PARS

AR-GE VE BİLGİ TEKNOLOJİLERİ LTD. ŞTİ.

PARS MOTION SENSOR

PMS-101 v0.2

Common Criteria Evaluation

Security Target Lite

Document Name:	PARS Motion Sensor Security Target Lite
Document ID:	Pars_PMS-101_v0.2_STLite_v0.1
Dissemination Level:	Public
Status:	Final version
Document Version:	0.1
Version Date:	12.02.2018
Author(s):	Sarp Ertürk

DOCUMENT HISTORY

Version	Prepared By	Date	Explanations
V0.1	Sarp Ertürk	12.02.2018	Final version

CONTENTS

1 ST INTRODUCTION

1.1 ST Reference

ST Title	PARS Motion Sensor PMS-101 v0.2 Security Target Lite
Version	V0.1

1.2 TOE Reference

Target of Evaluation	PARS Motion Sensor PMS-101
Version	v0.2

1.3 TOE OVERVIEW

1.3.1 TOE definitions and operational usage

The Target of Evaluation (TOE) addressed by this security target is a second generation Tachograph Motion Sensor in the sense of [5] Annex 1C, intended to be used in the digital tachograph system. The Digital Tachograph system additionally contains a vehicle unit, tachograph cards, an external GNSS module (if applicable) and remote early detection communication readers.

A motion sensor is installed within a road transport vehicle as part of a digital tachograph system. Its purpose is to provide a vehicle unit with motion data that accurately reflects the vehicle's speed and distance travelled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement is representative of the vehicle's speed and distance travelled. It may be located in the vehicle's gear box or in any other part of the vehicle. In the operational phase the motion sensor is connected to a vehicle unit. In its operational phase TOE will not conmnect any other device.

A motion sensor meeting the requirements of this ST can be paired and used with second generation vehicle units, and with first generation vehicle units.

The functional requirements for a Motion Sensor are specified in [5] 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 vehicle unit are described in ISO 16844-3 [7].

In its operational mode, the motion sensor is connected to a VU. PMS-101 motion sensor is described in the following figure:

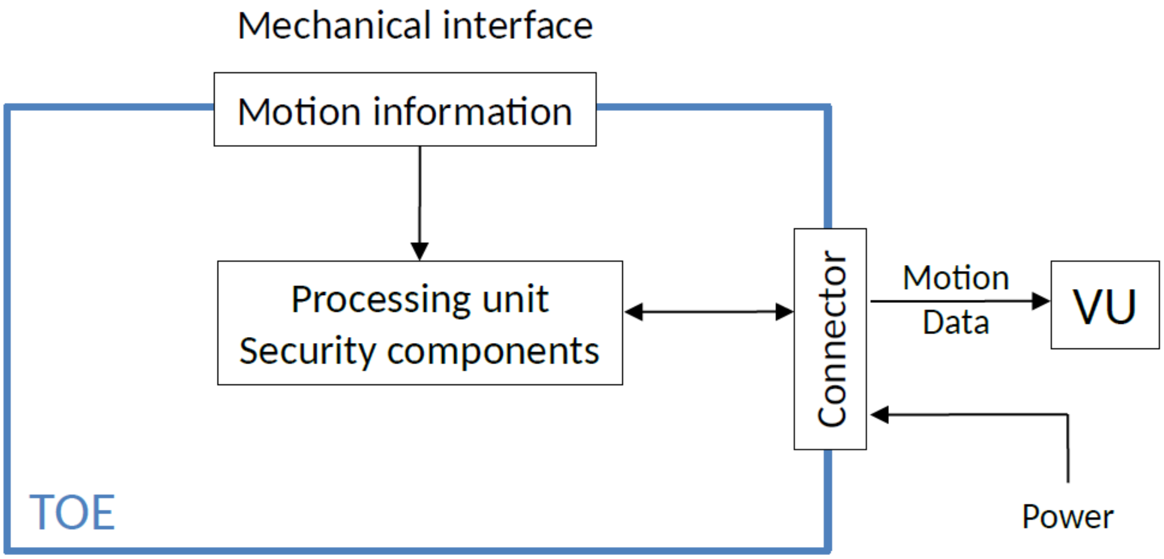

Figure 1 Typical motion sensor

Main objective of the digital tachograph system is given as "The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed". Usage of the motion sensor provides data to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance travelled.

1.3.2 TOE major security features

The motion sensor aims to protect data that is stored and transferred in such a way as to prevent unauthorised 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:

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

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

- Vehicle Unit identification and authentication;
- Access control to functions and stored data, according to [7];
- Alerting of events and faults;
- Integrity of stored data;

- Reliability of services , including self-testing, physical protection, control of executable code, resource management, and secure handling of events;
- Data exchange with a Vehicle Unit;
- Cryptographic support for VU to motion sensor mutual authentication and secure messaging according to [5] Annex 1C, Appendix 11.

All cryptographic mechanisms for communications with first or second-generation vehicle units, including algorithms and the length of corresponding keys, have to be implemented exactly as required and defined in [5] Annex 1C, Appendix 11, Parts A and B, respectively.

1.3.3 TOE Type

The TOE is a motion sensor in accordance with [5] Annex 1C, and Appendix 11 of that document.

PMS-101 motion sensor product life-cycle is composed of 5 phases as follows:

- Phase 1: Design
- Phase 2: Manufacturing
- Phase 3: Installation
- Phase 4: Operational
- Phase 5: End of life

