and the FTP_TDC.1 (AES&TDES) requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted. The FRU_PRS.1 ensures that the TOE processes motion data correctly based on correct prioritisation of access to resources.

OT.Physical is handled by FAU_GEN.1which ensures that audit records are stored when attempted physical tampering is detected. The FPT_PHP.2 requires that attempts at physical tampering are detected, and that, if the case is designed to

be opened, an audit record is generated. The FPT_PHP.3 (1&2) requires resistance to or reaction to magnetic physical attack that may interfere with motion data supply, and requires resistance to physical attacks designed to access TSF software.

OT.Secure_Communication is handled by FCS_CKM.4 (1&2), FCS_COP.1 (1:AES&2:TDES) which defines the required cryptography to be used by the TOE for authentication. The FDP_ITC.1 provides for the import of cryptographic session keys from the VU. The FIA_UAU.2 (1&2), FIA_UAU.3 and FIA_UID.2 ensures that the credentials of entities using the secure channel are established and maintained, and the FTP_ITC.1 requires use of a secure channel for communication with the VU

OT.Crypto_Implement is handled by FCS_CKM.4 (1&2), FCS_COP.1 (1:AES&2:TDES) which defines the required cryptography to be used by the TOE for authentication. The FDP_ITC.1 provides for the import of cryptographic session keys from the VU

7.1.3 SFRs' dependencies

The dependencies between SFRs are addressed as shown in Table 7.2.

SFR	Dependencies	Fulfilled by	Unfulfilled by
FAU_GEN.1	FPT_STM.1	-	FPT_STM1:see note 1 below
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	
FAU_STG.4	FAU_STG.1	FAU_STG.1	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1	FMT_MSA.3: see note 2 below
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1	
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1	
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	FDP_ACC.1	FMT_MSA.3: see note 3 below
FDP_SDI.2	-	-	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	
FIA_ATD.1	-	-	
FIA_UAU.3	-	-	
FIA_UID.2	-	-	
FPT_FLS.1	-	-	
FPT_PHP.2	FMT_MOF.1		FMT_MOF.1: see note 4 below
FPT_PHP.3 (1 & 2)	-	-	
FPT_TST.1	-	-	
FRU_PRS.1	-	-	
FTP_ITC.1	-	-	
2nd generation specific			
FCS_CKM.4 (1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FDP_ITC.1	

FCS_COP.1 (1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FDP_ITC.1 and FCS_CKM.4	
FIA_UAU.2 (1)	FIA_UID.1	FIA_UID.2	
FPT_TDC.1 (1)	-	-	
1st generation specific			
FCS_CKM.4 (2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FDP_ITC.1	
FCS_COP.1 (2:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FDP_ITC.1 and FCS_CKM.4 ((2nd generation))	
FIA_UAU.2 (2)	FIA_UID.1	FIA_UID.2	
FPT_TDC.1 (2)	-	-	

Table 7.2 - SFRs' dependencies

Note 1: Audit records are indicated to the VU as soon as they are available. The audit records are then transferred to the VU, which itself generates and stores motion sensor related events as defined by [6] Chapters 3.9, 3.12.8 and 3.12.9 and Appendix 1. Time stamping of these events is based on the VU internal clock. The requirement for the TOE to provide reliable time stamps is therefore not needed.

Note 2: The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Manufacturing Phase, and are fixed over the whole life time of the TOE. No management of default values for these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during the fitters and workshops phase, or within the usage phase of the TOE.

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

Note 4: CC Part 2 [2] paragraph 1220 states that the use of FMT_MOF.1 should be considered to specify who can make use of the capability, and how they can make use of the capability. Since the capability, if implemented, is always enabled use of FMT_MOF.1 is not relevant.

7.1.4 Rationales for SARs

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [6] Annex 1C, Appendix 10.

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre- defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects, entry ‘Attacker’). This decision represents a part of the conscious security policy for the recording equipment required by the regulations, and reflected by the current PP.

