DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

Common Criteria Protection Profile

Digital Tachograph – Motion Sensor (MS PP)

Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C)

Version 1.0, 9 May 2017

Foreword

This Protection Profile (PP) has been developed to outline the IT security requirements as defined in the Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council Fehler: Referenz nicht gefunden, Annex 1C, using the Common Criteria (CC) language and format (CC version 3.1 [1], [2], [3], Revision 4). This is to enable developers of motion sensors to create their specific Security Target document according to CC, in order for the products to undergo a CC evaluation and certification process. The CC motion sensor certificate is one pre-requisite to obtain type approval for a motion sensor.

The development of the PP has been sponsored by the Joint Research Centre of the European Commission. The PP has been approved by the governmental IT security certification bodies organised within the Joint Interpretation Working Group (JIWG), which supports the mutual recognition of certificates under the umbrella of the European SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates.)

The PP supports the intent of the European Commission to ensure a common and comparable level of assurance for the technical components of the Digital Tachograph System in Europe. This PP reflects the security requirements of the Regulation [5]. Detail is added to the security requirements, but in the event of any conflict the wording of the Regulation shall prevail. The coverage of the requirements of [5] by the CC Security Requirements defined in the current PP is stated in Annex B of this PP.

Notes and comments to this Protection Profile should be referred to:

European Commission
DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

PP Context

This section is informative and does not form part of the protection profile requirements.
Reference [5] identifies the need for a family of protection profiles covering the major elements of digital tachograph operation:

- Protection Profile for vehicle unit (VU),
- Protection Profile for tachograph card (TC),
- Protection Profile for motion sensor (MS),
- Protection Profile for external GNSS facility (EGF).

This document contains the protection profile for the motion sensor only. As the motion sensor is required to interface with the vehicle unit there is a need for alignment of the security functional requirements between them. For this reason the security functional requirements are presented in a modular manner, such that the consistency within the set of documents can be more easily determined.
The following diagram illustrates the operational environment, and the relationship between the protection profiles.