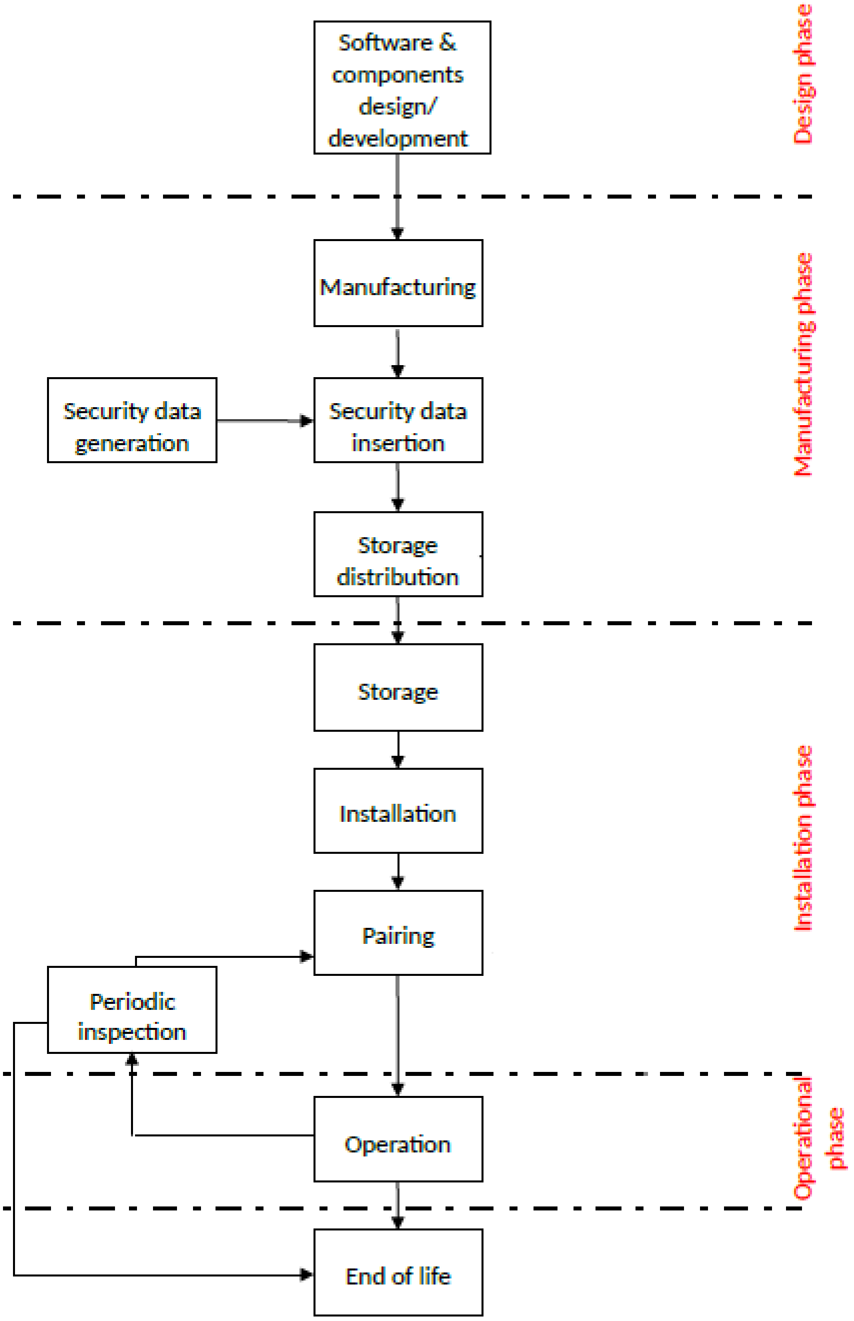

Figure 2 Motion Sensor Lifecycle

1.3.4 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 vehicle unit, and must be installed in a motor vehicle.

1.4 TOE DESCRIPTION

1.4.1 Physical Scope

TOE physically consists of the following hardware, software and documentation components;

- ✓ Hardware components
  - ➢ Sensor (takes motion information from gearbox and sends it to the comparator or directly to the motion sensor connector)
  - ➢ Microcontroller (uC) (do/manage motion sensor functionality according to regulations, see more information in section 1.4.2)
  - ➢ Peripheral Units
- ✓ Software components
  - ➢ Motion sensor software (Runs on the uC)
  - ➢ User data (In uC's memory)
  - ➢ TSF data (In uC's memory)
- ✓ Documentation
  - ➢ Preparative procedures
  - ➢ Operational user guidance

Physically TOE has hardware and software components. Hardware component version is v0.1 and software component version is v0.2.

1.4.2 Logical Scope

TOE logically consists of the following functionalities;

- ✓ **Identification and Authentication**

  The motion sensor performs an initial authentication of the VU during the pairing process. Authentication is performed by proofing knowledge of a common secret (K_M(Master key), K_{ID} (derived Master key – identification key)) between the motion sensor and the vehicle unit. During the pairing process a new secret (K_S (session key)) common only to the vehicle unit and the motion sensor that performed the pairing is established.

- ✓ **Data Exchange**

  The motion sensor communicates with the Vehicle Unit. During communication the motion sensor exports sensor data, motion sensor identification data, motion sensor initial security data to the Vehicle Unit and imports motion sensor pairing security data from the Vehicle Unit.

- ✓ **Cryptographic Support**

TOE uses Triple-DES (with 2 keys) encryption and decryption operations for first generation digital tachograph systems and AES (128 bit, 192 bit , 256 bit) encryption and decryption operations for second generation digital tachograph systems during data exchange with reading information (from file) instructions (10, 11) and reading sensor data instructions (70, 80).

The session key used for communication with the vehicle unit is generated by the vehicle unit during pairing and then distributed in a secure and authenticated way to the motion sensor.

- ✓ **Access Control**

Access controls ensure that access to the TOE functions can be performed only by those authorised to do so. There is only one authorised entity (VU) of the motion sensor at a given time. Access control is performed on the basis of the commands that the vehicle unit is allowed to submit to the motion sensor.

- ✓ **Integrity Protection**

The sensor and the processing unit (uC) of the motion sensor are installed in a box designed so that it cannot be opened and the TOE is a sealed device. So integrity protection of the stored data is provided by design. Beyond that property active stored data integrity checks are performed by data hashing within the TOE for the integrity of stored data in the internal memory.

- ✓ **Audit**

The motion sensor generates audit records of the following events and transmits them to the Vehicle Unit.

- ➢ security breach attempts (authentication failure, Stored data integrity error)
- ➢ sensor fault

The VU time stamps the audit events which come from the Motion sensor. So Motion sensor security functionality do not need to provide a reliable time stamp.

- ✓ **Reliability**

The physical construction of the motion sensor is of a way that opening the motion sensor box isn’t possible without destroying it. This way a manipulation gets obvious. Furthermore the motion sensor is sealed at the gearbox. The motion sensor contains a power supply unit that controls the voltage and smoothness of the power input. The TOE is designed in a way that each power cut-off or variation results in a reset which provides a secure state in each instance. TOE also provides a sensing element which is immune to magnetic fields. Self testing of the TOE is performed for the accuracy of the integrity of stored data.

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This Security Target and TOE claims conformance to

- ✓ Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- ✓ Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- ✓ Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

as follows

- ✓ Part 2 conformant,
- ✓ Part 3 conformant.

The

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

has to be taken into account during evaluation.

2.2 PP Conformance Claim

This Security Target claims strict conformance to the following Protection Profile:

Protection Profile: Digital Tachograph – Motion Sensor	
Title	: Common Criteria Protection Profile: Digital Tachograph – Motion Sensor (MS PP)
Sponsor	: Joint Research Centre, European Commission
Editors	: Julian Straw, David Bakker, Jacques Kunegel, Luigi Sportiello
CC version	: 3.1(Revision 4)
Assurance level	: EAL4 augmented with ATE_DPT.2 and AVA_VAN.5
Version number	: 1.0
Registration	: BSI-CC-PP-0093
Keywords	: Digital Tachograph, Motion Sensor

2.3 Package Conformance Claim

This Security Target claims conformance to package EAL4 augmented with ATE_DPT.2 and AVA_VAN.5.

2.4 Conformance Claim Rationale

The type of TOE defined in this ST is a motion sensor in accordance with [5] Annex 1C, and Appendix 11 of that document and strictly compliant with the TOE type defined in the PP claimed in the section 2.2.

3 SECURITY PROBLEM DEFINITION

3.1 Introduction

3.1.1 Assets

The assets to be protected by the TOE and its environment within phase 4 of the TOE's life-cycle are the application data defined in the tables below.

Table 1 Primary assets to be protected by the TOE and its environment

No.	Asset	Definition
1	Motion data (MOD)	Motion data (see Glossary for more details)

Table 2 Secondary assets to be protected by the TOE and its environment

No.	Asset	Definition
2	Audit data (AUD)	Details of events
3	Identification data (IDD)	Name of manufacturer, serial number, approval number, embedded security component identifier, operating system identifier.
4	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.
5	TOE design and software code (TDS)	Design information and source code (uncompiled or reverse engineered) for the TOE that could facilitate an attack.
6	TOE hardware (THW)	Hardware used to implement and support TOE functions.

The primary asset represents User Data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary asset. The secondary assets represent TSF-data in the sense of the CC. User data include motion data (see Glossary for more details), and match User Data in the sense of the CC. Security data are defined as specific data needed to support security enforcement, and match the TSF data in the sense of the CC.