The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC CMS.4 Problem tracking CM coverage
	ALC DEL.1 Delivery procedures
	ALC DVS.1 Identification of security measures
	ALC LCD.1 Developer defined life-cycle model
	ALC TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE CCL.1 Conformance claims
	ASE ECD.1 Extended components definition
	ASE INT.1 ST introduction
	ASE OBJ.2 Security objectives
	ASE REQ.2 Derived security requirements
	ASE SPD.1 Security problem definition
	ASE TSS.1 TOE summary specification
ATE: Tests	ATE COV.2 Analysis of coverage
	ATE DPT.1 Testing: basic design*
	ATE FUN.1 Functional testing
	ATE IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis*

The augmentation*of EAL4 chosen comprises the following assurance components:

- **ATE_DPT.2 and AVA_VAN.5.**

For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package.

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

Table 7.3 - SARs' dependencies (additional to EAL4 only)

8. TOE Summary Specification

In order for the TOE to fulfil the Security Functional Requirements (SFRs) and to protects itself against interference, logical manipulation and bypass it use for this purpose various security functions (TSFs). This chapter will describe each security function assigned to the corresponding SFR class described in Chapter 6.

8.1. TOE Security Functions

8.1.1. Security Audit (FAU)

The TOE generates audit events. The Security relevant events are all errors (e.g. authentication, communication etc.) in the TOE and significant states reached by the TOE (e.g. successful pairing). Each audit record contains the date and time of the event (provided by VU, **see 8.1.2-c**), the type of event, the subject identity and the outcome (success or failure) of the event.

Storages audit events by TOE are protected from unauthorized deletion and/or modification. In case of the audit trail is full, TOE overwrite the oldest storage record to prevent audit data loss.

The security functionality described above meets the requirements:

- FAU_GEN.1 & FAU_STG.1 & FAU_STG.4

8.1.2. Cryptographic support (FCS)

Application refinement note 12:

The description of the pre-pairing phase below is for an explanation of pairing process only and this phase is out of the scope of TOE evaluation.

a) Pre-pairing phase

Vehicle units and motion sensors shall use symmetric cryptographic system to provide the following security services:

- pairing of a vehicle unit and a motion sensor,
- mutual authentication between a vehicle unit and a motion sensor,
- ensuring confidentiality of data exchanged between a vehicle unit and a motion sensor.

In the first-generation tachograph system the mentioned above security services are supported by TDES algorithm. TDES keys shall have the form (K_a, K_b, K_a) where K_a and K_b are independent 64 bits long keys (in fact parity bits are ignored, so the effective key length is 112 bits).

In the second-generation tachograph system the mentioned above security services are supported by AES algorithm. Three generations of AES keys are considered with length dependent on motion sensor master keys K_M managed by MSCA. Appropriately they have lengths 128, 192 and 256 bits.

In every case above motion sensor master keys are generated by European Root Certification Authority (ERCA) and managed as follows:

- both parts of K_M (i.e. $K_{M\text{-}VU}$ and $K_{M\text{-}WC}$) are generated randomly and independently, then combined to constitute the final value of K_M: $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$,
- both parts of K_M ($K_{M\text{-}VU}$ and $K_{M\text{-}WC}$) are sent to MSCA with additional necessary information (e.g. key version number),
- MSCA derives an identification key K_{ID} from the motion sensor master key by XORing it with a constant vector CV: $K_{ID} = K_M$ XOR CV; K_{ID} is necessary for an initialization of the motion sensor; values of CV are key generation dependent as follows:
  - ✓ for the first generation VU (TDES) - 48 21 5F 00 03 41 32 8A 00 68 4D 00 CB 21 70 1D hexadecimal,

- ✓ for the second generation VU and 128-bit AES - B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83 hexadecimal,
- ✓ for the second generation VU and 192-bit AES - 72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25 hexadecimal,
- ✓ for the second generation VU and 256-bit AES - 1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60 hexadecimal.

TOE manufacturer generates randomly a pairing key K_P for every generation of VU and for every generation of AES keys and delivers them along with the extended serial number N_s in a secure manner to MSCA. These are the pairing keys for TDES, AES128, AES192 and AES256.