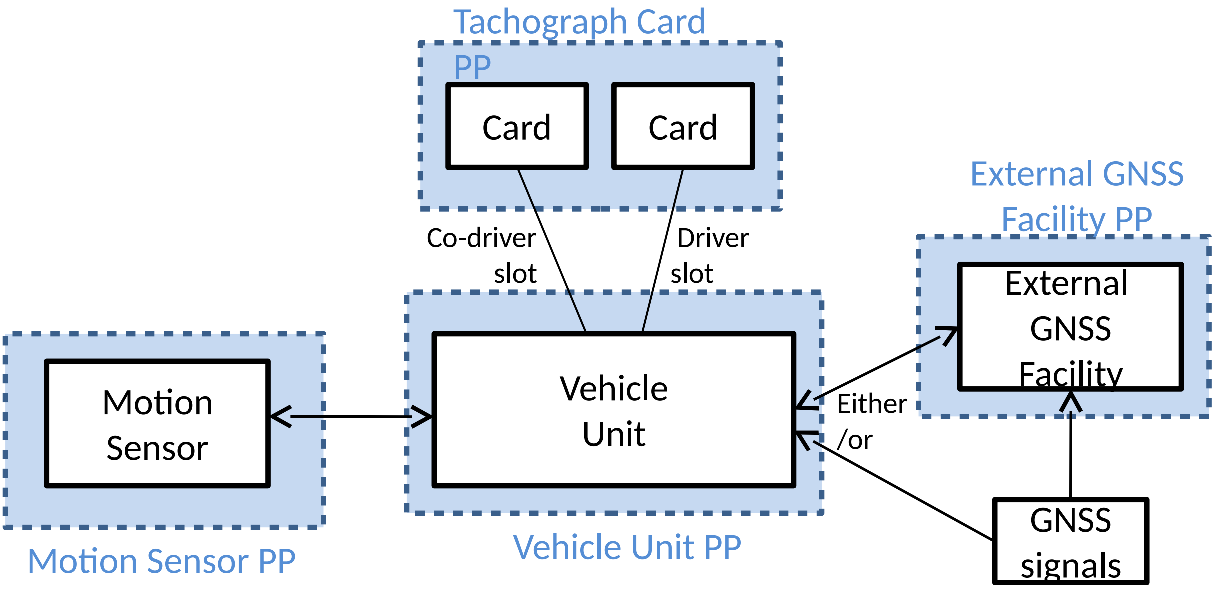

Figure 1: Protection Profile context

The motion sensor monitors the vehicle gearbox and provides signals to the vehicle unit that are representative of vehicle movement and speed. The vehicle unit processes and stores the input data, associates data with users, and provides external connectivity. Tachograph cards identify and authenticate users to the vehicle unit, and provide data storage. A GNSS receiver receives GNSS satellite signals and based on those calculates the vehicle's position and speed, among other quantities. The GNSS receiver can be within the same physical boundary as the vehicle unit. Alternatively, the receiver may have a separate physical boundary in the form of an External GNSS Facility (EGF).
This family of protection profiles addresses the evaluation of second generation digital tachograph components only. However, given the need to allow for a gradual migration from first generation to second generation components, it has been necessary to mandate a level of interoperability with first generation components. This necessitates the support (mandatory or

optional according to situation) for the communication protocols of the earlier generation to be expressed within the new protection profiles. Again, these security functional requirements have been separated for clarity.

Table of Contents

Table of Tables

Table of Figures

Revision history

Version	Date	Changes
1.0	9 May 2017	

1 PP Introduction

1 This section provides document management and overview information being required to register the protection profile and to enable a potential user of the PP to determine, whether the PP is of interest.

2 [5] Annex 1C requirements not included in this protection profile are not the subject of security certification.

3 The general characteristics and functions of the recording equipment, of which the motion sensor is a part are described in [5] Annex 1C, Chapter 3.

1.1 PP Reference

4

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

1.2 TOE overview

1.2.1 TOE definition and operational usage

5 The Target of Evaluation (TOE) addressed by this protection profile 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.

6 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.

7 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. It may also be connected to specific equipment for management purposes, as defined by the manufacturer. Such connections are not addressed by this PP, but they must be defined and shown not to introduce exploitable vulnerabilities.

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

9 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].

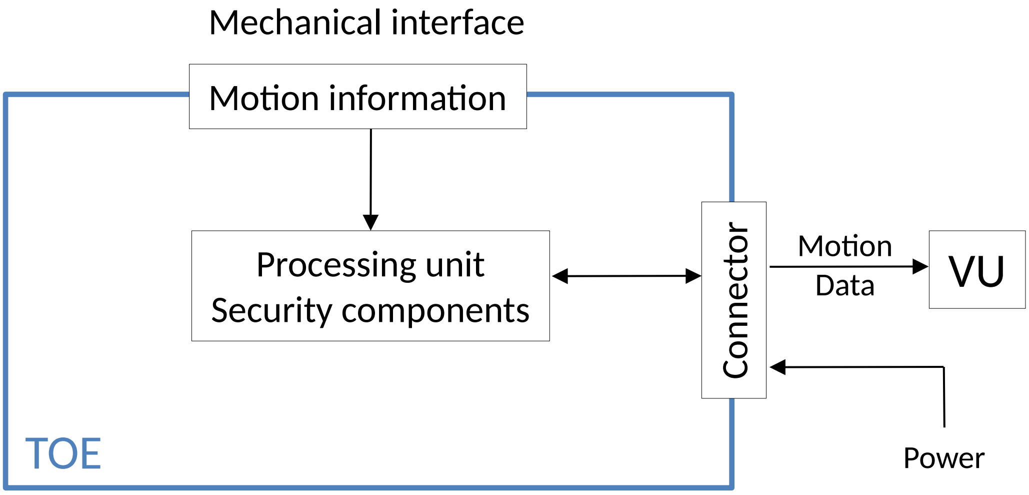

Figure 2 - Motion Sensor

1.2.2 TOE major security features for operational use

10 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.

11 The main security features of the TOE are as follows:

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

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

a) Vehicle Unit identification and authentication;
b) Access control to functions and stored data, according to [7];
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 Vehicle Unit;
g) Cryptographic support for VU to motion sensor mutual authentication and secure messaging according to [5] Annex 1C, Appendix 11.

13 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.