3.1.2 Subjects and external entities

This Security Target considers the following subjects, who can interact with the TOE.

Table 3 Subjects and external entities

No.	Role	Definition
1	Vehicle Unit[1]	Vehicle unit (authenticated), to which the motion sensor is paired. The term “user” is also used within this ST to refer to a vehicle unit.
2	Other Device	Other device (not authenticated) to which the motion sensor may be connected. This includes an unauthenticated vehicle unit.
3	Attacker	A human, or process acting on their behalf, located outside the TOE. For example, a driver could be an attacker if he attempts to interfere with the motion sensor. An attacker is a threat agent (a person with the aim of manipulating user data, or a process acting on their behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the maintained assets. The attacker is assumed to possess at most a high attack potential.

Application note 1: The above table defines the 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”.

3.2 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats arise from the assets protected by the TOE and the method of TOE’s use in the operational environment.

[1] Motion sensors may be paired with 2nd generation Vehicle Units, and 1nd generation vehicle units.

The threats are defined in the following table.

Table 4 Threats addressed by the TOE

Label	Threat
T.Access	**Access control** – A vehicle unit or other device (under control of an attacker) could try to use functions not allowed to them, and thereby compromise the integrity or authenticity of motion data (MOD).
T.Design	**Design knowledge -** An attacker could try to gain illicit knowledge of the motion sensor design (TDS), either from manufacturer's material (e.g. through theft or bribery) or from reverse engineering, and thereby more easily mount an attack to compromise the integrity or authenticity of motion data (MOD).
T.Environment	**Environmental attacks –** An attacker could compromise the integrity or authenticity of motion data (MOD) through physical attacks on the motion sensor (thermal, electromagnetic, optical, chemical, mechanical).
T.Hardware	**Modification of hardware -** An attacker could modify the motion sensor hardware (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.Tests	**Invalid test modes -** The use by an attacker of non-invalidated test modes or of existing back doors could permit manipulation of motion data (MOD).
T.Power_Supply	**Interference with power supply** – An attacker could vary the power supply to the motion sensor, and thereby compromise the integrity or availability of motion data (MOD).

3.3 Assumptions

This section describes the assumptions that are made about the operational environment in order to be able to provide the security functionality. If the TOE is placed in an operational environment that does not uphold these assumptions it may be unable to operate in a secure manner.

The assumptions are provided in the following table.

Table 5 Assumptions

Label	Assumption
A.Approved_Workshops	**Approved Workshops -** The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, checks, inspections and repairs.
A.Controls	**Controls -** Law enforcement controls of the TOE will be performed regularly and randomly, and must include security audits (as well as visual inspection of the TOE).
A.Type_Approved	**Type Approved VU -** The motion sensor will only be operated together with a vehicle unit being type approved according to [5] Annex 1C.

3.4 Organisational Security Policies

This section shows the organisational security policies that are to be enforced by the TOE, its operational environment, or a combination of the two.

The organisational security policies are provided in the following table.

Table 6 Organisational Security Policy

Label	Organisational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [5] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

4 SECURITY OBJECTIVES

This section identifies the security objectives for the TOE and for its operational environment. The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- Provide a high-level, natural language solution to the problem;
- Divide this solution into two part wise solutions, that reflect that different entities each have to address a part of the problem;
- Demonstrate that these part wise solutions form a complete solution to the problem.

4.1 Security Objectives for the TOE

The TOE security objectives address the protection to be provided by the TOE, independent of the TOE environment, and are listed in the table below.

Table 7 Security objectives for the TOE

Short Name	Security objectives for the TOE
O.Sensor_Main	**Accuracy, integrity and authenticity of data -** The authentic motion data transmitted by the TOE must be provided to the vehicle unit, to allow the vehicle unit to accurately determine the movement of the vehicle in terms of speed and distance travelled.
O.Access	**Access** – The TOE must control access to functions and data.
O.Audit	**Audit -** The TOE must audit attempts to undermine its security.
O.Authentication	**Authenticated access -** The TOE must authenticate a connected user (vehicle unit) before allowing access to data and functions.
O.Processing	**Motion data derivation –** The TOE must ensure that processing of input to derive motion data is accurate.
O.Reliability	**Reliable service** - The TOE must provide a reliable service.
O.Physical	**Physical protection -** The TOE must resist attempts to access TSF software, and must ensure that physical tampering attacks on the TOE hardware can be detected.
O.Secure_Communication	**Secure data exchange –** The TOE must secure data exchanges with

	the vehicle unit.
O.Crypto_Implement	**Cryptographic operation** – The cryptographic functions must be implemented within the TOE as required by [5] Annex 1C, Appendix 11.
O.Software_Update	**Software updates -** Where updates to TOE software are possible, the TOE must accept only those that are authorised.

4.2 Security objectives for the operational environment

The security objectives for the operational environment address the protection that must be provided by the TOE environment, independent of the TOE itself, and are listed in the table below.

Table 8 Security objectives for the TOE Environment

Phase	Short Name	Security objectives for the operational environment
Design phase	OE.Development	**Responsible 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	**Protection during manufacture -** Manufacturers must ensure that the assignment of responsibilities during manufacturing of the TOE is done in a manner that maintains IT security, and that during the manufacturing process the TOE is protected from physical attacks that might compromise IT security.
	OE.Data_Generation	**Data generation -** Security data generation algorithms must be accessible to authorised and trusted persons only.
	OE.Data_Transport	**Handling of security data -** Security data must be generated, transported, and inserted into the TOE in such a way as to preserve its appropriate

		confidentiality and integrity.
	OE.Delivery	**Protection during delivery –** Manufacturers of the TOE, vehicle manufacturers and fitters or workshops must ensure that handling of the TOE is done in a manner that maintains IT security. Fitters and workshops shall particularly be informed of their responsibility related to proper sealing of the mechanical interface.
	OE.Data_Strong	**Strong crypto -** Security data inserted into the TOE must be as cryptographically strong as required by [5] Annex 1C, Appendix 11.
	OE.Test_Points	**Disabled test points -** All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE must be disabled or removed before the end of the manufacturing process.
Installation phase	OE.Approved_Workshops	**Use of approved workshops –** Installation, calibration and repair of the TOE must be carried by trusted and approved fitters or workshops.
	OE.Correct_Pairing	**Correct pairing -** Approved fitters and workshops must correctly pair the TOE with a vehicle unit during the installation phase.
Operational phase	OE.Mechanical	**Protection of interface –** A means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)
	OE.Regular_Inspection	**Regular inspections -** The TOE must be periodically inspected.
	OE.Controls	**Law enforcement checks -** Law enforcement controls must be performed regularly and randomly, and must include security audits.

	OE.Crypto_Admin	**Implementation of cryptography** – All requirements from [5] Annex 1C concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.
	OE.Type_Approved_VU	**Type approved vehicle unit –** The vehicle unit to which the TOE is connected must be type approved.
	OE.EOL	**End of life –** When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric cryptographic keys has to be safeguarded.

5 EXTENDED COMPONENTS DEFINITION

No extended components are defined.

6 SECURITY REQUIREMENTS

This section defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements defines the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [1] of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and changed words are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted by underlined text. Selections filled by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted by underlined text. Assignments filled by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*.

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator.