MSCA encrypts the extended serial number N_s with the appropriate identification key K_{ID} and the pairing key K_P with the appropriate motion sensor master key K_M. Both cryptograms are returned in a secure manner to the TOE manufacturer (i.e. 4 pairs of cryptograms).

The structure of extended serial number is given in Table 34 [ISO 18644-3:2022].

For every generation of tachograph system and every generation of AES the following values have to be stored in non-volatile memory of the TOE (**see 8.1.3-a**):

- the extended serial-number N_S of the motion sensor in plain text [ISO 16844-3[7]] (the same for every generation of tachograph system and every generation of AES);
- the extended serial-number of the motion sensor encrypted with the appropriate identification key*;*
- the pairing key K_P of the motion sensor in plain text;
- the pairing key of the motion sensor encrypted with the appropriate master key.

The TOE establishes an appropriate algorithm and key length during the pairing with VU, so before delivery four complete sets of encrypted extended serial number and encrypted pairing keys have to be installed in the TOE.

The pairing key of the motion sensor encrypted with the K_M is used to transfer confidentially during pairing the value of K_P to VU. It is used to transfer confidentially the session key K_S and the pairing information from VU to TOE.

The pairing information shall be assembled as specified in section 7.6.10 of [ISO 16844-3:2004] for pairing with 1-st generation VU, and for pairing with 2-nd generation VU the AES algorithm shall be used instead of the TDES algorithm in the pairing data encryption scheme, thus resulting in two AES encryptions, and adopting the padding method 2 defined in [ISO 9797-1] (in case the plaintext data length is not a multiple of 16 bytes) to fit with the AES block size. The key K'p used for this encryption shall be generated as follows:

- In case the pairing key K_P is 16 bytes long: $K'p = K_P \text{ XOR } (N_s \| N_s)$
- In case the pairing key K_P is 24 bytes long: $K'p = K_P \text{ XOR } (N_s \| N_s \| N_s)$
- In case the pairing key K_P is 32 bytes long: $K'p = K_P \text{ XOR } (N_s \| N_s \| N_s \| N_s)$

where N_s is the 8-byte serial number of the motion sensor [CSM 219, Annex 1C, COMMISSION IMPLEMENTING REGULATION (EU) 2016/799[6]].

The session key K_S is used for the purpose of data encryption until the next pairing of the TOE with the same or another VU or the end of life cycle.

The keys are stored in the Security Module embedded in the TOE and accessed using an application running on the Security Module).

b) Pairing

From the point of view of TOE the pairing procedure consists of the following consecutive steps [CSM 217, Annex 1C, COMMISSION IMPLEMENTING REGULATION (EU) 2016/799[6]],

1. The VU sends the instruction to initiate the pairing process towards the motion sensor, as described in [ISO 16844-3[7]], and encrypts the serial number it receives from the motion sensor with the identification key K_{ID}. The VU sends the encrypted serial number back to the motion sensor.

2. The motion sensor compares the encrypted serial number consecutively with each of the encryptions of the serial number it holds internally. If it finds a match, the VU is authenticated (**see 8.1.4-c**). The motion sensor notes the kind (TDES or AES) and generation of K_{ID} used by the VU and returns the matching encrypted version of its pairing key; i.e. the encryption that was created using the same kind (TDES or AES) and generation of K_M.
3. The VU decrypts the pairing key using K_M, generates a session key K_S, encrypts it with the pairing key and sends the result to the motion sensor. The motion sensor decrypts K_S (**see 8.1.3-b**).
4. The VU assembles the pairing information as defined in [ISO 16844-3], encrypts the information with the pairing key, and sends the result to the motion sensor (**see 8.1.4-c**). The motion sensor decrypts the pairing information.
5. The motion sensor encrypts the received pairing information with the received K_S and returns this to the VU. The VU verifies that the pairing information is the same information which the VU sent to the motion sensor in the previous step. If it is, this proves that the motion sensor used the same K_S as the VU and hence in step 2 sent its pairing key encrypted with the correct generation of K_M. Hence, the motion sensor is authenticated.