Application note 1: First generation VUs (compliant with [6] Annex 1B) will not have to be replaced following the application of the new [5] Annex 1C. They will continue to be used in the field, until their end of life. Second generation VUs (compliant with [5]) will then be gradually introduced in the field, starting from the introduction date defined in Regulation (EU) 2016/799 [5].

The main differences between the second generation Digital Tachograph System and the first generation are:

- the security mechanisms, which have been changed,
- new functions that have been added (GNSS, short distance communication, optional ITS interface),
- the stored data structure, which has been changed due to the new functions added.

Motion sensors complying with this PP need to be interoperable with second generation VUs. Optionally, the motion sensor may be interoperable with both first and second generation VUs, in which case the appropriate security mechanisms will be used for communication.

1.2.3 TOE type

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

15 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

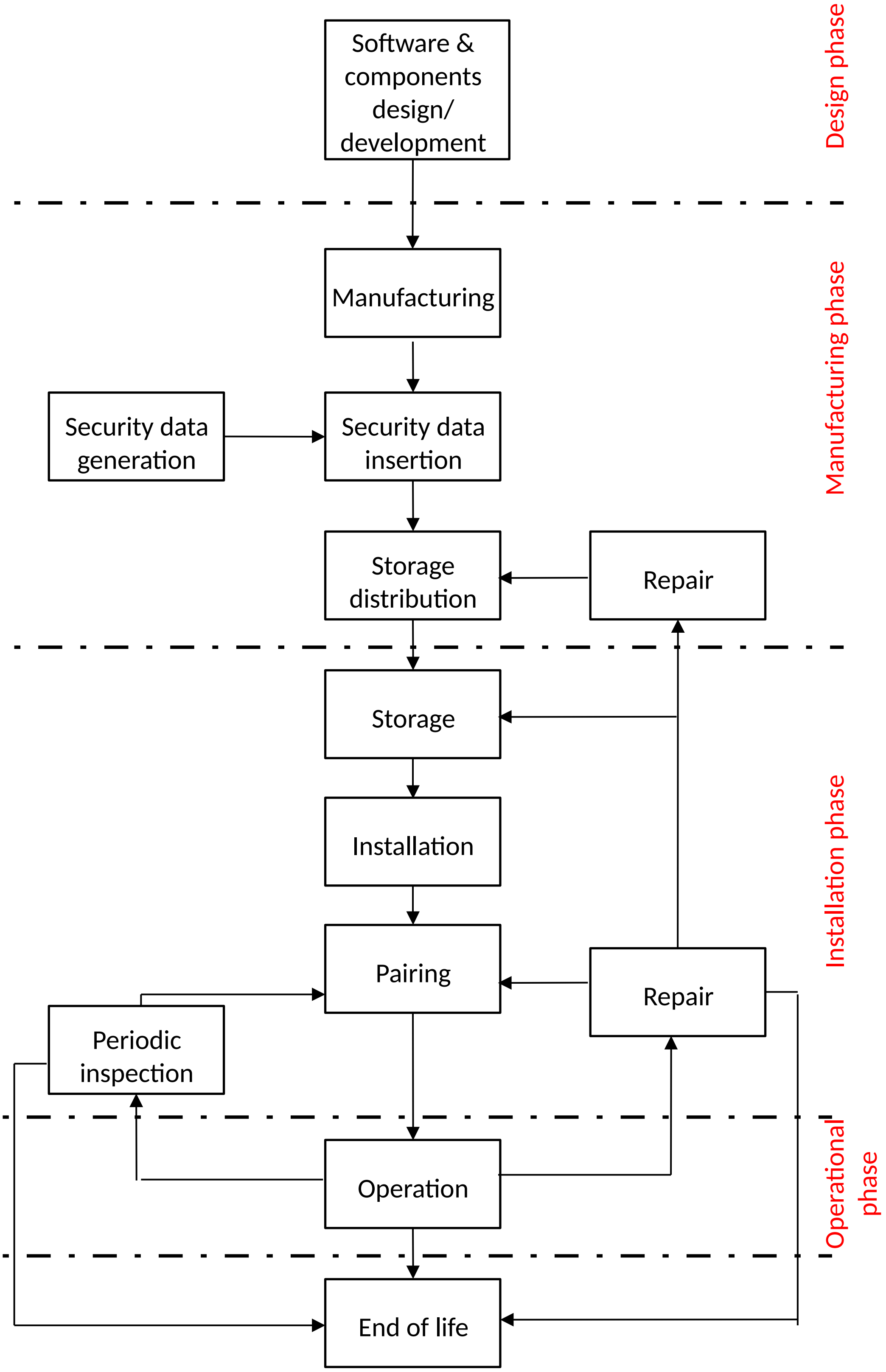

Figure 3 - Motion sensor lifecycle

16 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 (including the development as well as the production of the TOE)
b) TOE delivery
c) TOE operational use