6.1 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. Section 6.1.1 addresses security functional requirements fort he motion sensor , Section 6.1.2 addresses the communication requirements for 2st generation vehicle units Section 6.1.3 addresses the communication requirements for 1st generation vehicle units to be used with the TOE.

6.1.1 Security functional requirements for the Motion Sensor

6.1.1.1 Class FAU - Security Audit

6.1.1.1.1 FAU_GEN.1 - Security Audit Data Generation

FAU_GEN.1: Security Audit Data Generation

Hierarchical to	: No other components
Dependencies	: FPT_STM.1 Reliable time stamps

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[2];

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

c) [The following events:error in non-volatile memory, error in controller RAM, error in controler instruction, error in communication, error in authentication, [assignment : *none*]].

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

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

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

Application note 2:The occurrence of an auditable event on the motion sensor is flagged to the vehicle unit, which can then request a transfer of the event data for storage in the vehicle unit. The minimum list of events available from the motion sensor is specified in [7]. The vehicle unit itself generates and stores motion sensor related events as defined by [5] 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 vehicle unit adds a date/time stamp to the records.

6.1.1.1.2 FAU_STG.1 - Protected Audit Trail Storage

FAU_STG.1: Protected Audit Trail Storage

Hierarchical to	: No other components
Dependencies	: FAU_GEN.1 Security audit data generation

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] unauthorized modifications to the stored audit records in the audit trail.

[2] Since audit functions on the TOE are always enabled this requirement can be considered satisfied.

6.1.1.1.3 FAU_STG.4 – Prevention of Audit Data Loss

FAU_STG.4: Prevention of Audit Data Loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss
Dependencies : FAU_STG.1 Security audit data generation

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

6.1.1.2 Class FDP - User Data Protection

6.1.1.2.1 FDP_ACC.1: Subset Access Control

FDP_ACC.1: Subset Access Control for Motion Sensor

Hierarchical to : No other components
Dependencies : FDP_ACF.1 Security attribute based access control

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

subjects :

- Vehicle Unit,
- Other devices

objects :

- TOE symmetric keys ,
- 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
- Command, actions, or test points, specific to the testing needs of the manufacturing phase

Operations :

- Read,
- Write
- Modify
- Delete]

6.1.1.2.2 FDP_ACF.1: Security Attribute based Access Control

FDP_ACF.1: Security Attribute based Access Control for Motion Sensor

Hierarchical to : No other components

Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

subjects :

- Vehicle Unit,
- Other devices

objects :

- TOE symmetric keys ,
- 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
- Command, actions, or test points, specific to the testing needs of the manufacturing phase].

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

- The send data and pairing functions of the TOE are only accessible to an authenticated vehicle unit, according to [7];
- Identification data, encrypted K_P, encrypted motion sensor serial number and pairing data from first pairing shall be written once only;
- Secret keys shall not be externally readable;
- The TOE file system and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion;
- 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;
- Unauthenticated inputs from external sources shall not be accepted as executable code ;
- The TSF shall export motion data to the vehicle unit such that the vehicle unit can verify its integrity and authenticity;
- Motion data shall only be processed and derived from the TOE's mechanical input].

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

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

6.1.1.2.3 FDP_ETC.1: Export of User Data without Security Attribute

FDP_ETC.1: Export of User Data without security attribute

Hierarchical to : No other components
Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

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

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

Application note 3: FDP_ETC.1 covers the requirement to send motion data, including audit records, to the VU.

6.1.1.2.4 FDP_ETC.2: Export of User Data with security attribute[3]

FDP_ETC.2: Export of User Data with security attribute

Hierarchical to : No other components
Dependencies : FDP_ACC.1 Subset access control
FDP_IFC.1 Subset information flow control

FDP_ETC.2.1 The TSF shall enforce the [Access Control SFP] 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: [assignment: *none*].

[3] The motion sensor sends data to the vehicle unit accompanied by attributes that serve to authenticate the data.

6.1.1.2.5 FDP_ITC.1: Import of User Data without Security Attribute

FDP_ITC.1: Import of Motion Sensor Data without security attribute

Hierarchical to : No other components
Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

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

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

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

Application note 4: FDP_ITC.1 covers the import of the motion sensor session key from the VU during pairing.

6.1.1.2.6 FDP_SDI.2: Stored Data Integrity Monitoring and Action

FDP_SDI.2: Stored Data Integrity Monitoring and Action

Hierarchical to : No other components
Dependencies : No dependencies

FDP_SDI.2.1 TSF shall monitor user data stored in **the TOE's data memory** containers controlled by the TSF for [assignment: *integrity errors (for data stored in EEPROM and FLASH)]* on all objects, based on the following attributes [assignment: *Data hashing*].

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

6.1.1.3 Class FIA - Identification and Authentication

6.1.1.3.1 FIA_AFL.1: Authentication Failure Handling

FIA_AFL.1: Authentication Failure Handling

Hierarchical to : No other components
Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [assignment*: 1*] unsuccessful authentication attempts occur related to [pairing of a Vehicle Unit].

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

6.1.1.3.2 FIA_ATD.1: User Attribute Definition

FIA_ATD.1: User Attribute Definition

Hierarchical to : No other components
Dependencies : No dependencies

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

- first pairing with a VU;
- last pairing with a VU].

6.1.1.3.3 FIA_UAU.3: Unforgeable Authentication

FIA_UAU.3: Unforgeable Authentication of VU

Hierarchical to : No other components
Dependencies : No dependencies

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

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

Application note 5: "User" in FIA_UAU.3 includes any attacker.

6.1.1.3.4 FIA_UID.2: User Identification before any action

FIA_UID.2: User Identification before any action

Hierarchical to : FIA_UID.1 Timing of identification
Dependencies : No dependencies

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

6.1.1.4 Class FPT - Protection of the TSF

6.1.1.4.1 FPT_FLS.1: Failure with preservation of secure state

FPT_FLS.1: Failure with preservation of secure state

Hierarchical to : No other components
Dependencies : No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state[4] when the following types of failures occur: Reset, Power Supply cut-off, Deviation from the specified values of the power supply , Transaction stopped before completion[5]].

6.1.1.4.2 FPT_PHP.2: Notification of Physical Attack

FPT_PHP.2: Notification of Physical Attack

Hierarchical to : FPT_PHP.1 Passive detection of physical attack
Dependencies : FMT_MOF.1 Management of security functions behaviour

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], the TSF shall monitor the devices and elements and notify [a paired VU] when physical tampering with the TSF's devices or TSF's elements has occurred.

Application note 7: TOE is designed so that it cannot be opened, hence 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).

6.1.1.4.3 FPT_PHP.3: Resistance to Physical Attack (1)

FPT_PHP.3: Resistance to Physical Attack (1)

Hierarchical to : No other components
Dependencies : No dependencies

FPT_PHP.3.1(1) The TSF shall resist [use of magnetic fields to disturb vehicle motion detection] to the [TOE components implementing the TSF] by responding automatically such

[4] A secure state is defined here as one in which all security data is protected.

[5] "Transaction stopped" here means an incomplete request received from the vehicle unit, or the incomplete transmission of a response to the vehicle unit.

that the SFRs are always enforced.

Application note 8: FPT_PHP.3(1) is addressed by immune sensing element.