All above steps are performed by consecutive sending by VU specific instructions specified in [ISO 16844-3[7]] with numbers 40, 41, 42, 43 and 50 respectively.

All keys involved in the pairing of a first-generation VU and a motion sensor shall be TDES keys as specified in [ISO 16844-3[7]].

All keys involved in the pairing of a second-generation VU and a motion sensor shall be AES keys. These AES keys may have a length of 128, 192 or 256 bits. Since the AES block size is 16 bytes, the length of an encrypted message must be a multiple of 16 bytes, compared to 8 bytes for TDES.

The differences between the lengths of plain and encrypted data in the case of both VU generations during pairing are presented in Table 6 CSM 216 [7].

The security functionality concerning data encryption described above meets the requirements:

FCS_COP.1 (1:AES) & FCS_COP.1 (2:TDES)

c) Communication and session key usage

After the successful pairing the session key K_S is used to protect exchanged data between a motion sensor and VU. According [ISO 16844-3[7]] two cases of data exchange occur for this purpose.

The first one, represented by instructions with numbers 70 and 80, is used to transfer confidentially the motion sensor counter value and other data appropriate for the description of motion sensor state to VU.

The second, represented by instructions with numbers 10 and 11, is used to transfer confidentially the contents of one from 7 files numbered from 0 to 6 and defined in [ISO 16844-3[7]].

All keys involved in this communication of a first-generation VU and a motion sensor shall be TDES keys as specified in [ISO 16844-3].

All keys involved in this communication of a second-generation VU and a motion sensor shall be AES keys. These AES keys may have a length of 128, 192 or 256 bits. Since the AES block size is 16 bytes, the length of an encrypted message must be a multiple of 16 bytes, compared to 8 bytes for TDES.

The differences between the lengths of plain and encrypted data in the case of both VU generations during mentioned above data exchanges are presented in Table 6 CSM 216 [7].

The data exported from the TOE depend on instruction number sent to the TOE by VU. For instructions pair 10/11 the contents of the one of 7 files defined in [ISO 13866-3[7]] is exported to VU. In the case of 70/80 instruction pair the counter value and other data appropriate for the description of motion sensor state are exported (**see 8.1.3-b**).

The security functionality concerning data encryption described above meets the requirements:

FCS_COP.1 (1:AES) & FCS_COP.1 (2:TDES)

d) Key destruction

The session key K_S is made unavailable when the TOE is paired to another (or the same) VU or by the Security Module software during error detection handling process.

All the pairing keys K_P stored in non-volatile memory of the TOE are made unavailable when the motion sensor has reached end of life.

The security functionality described above meets the requirements:

- **FCS_CKM.4 (1) & FCS_CKM.4 (2)**

8.1.3. User Data Protection (FDP)

a) Access control

TOE controls access rights to its functions and identification data. TOE only accepts and stores user data from authenticated VU only. TOE stores in its memory software installation data and has the ability to block access to it from any future changes including updates or deletion. Upon request from authenticated VU, TOE has the capability to manufacturing accountability data (counter value).

The security functionality described above meets the requirements:

- FDP_ACC.1 & FDP_ACF.1

b) Export and import user data

TOE provides information flow control when importing and exporting data during the pairing (**see 8.1.2-b**) and following data exchange with authenticated VU (**see 8.1.2-c**). TOE assures the export of motion data (e.g. serial number) in compliance with policy to support verification of motion data authenticity. Recorded audit records are transmitted by TOE to the VU for storage

The security functionality described above meets the requirements:

- FDP_ETC.1 & FDP_ETC.2 & FDP_ITC.1

c) Stored data integrity monitoring and action

The TOE checks user data stored in its memory for integrity errors (just after successful start-up and periodically during operation). When an integrity error (the checksum is incorrect) in the stored data is detected, the TOE generates an audit record.