17 For the evaluation of the motion sensor, phases 1 and 2 are part of the TOE development in the sense of the CC. Phase 4 is explicitly in focus of the current PP and is part of the operational use in the sense of the CC. Phase 3 may be part of one of these CC phases, or may be split between them depending on the specific model used by the TOE Manufacturer[1]. The ST author is required to define the exact boundary.

18 As mentioned above, the operational use of the TOE is explicitly the focus of the current PP. Nevertheless, the security target authors have to define the procedure for TOE delivery exactly. TOE delivery could take place before loading of security data is finished. Depending on the TOE delivery procedure, the corresponding guidance for initialisation of data has to be prepared and delivered for evaluation. It is assumed in this PP that all of the initialisation activities will take place in secure environments.

19 The specific production steps for data initialisation are of security relevance, and these have to form part of the CC evaluation under the ALC activities. All production, generation and installation procedures after TOE delivery, up to entering use, have to be considered in the product evaluation process under the AGD assurance activities.

20 The following remarks may show how some CC assurance activities apply to parts of the life-cycle[2]

a) The ALC class, which deals with security measures in the development environment of the TOE, applies to all development and production environments of phases 1 and 2, and to those parts of phase 3 belonging to TOE development, as defined in the ST for a TOE. In particular, the sites where the software of the TOE is developed, as well as the hardware development and production sites, are subject to this CC class (for example with regard to site visits).
b) The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures is covered by AGD_PRE. Since the approved workshop is the first "user" of the TOE after delivery, the guidance documentation is mainly directed to them. They may be defined as the administrator of the TOE, or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:
   - Secure handling of the installation/initialisation of the TOE including security measures needed for the initialisation and secure handling of the initialisation data.

[1] Therefore in the remaining text of this PP the TOE Manufacturer will be the subject responsible for everything up to and including TOE delivery.

[2] These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However, these explicit notes may serve as a help for ST writers and TOE developers to understand the connection between the life-cycle model and some CC requirements.

- Security measures for end-usage, which the installer/initialiser issuer needs to communicate to the end user.

1.2.4 Non-TOE hardware/software/firmware

21 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.

22 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.

2 Conformance Claims

2.1 CC conformance claim

23 This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 4, September 2012 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 4, September 2012 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1, Revision 4, September 2012 [3]

as follows:

Part 2 conformant,

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

2.2 PP claim

24 This protection profile does not claim conformance to any other protection profile.

2.3 Package claim

25 This protection profile claims conformance to the assurance package defined in [5] 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

26 This protection profile does not claim any conformance with other protection profiles. Therefore, no conformance claim rationale is provided here.

2.5 Conformance statement

27 This protection profile requires *strict* conformance of any security target or protection profile claiming conformance to this protection profile.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

28 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.

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

Table 1 – Primary 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.

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

29 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

30 This Protection Profile considers the following subjects, who can interact with the TOE.

No.	Role	Definition
1	Vehicle Unit[3]	Vehicle unit (authenticated), to which the motion

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

No.	Role	Definition
		sensor is paired. The term “user” is also used within this PP 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.[4]
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 PP, especially to change properties of the maintained assets. The attacker is assumed to possess at most a *high* attack potential.

Table 3 - Subjects and external entities

Application note 2: 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

31 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.

32 The threats are defined in the following table.

[4] Manufacturers may make provision for the connection of management devices to a motion sensor. Such connections should be identified in the ST, and elaborated in the design, to demonstrate that this does not introduce exploitable vulnerabilities.

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).

Label	Threat
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).

Table 4 – Threats addressed by the TOE

3.3 Assumptions

33 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.

34 The assumptions are provided in the following table.

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.[5]

Table 5 – Assumptions

3.4 Organisational security policies

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

36 The organisational security policies are provided in the following table.

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.