6.1.1.4.4 FPT_PHP.3: Resistance to Physical Attack (2)

FPT_PHP.3: Resistance to Physical Attack (1)

Hierarchical to : No other components
Dependencies : No dependencies

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

6.1.1.4.5 FPT_TST.1: TSF Testing

FPT_TST.1: TSF Testing

Hierarchical to : No other components
Dependencies : No dependencies

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

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

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

6.1.1.5 Class FRU – Resource Utilization

6.1.1.5.1 FRU_PRS.1: Limited priority of services

FRU_PRS.1: Limited priority of services

Hierarchical to : No other components
Dependencies : No dependencies

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

FRU_PRS.1.1 The TSF shall ensure that each access to [assignment: *none*] shall be mediated on the basis of the subjects assigned priority.

6.1.1.6 Class FTP - Trusted Path/Channel

6.1.1.6.1 FTP_ITC.1: Inter-TSF Trusted Channel

FTP_ITC.1: Inter-TSF Trusted Channel

Hierarchical to : No other components
Dependencies : No dependencies

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

FTP_ITC.1.2 The TSF shall permit another trusted IT product (Vehicle Unit)] to initiate communication via the trusted channel.

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

6.1.2 Security functional requirements for external communication (2nd Generation)

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

6.1.2.1 Class FCS - Cryptographic Support

6.1.2.1.1 FCS_CKM.4 - Cryptographic Key Destruction (1)

FCS_CKM.4: Cryptographic Key Destruction (1)

Hierarchical to : No other components
Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [cryptographic key destruction method described in Table 17] that meets the following: [

- requirements in Table 17,

- 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[6],
- Assignment : [*none*]].

6.1.2.1.2 FCS_COP.1 - Cryptographic Operation (1:AES)

FCS_COP.1: Cryptographic Operation (1:AES)

Hierarchical to : No other components
Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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

6.1.2.2 Class FIA - Identification and Authentication

6.1.2.2.1 FIA_UAU.2: User Authentication before any action (1)

FIA_UAU.2: User Authentication before any action (1)

Hierarchical to : No other components
Dependencies : FIA_UID.1 Timing of identification

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, Chapter 12** before allowing any other TSF-mediated actions on behalf of that user.

Application note 10: In the case of a motion sensor authentication (pairing) can be done only in the presence of a workshop card.

6.1.2.3 Class FPT – Protection of the TSF

6.1.2.3.1 FPT_TDC.1: Inter TSF basic TSF data consistency (1)

FPT_TDC.1: Inter TSF basic TSF data consistency (1)

[6] 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.

Hierarchical to : No other components
Dependencies : No dependencies

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] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

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

6.1.3 Security functional requirements for external communication (1^{nd} Generation)

The security functional requirements in this section are required to support communications specifically with 1^{nd} generation vehicle units.

6.1.3.1 Class FCS - Cryptographic Support

6.1.3.1.1 FCS_CKM.4 - Cryptographic Key Destruction (2)

FCS_CKM.4: Cryptographic Key Destruction (2)

Hierarchical to : No other components
Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [cryptographic key destruction method described in Table 16] that meets the following: [

- requirements in Table 16 ,
- 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[7],
- Assignment : *[none]*].

6.1.3.1.2 FCS_COP.1 - Cryptographic Operation (2:TDES)

FCS_COP.1: Cryptographic Operation (2:TDES)

Hierarchical to : No other components
Dependencies : [FDP_ITC.1 Import of user data without security attributes, or

[7] 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.

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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

6.1.3.2 Class FIA - Identification and Authentication

6.1.3.2.1 FIA_UAU.2: User Authentication before any action (2)

FIA_UAU.2: User Authentication before any action (2)

Hierarchical to	: No other components
Dependencies	: FIA_UID.1 Timing of identification

FIA_UAU.2.1(2) The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Part A, Chapter 3** before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 Class FPT – Protection of the TSF

6.1.3.3.1 FPT_TDC.1: Inter TSF basic TSF data consistency (2)

FPT_TDC.1: Inter TSF basic TSF data consistency (2)

Hierarchical to	: No other components
Dependencies	: No dependencies

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] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

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] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit** .

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.

Table 9 Security Objectives Covarage

	T.Access	T.DEsign	T.Environment	T.Hardware	T.Mechanical	T.Motion_Data	T.Security_Data	T.Software	T.Tests	T.Power_Supply	A.Approved_Workshops	A.Controls	A.Type_Approved	P.Crypto
O.Sensor_Main			X	X	X	X		X		X				
O.Access	X													
O.Audit			X			X	X	X						
O.Authentication	X					X	X	X						
O.Processing			X			X								
O.Reliability			X	X			X	X	X	X				
O.Physical		X	X	X		X	X	X		X				
O.Secure_Communication	X					X	X	X						
O.Crypto_Implement														X
O.Software_Update								X						
OE.Development		X		X				X						
OE.Manufacturing		X		X				X	X					
OE.Data_Generation		X					X							
OE.Data_Transport		X					X							
OE.Delivery		X		X				X						
OE.Data_Strong														X
OE.Test_Points	X	X							X					

OE.Approved_Workshops		X		X			X				X			
OE.Correct_Pairing						X								
OE.Mechanical			X		X									
OE.Regular_Inspection			X	X	X			X		X		X		
OE.Controls			X	X	X					X		X		
OE.Crypto_Admin														X
OE.Type_Approved_VU													X	
OE.EOL							X							

Table 10 Security Objectives Sufficiency

Threat, OSP, Assumption	Objective	Rationale
T.Access	O.Access O.Authentication O.Secure_Communication OE.Test_Points	T.Access is addressed directly by O.Access, which requires the TOE to control access to functions and data. This is supported by O.Authentication, which allows access only to an authenticated vehicle unit. O.Secure_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	O.Physical OE.Development OE.Manufacturing OE.Data_Generation OE.Data_Transport OE.Delivery OE.Approved_Workshops OE.Test_Points	T.Design is addressed by O.Physical, which would allow any unauthorised physical access to the TOE during operation to be detected. OE.Development, OE.Manufacturing, OE.Data_Generation, OE.Data_Transport and OE.Delivery all contribute to the protection of sensitive information about the TOE before it comes into operation. OE.Approved_Workshops ensures that the TOE is correctly installed under controlled

		conditions. OE.Test_Points helps to ensure that no access to modes that may disclose design information are available during operation.
T.Environment	O.Sensor_Main O.Reliability O.Processing O.Physical O.Audit OE.Mechanical OE.Controls and OE.Regular_Inspection	T.Environment is addressed by O.Sensor_Main, which requires that motion data must be available to the VU, by O.Reliability, which requires a reliable service, and by O.Processing, which requires accurate processing of input data. O.Physical addresses the need to resist physical attacks, and OE.Mechanical, OE.Controls and OE.Regular_Inspection help to detect signs of interference with TOE hardware. O.Audit aims to record attempted attacks.
T.Hardware	O.Sensor_Main O.Reliability O.Physical OE.Regular_Inspection OE.Controls OE.Development OE.Manufacturing OE.Delivery OE.Approved_Workshops.	T.Hardware is addressed by O.Sensor_Main, which requires that motion data must be available to the VU, and by O.Reliability, which requires a reliable service. O.Physical addresses the need to resist physical attacks. OE.Regular_Inspection and OE.Controls help to detect signs of interference with TOE hardware. Interference with TOE hardware during development, manufacturing, delivery, installation and repair is addressed by OE.Development, OE.Manufacturing, OE.Delivery and OE.Approved_Workshops.
T.Mechanical	O.Sensor_Main E.Mechanical OE.Regular_Inspection OE.Controls	T.Mechanical is addressed by O.Sensor_Main, which requires that authentic motion data must be available to the VU. OE.Mechanical, OE.Regular_Inspection and OE.Controls help to detect signs of interference with