The security functionality described above meets the requirements:

- FDP_SDI.2

8.1.4. Identification and authentication (FIA)

a) Authentication failure handling

The TOE defines the actions to be taken when there is an authentication failure with the VU. When the defined number of unsuccessful authentication attempts has been met, the TOE generates an audit record of the event, warns the VU about it and continues with the export of motion data in unsecured mode, i.e. only analogue pulses on pin 3.

The security functionality described above meets the requirements:

- FIA_AFL.1

b) User attribute definition

The TOE maintains security attributes set during the first and last pairing with VU using the secure channel (**see 8.1.2-c**).

The security functionality described above meets the requirements:

- FIA_ATD.1

c) User authentication and identification

The TOE maintains the credentials of the VU shared with TOE using a secure channel (**see 8.1.2-c**). The TOE is able to authenticate any VU or management device to which it is connected (both when the VU is connected and when power is

restored). Additionally, the TOE detects and prevents the use of credentials that have been copied and replayed, and provides associated audit events.

The security functionality described above meets the requirements:

- FIA_UAU.2 (1), FIA_UAU.2 (2), FIA_UAU.3, FIA_UID.2

8.1.5. Protection of the TSF (FPT)

a) Failure with preservation of secure state

The TOE requires a secure state to be maintained in the event of certain failure events ((e.g. detection of broken EEPROM cells, corruption of check-summed objects, etc.). When a failure occurs, the TOE interrupts secure data communication, generates and stores an audit events.

The security functionality described above meets the requirements:

- FPT_FLS.1

b) Notification of physical attack

TOE provides physical tampering detection by the use of a protective casing which is not designed for opening. TOE shall be designed in such a way that physical tampering attempts can be easily detected (e.g. through visual inspection the security seal used to seal the TOE in the manner the seal cannot be removed and re-attached).

The security functionality described above meets the requirements:

- FPT_PHP.2

c) Resistance to physical attack

TOE requires resistance or reaction to magnetic physical attack that may interfere with motion data supply and resistance to physical attacks designed to access TSF software.

The security functionality described above meets the requirements:

- FPT_PHP.3 (1) & FPT_PHP.3 (2)

d) Inter-TSF basic TSF data consistency

TOE requires a secure protocol defined by [CIR-EU-2016/799[6]] Annex 1C, Appendix 11 Part B (2nd generation) and Part A, Chapter 5 (1st generation), such that the attributes of the user data transferred to VU can be consistently interpreted.

The security functionality described above meets the requirements:

- FPT_TDC.1 (1) & FPT_TDC.1 (2)

e) TSF testing

TOE runs self-tests during initial start-up and during normal operation to detect a sensor fault. These self-tests verify the integrity of executable code of the main microcontroller that is stored in the non-volatile memory. The self-tests also verify the correct operation of the TOE.

TOE also monitors application code, application data and application keys for integrity errors (keys are stored in secure structures of JavaCard and are protected by JCOP system [8]). Upon detection of an integrity error for the application code/data it stops the current instruction execution, throws a Security Exception and sets a register bit which is checked by the TOE. The TOE then generates an audit record (sensor fault), sets the flag NARA and all keys will be deleted (when the detected inconsistencies are repeated cyclically under the TOE end of life all keys and serial number are destroyed).

The security functionality described above meets the requirements:

- FPT_TST.1

8.1.6. Resource utilization (FRU)

TOE ensures that access to resources is correctly prioritized. Controlled resources are information which are processed in the TOE and they concern information needed for pairing and operation (specifically the following: extended serial number in plaintext, extended serial number encrypted with identification key, operating system identifier, security identifier, type approval, pairing key in plaintext, pairing key encrypted with master key, session key). The priority is given by a given instruction sequence which is defined in specifications: [6] section 12, and [7] section 7.

The security functionality described above meets the requirements:

- FRU_PRS.1

8.1.7. Trusted path/channels (FTP)

TOE ensures the trusted channel between itself and the VU to ensure that the motion data are not manipulated or changed unintentionally during the transport to the VU (see 8.1.2-c).