		TOE hardware and its connection to the vehicle.
T.Motion_Data	O.Sensor_Main O.Processing O.Authentication O.Secure_Communication O.Physical O.Audit OE.Correct_Pairing	T.Motion_Data is addressed by O.Sensor_Main, which requires that motion data must be available to the VU. O.Processing requires that processing of inputs to derive the motion data is accurate. O.Authentication and OE.Correct_Pairing control the ability to connect to the TOE and to retrieve data, helping to protect against unauthorised access and tampering. O.Secure_Communication addresses security of the data transfer, helping to detect any modification or attempt to replay. O.Physical aims to detect physical interference, and O.Audit aims to record attempted attacks.
T.Security_Data	O.Reliability O.Authentication O.Secure_Communication O.Physical O.Audit OE.Data_Generation OE.Data_Transport OE.Approved_Workshops OE.EOL	T.Security_Data is addressed by O.Reliability, which requires a reliable service. O.Authentication and O.Secure_Communication restrict the ability of a connected entity to access this data. OE.Data_Generation, OE.Data_Transport and OE.Approved_Workshops aim to protect the confidentiality and integrity of the security data before the TOE is brought into operational use, or during maintenance. OE.EOL requires that the TOE is disposed of securely when it no longer in service. O.Physical aims to detect physical interference, and O.Audit aims to record attempted attacks.
T.Software	O.Sensor_Main O.Reliablility O.Authentication	T.Software is addressed by O.Sensor_Main, which requires that

	O.Secure_Communication O.Software_Update O.Physical O.Audit OE.Development OE.Manufacturing OE.Delivery OE.Regular_Inspection	motion data must be available to the VU, and by O.Reliablility, which requires a reliable service. O.Authentication, O.Secure_Communication and O.Software_Update aim to prevent unauthorised connections to the TOE that could attempt to modify software during operation. O.Physical deals with attempts to modify the software by means of a physical attack on the TOE, and O.Audit aims to record attempted attacks. OE.Development, OE.Manufacturing and OE.Delivery address the prevention of software modification prior to installation. OE.Regular_Inspection helps to detect signs of interference with TOE software.
T.Tests	O.Reliability OE.Manufacturing OE.Test_Points	T.Tests is addressed by O.Reliability, OE.Manufacturing and OE.Test_Points. If the TOE provides a reliable service as required by O.Reliability, if its security cannot be compromised during the manufacturing process (OE.Manufacturing) and if all test points are disabled, the TOE can neither enter any non-invalidated test mode nor have any back door. Hence, the related threat will be mitigated.
T.Power_Supply	O.Reliability O.Sensor_Main O.Physical OE.Regular_Inspections OE.Controls	T.Power_Supply is addressed through O.Reliability, which requires that the TOE should operate reliably and predictably, and through O.Sensor_Main, which requires a supply of authentic data. O.Physical requires that physical attacks that attempt to modify motion data can be detected. Within the operational environment regular workshop inspections

		(OE.Regular_Inspections) and law enforcement controls (OE.Controls) will help to detect any interference.
A.Approved_Workshops	OE.Approved_Workshops	A.Approved_Workshops is supported by OE.Approved_Workshops, which requires the use of approved workshops for installation, pairing and repair of the TOE.
A.Controls	OE.Controls OE.Regular_Inspections	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	OE.Type_Approved_VU	A.Type_Approved is supported by OE.Type_Approved_VU, which requires that the vehicle unit that is coupled with the TOE is type approved.
P.Crypto	O.Crypto_Implement OE.Data_Strong OE.Crypto_Admin	P.Crypto is supported by O.Crypto_Implement, which calls for the correct cryptographic functions to be implemented in the TOE. OE.Data_Strong calls for correct cryptographic material to be loaded into the TOE before operation, and OE.Crypto_Admin addresses the handling and operation of cryptographic material to be done in accordance with requirements.

7.2 Security Requirements Rationale

7.2.1 Rationale for Security Functional Requirements Dependencies

The following table shows how the dependencies for each SFR are satisfied.

Table 11 Security functional requirements dependencies

SFR	Dependencies	Fulfilled by Security requirements in this ST or justified
FAU_GEN.1	➢ FPT_STM.1	Not fulfilled but justified. Audit records are indicated to the vehicle unit as soon as they are available. The audit records are then transferred to the vehicle unit, which itself generates and stores motion sensor related events as defined by [5] Chapters 3.9, 3.12.8 and 3.12.9 and Appendix 1. Time stamping of these events is based on the vehicle unit internal clock. The requirement for the TOE to provide reliable time stamps is therefore not needed.
FAU_STG.1	➢ FAU_GEN.1	fulfilled by FAU_GEN.1
FAU_STG.4	➢ FAU_STG.1	fulfilled by FAU_STG.1
FDP_ACC.1	➢ FDP_ACF.1	fulfilled by FDP_ACF.1
FDP_ACF.1	➢ FDP_ACC.1	fulfilled by FDP_ACC.1
	➢ FMT_MSA.3	Not fulfilled but justified. The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Manufacturing Phase, and are fixed over the whole life time of the TOE. No management of default values for these security attributes (i.e. SFR FMT_MSA.3)

		is necessary here, either during the fitters and workshops phase, or within the usage phase of the TOE.
FDP_ETC.1	➢ FDP_ACC.1 or FDP_IFC.1	fulfilled by FDP_ACC.1
FDP_ETC.2	➢ FDP_ACC.1 or FDP_IFC.1	fulfilled by FDP_ACC.1
FDP_ITC.1	➢ FDP_ACC.1 or FDP_IFC.1	fulfilled by FDP_IFC.1
	➢ FMT_MSA.3	Not fulfilled but justified. 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.
FDP_SDI.2	No dependencies	-
FIA_AFL.1	➢ FIA_UAU.1	Fulfilled by FIA_UAU.2 (1,2) which is hierchical to UIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_UAU.3	No dependencies	-
FIA_UID.2	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_PHP.2	FMT_MOF.1	Not fulfilled but justified. 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.
FPT_PHP.3 (1,2)	No dependencies	-
FPT_TST.1	No dependencies	-

FRU_PRS.1	No dependencies	-
FTP_ITC.1	No dependencies	-
2nd generation specific		
FCS_CKM.4(1)	➢ [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	fulfilled by FDP_ITC.1
FCS_COP.1(1:AES)	➢ [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	fulfilled by FDP_ITC.1
	➢ FCS_CKM.4	fulfilled by FCS_CKM.4(1)
FIA_UAU.2(1)	➢ FIA_UID.1	Fulfilled by FIA_UID.2 which is hierchical to UIA_UID.1
FPT_TDC.1(1)	No dependencies	-
1nd generation specific		
FCS_CKM.4(2)	➢ [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	fulfilled by FDP_ITC.1
FCS_COP.1(2:TDES)	➢ [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	fulfilled by FDP_ITC.1
	➢ FCS_CKM.4	fulfilled by FCS_CKM.4(2)
FIA_UAU.2(2)	➢ FIA_UID.1	Fulfilled by FIA_UID.2 which is hierchical to UIA_UID.1
FPT_TDC.1(2)	No dependencies	-

7.2.2 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.

Table 12 Security Functional Requirements Covarage

	O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update
FAU_GEN.1			X				X			
FAU_STG.1			X							
FAU_STG.4			X							
FDP_ACC.1		X		X		X				X
FDP_ACF.1		X		X		X				X
FDP_ETC.1	X		X							

FDP_ETC.2	X									
FDP_ITC.1				X				X	X	
FDP_SDI.2	X				X	X				
FIA_AFL.1				X						
FIA_ATD.1				X						
FIA_UAU.3	X	X		X				X		
FIA_UID.2	X	X		X				X		
FPT_FLS.1						X				
FPT_PHP.2	X					X	X			
FPT_PHP.3(1)	X					X	X			
FPT_PHP.3(2)	X					X	X			
FPT_TST.1	X				X	X				
FRU_PRS.1					X	X				
FTP_ITC.1	X							X		
FCS_CKM.4(1)				X				X	X	
FCS_COP.1(1)				X				X	X	
FIA_UAU.2(1)	X	X		X				X		
FPT_TDC.1(1)	X				X	X				
FCS_CKM.4(2)				X				X	X	
FCS_COP.1(2)				X				X	X	
FIA_UAU.2(2)	X	X		X				X		
FPT_TDC.1(2)	X				X	X				

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

Table 13 Security Functional Requirements Suffciency

Objective	SFR	Rationale
O.Sensor_Main	FDP_ETC.1	Addresses the export of motion data in compliance with policy.
	FDP_ETC.2	The motion sensor serial number is exported to support verification of motion data authenticity.
	FDP_SDI.2	Requires the TOE to monitor stored data for integrity errors.

	FIA_UAU.2(1,2) FIA_UAU.3 FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
	FPT_PHP.2	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1,2)	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.
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
	FTP_ITC.1	Requires use of a secure channel for communication with the VU.
	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.
O.Access	FDP_ACC.1 FDP_ACF.1	Defines the access control policy for the TOE.
	FIA_UAU.2(1,2) FIA_UAU.3 FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
O.Audit	FAU_GEN.1	Specifies what must be audited.
	FAU_STG.1	Requires that the audit records are protected against unauthorised deletion while held on the TOE.
	FAU_STG.4	Specifies the actions to be taken when the available storage for audit records on the TOE is full.
	FDP_ETC.1	Requires that recorded audit records are transmitted to the vehicle unit for storage.
O.Authentication	FDP_ACC.1 FDP_ACF.1	Defines policy for protection of TOE identification data.
	FDP_ITC.1	Provides for the import of cryptographic session keys from the VU.
	FIA_ATD.1 FIA_UAU.2(1,2) FIA_UAU.3 FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.

	FIA_AFL.1	Defines the actions to be taken when there is an authentication failure with the VU.

	FCS_CKM.4(1,2)
	FCS_COP.1(1,2)
		Define the required cryptography to be used by the TOE for authentication.

O.Processing	FDP_SDI.2	Requires the TOE to monitor stored data for integrity errors.
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
	FPT_TDC.1(1,2)	Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.
	FRU_PRS.1	Ensuring that access to resources is correctly prioritised assists in ensuring that the TOE processes motion data correctly.
O.Reliability	FDP_ACC.1 FDP_ACF.1	Requires that testing commands, actions and test points are disabled to prevent their use by an attacker.
	FDP_SDI.2	Requires the TOE to monitor stored data for integrity errors.
	FPT_FLS.1	Requires the TOE to preserve a secure state in the event of certain failure events.
	FPT_PHP.2	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1,2)	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.
	FPT_TDC.1(1,2)	Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
	FRU_PRS.1	Ensuring that access to resources is correctly prioritised assists in ensuring that the TOE operates reliably.
O.Physical	FAU_GEN.1	Audit records are stored when attempted physical tampering is detected.

	FPT_PHP.2	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1,2)	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.

O.Secure_Communication	FCS_CKM.4(1,2)
	FCS_COP.1(1,2)
		Define the required cryptography to be used by the TOE for authentication and data protection.

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

O.Crypto_Implement	FCS_CKM.4(1,2)
	FCS_COP.1(1,2)
		These requirements define the required cryptography to be used by the TOE for authentication and data protection.

	FDP_ITC.1	Provides for the import of cryptographic session keys from the VU.
O.Software_Update	FDP_ACC.1 FDP_ACF.1	Require that unauthenticated software is not accepted.

7.2.3 Security Assurance Requirements Rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [5] 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. This decision represents a part of the conscious security policy for the recording equipment required by the regulations, and reflected by the current ST.

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

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

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

Table 14 Augmented assurance components dependencies

SAR	Dependencies required by CC Part 3	Fulfilled by Security assurance requirements in this ST
ATE_DPT.2	➢ ADV_ARC.1	fulfilled
	➢ ADV_TDS.3	fulfilled
	➢ ATE_FUN.1	fulfilled
AVA_VAN.5	➢ ADV_ARC.1	fulfilled
	➢ ADV_TDS.3	fulfilled
	➢ ADV_FSP.4	fulfilled
	➢ ADV_IMP.1	fulfilled
	➢ AGD_OPE.1	fulfilled
	➢ AGD_PRE.1	fulfilled
	➢ ATE_DPT.1	fulfilled

7.2.4 Security Requirement - Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

7.2.4.1 SFRs

The dependency analysis in section 7.2.1 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section 6.1.1.2 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current ST accurately reflects the requirements of Commission Implementing Regulation (EU) 2016/799 [5], Annex 1C, which is assumed to be internally consistent.

7.2.4.2 SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 7.2.3 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

7.2.4.3 SFR - SAR

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met –an opportunity having been shown not to arise in sections Rationale for SFR's Dependencies and Security Assurance Requirements Rationale. Furthermore, as also discussed in section 7.2.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

8 TOE SUMMARY SPECIFICATION

8.1 Security Enforcing Functions

TOE carries out its security related operations with security enforcing functions which defined below sections.

8.1.1 SEF.Identification/Authentication

The motion sensor performs an initial authentication of the VU during the pairing process. Authentication is performed by proofing knowledge of a common secret (K_M(Master key), K_{ID} (derived Master key – identification key)) between the motion sensor and the vehicle unit. During the pairing process a new secret common (Ks (session key)) only to the vehicle unit and the motion sensor that performed the pairing is established. This new secret key is than used as the encryption key in the communication in the operational mode between the two entities and thereby also is used as the mechanism to authenticate and establish the identity of the vehicle unit to the motion sensor. Any data transferred from the motion sensor is thereafter encrypted using this key, so only the authorised vehicle unit is able to decrypt the information, i. e. has access to it. Forging or copying of authentication data is prohibited because they are stored securely in the motion sensor and the vehicle unit and cryptographically protected when they are transferred.

Every request to the motion sensor contains a check with authentication data. This authentication data consists of an encrypted field (with Ks (session key)) that contains a random number and a check sum of this random number. The entity is authenticated only if this data has been formatted correctly. The authentication data consists further of an check value of the previous instruction, which depends on the latched impulse counter and the authentication data of the previous instruction.

Every motion sensor has only one authorised entity (VU) at a given time with a known user attribute (first pairing or last pairing).

The authentication process is based on symmetric encryption. Unsuccessful authentication attempts are handled in the following way:

- the respective entity request isn’t performed;
- an error code for failed entity authentication is generated and stored;
- the vehicle unit is informed about the error.

8.1.2 SEF.Access_Control

Access controls ensure that access to the TOE functions only by those authorised to do so. There is only one authorised entity (VU) of the motion sensor at a given time. Access control is performed on the basis of the commands that the vehicle unit is allowed to submit to the motion sensor. The motion sensor checks if the command code submitted corresponds to a valid command or not and if the entity is authorised or not.