The security functionality described above meets the requirements:

- FTP_ITC.1

9. Glossary

9.1 Glossary

Glossary Term	Definition
Application note	Informative part of the PP containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE.
Approved Workshops	Fitters and workshops installing, calibrating and (optionally) repairing motion sensors, and being approved to do so by an EU Member State, so that the assumption A.Approved_Workshops is fulfilled.
Attacker	A person, or a process acting on their behalf, trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained.
Authentication	A function intended to establish and verify a claimed identity.
Authentication data	Data used to support verification of the identity of an entity.
Authenticity	The property that information is coming from a party whose identity can be verified.
Calibration	Updating or confirming motion sensor parameters held in the data memory of a VU. Calibration of a VU requires the use of a workshop card.
CRC	An error-detecting code used to detect changes to digital data.
Data memory	An electronic data storage device built into the motion sensor.
Digital Signature	Data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data.
Event	An abnormal operation detected by the motion sensor that may result from a fraud attempt.
Fault	An abnormal operation detected by the motion sensor that may arise from an equipment malfunction or failure.
Installation	The mounting of a motion sensor in a vehicle.
Integrity	The property of accuracy and completeness of information.
Interface	A facility between systems that provides the media through which they can connect and interact.

Manufacturer	The generic term for a manufacturer producing the motion sensor as the TOE.
Motion Sensor	A part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Motion sensor identification data	Data identifying the motion sensor: name of manufacturer, serial number, approval number, embedded security component identifier and operating
	system identifier. Motion sensor identification data are part of security data. These are stored in clear in the motion sensor's permanent memory.
Motion data	Data sent from the motion sensor to the paired VU, reflecting the vehicle's speed and distance travelled. There are two aspects of motion data: real time speed pulses sent from a motion sensor; and secure data communications between a motion sensor and a VU
Pairing	A process whereby, in the presence of a workshop card, a VU and a motion sensor mutually authenticate each other, and establish a session key to be used to protect the confidentiality and authenticity of motion data exchanged between them in operation.
Pairing Data	Pairing data contains encrypted information about the date of pairing, VU type approval number, and VU serial number of the VU with which the motion sensor was paired.
Personalisation	The process by which the equipment-individual data are stored in and unambiguously, inseparably associated with the related equipment.
Security Certification	Process to certify, by a Common Criteria certification body, that the TOE fulfils the security requirements defined in the relevant Protection Profile.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys and certificates).
Self Test	Tests run cyclically and automatically to detect faults.
Smart Tachograph System	The recording equipment, tachograph cards and the set of all directly or indirectly interacting equipment during their construction, installation, use, testing and control, such as cards, remote early detection communication readers and any other equipment for data downloading, data analysis, calibration, generating, managing or introducing security elements, etc.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]). In this PP TSF data the term security data is also used.
User	A legitimate user of the TOE, being a paired VU.
User Data	Any data, other than security data, recorded or stored by the motion sensor. User data include motion sensor identification data and motion data. The CC gives the following generic definitions for user data: Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
VU	The tachograph excluding the motion sensor and the cables connecting the motion sensor.

Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
Workshop Card	A tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the user and allows for the testing, calibration and activation of tachographs, and/or downloading from them.

10. Bibliography

Common Criteria

[1]. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, September 2017

[2]. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, September 2017

[3]. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, September 2017

[4]. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, September 2017

Digital tachograph: directives and standards

[5]. Common Criteria Protection Profile, Digital Tachograph – Motion Sensor (MS PP), BSI-CC-PP-0093, Version 1.0, 9 May 2017, DG JRC – Directorate E – Space, Security and Migration Cyber and Digital Citizens' Security Unit E3

[6]. Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

[7]. ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

[8]. Certification Report JCOP 4.7 SE051, EAL 6 augmented with ASE_TSS.2 and ALC_FLR.1. TÜV Rheinland Nederland B.V. July 2020

[9]. EN 16882:2016, June 2017, Road vehicles – Security of the mechanical seals used on tachographs – Requirements and test procedures

[10]. Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex I B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13 March 2004 (OJ L 71)

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