The design of the PMS 101 software prohibits to analyse or debug the motion sensor software in the field. A software upgrade is performed with only the installation of a new motion sensor in the vehicle. After this a new pairing must be done.

8.1.3 SEF.Cryptographic_Support

The TOE uses Triple-DES (with 2 keys) for first generation and AES (128, 192 and 256 bits) for second generation encryption and decryption for imported data from and exported to the the Vehicle Unit. No other cryptographic algorithms are currently implemented within the TOE.

The TOE does not generate keys. The session key used for communication with the vehicle unit is generated by the vehicle unit during pairing and then distributed in a secure and authenticated way to the motion sensor. The TOE uses the key distribution method for session key described in the ISO 16844-3:2004 section 7.4.5 and for pairing key described in the ISO 16844-3:2004 section 7.4.4.

The TOE uses cryptographic key destruction method which is described in Table 16 and Table 17.

8.1.4 SEF.Data_Exchange

TOE protects the data objects (Sensor data, Motion sensor identification data, Motion sensor initial security data) transmitted to the VU or (Motion sensor pairing security data) received from the VU over a trusted channel by using encryption.

This prevents read access to the data objects by unauthorised entities. Checksums as part of the encrypted data items and tests if the value of data items are within their defined ranges are used to detect unauthorised modifications during transmission. This verifies the validity of the information. The originator (vehicle unit) is authenticated by the key (i. e. only the vehicle unit knows the session key).

Evidence of origin is generated by the session key that is used for encryption. Since only two parties (the motion sensor and the vehicle unit that performed the current pairing with the motion sensor) know this session key, either party can authenticate the other by verifying that the correct session key has been used. The motion sensor generates an acknowledgement message for each received command. This acknowledgement message contains an indication of the last received command.

8.1.5 SEF.Audit

The motion sensor generates audit records of the following events; error in non-volatile memory, error in controller RAM, error in controler instruction, error in communication, error in authentication. For audit records at least following informations are used; Date and time of the event, type of event, connected external entity (Vehicle unit) identity, and the outcome of the event.

The motion sensors indicates the presence of an error to the vehicle unit in the next instance of communication. Actually the motion sensor doesn't store audit records. This is done in the vehicle unit. Since there is only one entity at a given time all actions can be automatically related to this entity. There is room for only one audit event within the TOE. The data is transferred upon request of the vehicle unit.

8.1.6 SEF.Integrity_Protection

The sensor, the signal processing, central processing unit including volatile and non-volatile memories of the motion sensor are installed in a box designed which cannot be opened. TOE is a sealed device. Active stored data integrity checks are performed within the TOE for the integrity of stored data in the internal memory.

SEF.Integrity_Protection prevent unauthorized modifications to the stored audit records in the audit trail with the help of motion sensor (TOE) design which is designed to not open after manufacturing.

8.1.7 SEF.Reliability

Self testing of the TOE is performed for the accuracy of the integrity of stored data. TOE self tests are fulfilled during start-up, after reset, and on request (with command No. 70 and 80). Upon detection of an fault during the self test the TOE generates an error.

The motion sensor contains a power supply unit that controls the voltage and smoothness of the power input. The internal memory and processing elements are supplied with either proper energy or are inactive. The TOE is designed in a way that each power cut-off or variation results in a reset which provides a secure state in each instance. The occurrence of a reset is indicated to the vehicle unit. After power reset a synchronisation process between motion sensor and vehicle unit is initiated.

The motion sensor is designed so that it cannot be opened, hence it isdesigned such that physical tampering attempts can be easily detected. There are no software functions to detect hardware sabotage. The motion sensor is sealed so that any attempt to tamper with the motion sensor can be detected visually. TOE also provides a sensing element which is immune to magnetic field.

8.2 Security Enforcing Functions Coverage

Table 15 provides an overview for security enforcing functions coverage also giving an evidence for covarage of the SEFs defined.

Table 15 Security Enforcing Functions Covarage

	FAU_GEN.1	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FDP_ETC.1	FDP_ETC.2	FDP_ITC.1	FDP_SDI.2	FIA_AFL.1	FIA_ATD.1	FIA_UAU.3	FIA_UID.2	FPT_FLS.1	FPT_PHP.2	FPT_PHP.3(1,2)	FPT_TST.1	FRU_PRS.1	FTP_ITC.1	FCS_CKM.4(1,2)	FCS_COP.1(1,2)	FIA_UAU.2(1,2)	FPT_TDC.1(1,2)
SEF.Identification/Authentication										X	X	X	X					X			X	X	
SEF.Access_Control				X	X																		
SEF.Cryptographic_Support								X												X	X		
SEF.Data_Exchange				X	X	X	X												X				X
SEF.Audit	X		X																				
SEF.Integrity_Protection		X							X														
SEF.Reliability														X	X	X	X						

9 GLOSSARY and ACRONYMS

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.
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	Data identifying the motion sensor: name of manufacturer, serial number,

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

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

9.2 Acronyms

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
MAC	Message Authentication Code
MS	Motion Sensor
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES
TOBB	Türkiye Odalar ve Borsalar Birliği
TOE	Target of Evaluation

TSF	TOE Security Functionality
TSP	TOE Security Policy
VU	Vehicle Unit

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 4, September 2012.
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012.
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012.
[4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

Digital Tachograph: Directives and Standards

[5]	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.
[6]	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).
[7]	ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface, 1 November 2004.

11 ANNEX A – KEY & CERTIFICATE TABLES

This annex provides details of the cryptographic keys and certificates required by the Motion Sensor during its lifetime, and to support communication with 1^{st} and 2^{nd} generation devices.

A motion sensor does not contain any plaintext keys except for the (second-generation) session key K_S and the pairing key K_P, as shown in Table 17. Optionally, a motion sensor may also contain the first-generation session key K_S and pairing key K_P shown in Table 16.

Additionally, as explained in section 9.2.1 of [5] Annex 1C, Appendix 11, a motion sensor contains the value of the pairing key K_P encrypted under the motion sensor master key K_M. It also contains the value of its serial number encrypted under the identification key K_{ID}. In fact, because the motion sensor master key and all associated keys are regularly replaced, up to three different encryptions of K_P and the serial number (based on consecutive generations of the K_M and K_{ID}) may be present in a motion sensor. This encrypted data is not included in Table 17.

If a motion sensor contains the first-generation session key K_S and pairing key K_P, it also contains the value of K_P encrypted under the (first-generation) motion sensor master key K_M and the value of its serial number encrypted under the (first-generation) identification key K_{ID}. This encrypted data is not included in Table 16.

In general, a motion sensor will not be able to know when it has reached end of life and thus will not be able to make unavailable its permanently stored keys. Making unavailable the permanently stored keys mentioned in these tables, if feasible, is a matter of organisational policy.

Table 16	First-generation symmetric keys stored or used by a motion sensor
Table 17	Second-generation symmetric keys stored or used by a motion sensor

Table 16 First-generation symmetric keys stored or used by a motion sensor

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and timr	Stored in
K_S	Motion sensor session key[8]	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) vehicle unit.	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).

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

Table 17 Second-generation symmetric keys stored or used by a motion sensor

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and timr	Stored in
K_S	Motion sensor session key[9]	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) vehicle unit.	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 KP, 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

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