Table 6 – Organisational security policy

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

4 Security Objectives

37 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

38 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.

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.[6]

Table 7 – Security objectives for the TOE

4.2 Security objectives for the operational environment

39 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.

Specific phase	Short name	Security objective for the 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.

[6] Implementation of a software update facility is optional for developers, but, if implemented the requirements of this PP must be met. Where software update is implemented in the TOE the ST author must add iterations of FCS components to describe the approach employed to protect the authenticity and integrity of the update.

Specific phase	Short name	Security objective for the environment
	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.

Table 8 – Security objectives for the TOE environment

5 Extended Components Definition

40 This protection profile does not use any components defined as extensions to CC Part 2.

6 TOE Security Requirements

41 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.

42 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 PP.

43 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~~.

44 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 to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

45 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 to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicised. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this text is underlined and italicised like *this*.

46 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 for the TOE

47 This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications. This is to facilitate comparison of the communication requirements between this PP and others in the PP family. Section 6.3 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

Hierarchical to: -
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[7];
b) All auditable events for the [not specified] level of audit; and

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

c) [The following events[8]:
   - 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 (optional)
   - vii) Over temperature (optional)
   - viii) Case opening (optional[9])
   - ix) 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, [assignment: *other audit relevant information*].

Application note 3: 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

Hierarchical to: -

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.

6.1.1.1.3 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 Protected audit trail storage

FAU_STG.4.1 The TSF shall [“overwrite the oldest storage record”] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

[8] For the events marked as optional the ST author shall indicate clearly whether they are implemented.

[9] If the TOE casing is designed to be opened then an audit event shall be generated when that is done.

[10] When required data is not available an appropriate default indication shall be given (to be defined by manufacturer).

6.1.1.2 *Class FDP User data protection*

6.1.1.2.1 FDP_ACC.1 Subset access control

Hierarchical to: -

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 device

Objects

- TOE symmetric keys (see Fehler: Referenz nicht gefunden Table 14Fehler: Referenz nicht gefunden and Table 15)
- 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

Operations

Read, write, modify, delete].

6.1.1.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: -

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 device

Objects

- TSF secret keys (seeFehler: Referenz nicht gefunden Table 14Fehler: Referenz nicht gefunden and Table 15)
- Encrypted K_P (with K_M) and encrypted motion sensor serial number (with K_{ID})
- TOE executable code
- TOE file system
- Motion sensor identification data
- Pairing data from first pairing
- Motion data
- Commands, actions, or test points, specific to the testing needs of the manufacturing phase].

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

a) The send data and pairing functions of the TOE are only accessible to an authenticated vehicle unit, 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 vehicle unit such that the vehicle unit can verify its integrity and authenticity;

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

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

6.1.1.2.3 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: -

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 the TOE.

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

Application note 4: 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 attributes[11]

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control

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

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: *additional exportation control rules*].

6.1.1.2.5 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: -

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 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].

Application note 5: 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

Hierarchical to: -

Dependencies: -

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

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

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [assignment: *positive integer number* ***less than 21***] 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 [
a) generate an audit record of the event;

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

6.1.1.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: -

Dependencies: -

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].

6.1.1.3.3 FIA_UAU.3 Unforgeable authentication

Hierarchical to: -

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 6: “User” in FIA_UAU.3 includes any attacker.

6.1.1.3.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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 7: 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

Hierarchical to: -

Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state[12] when the following types of failures occur [

a) Reset;

b) Power supply cut-off;

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

d) Transaction stopped before completion[13]].

6.1.1.4.2 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.

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

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

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 8: 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).

6.1.1.4.3 FPT_PHP.3 Resistance to physical attack (1)

Hierarchical to: -

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 that the SFRs are always enforced.

Application note 9: FPT_PHP.3(1) may be addressed in one of two ways: either a) the sensing element shall be immune or protected from magnetic fields; or b) the TSF shall detect such interference and provide means to the vehicle unit to record a sensor fault.

6.1.1.4.4 FPT_PHP.3 Resistance to physical attack (2)

Hierarchical to: -

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

Hierarchical to: -

Dependencies: -

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

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

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].

Application note 10: The ST author specifies a strategy for running self-tests in the TOE summary specification, and justifies why this is appropriate.

6.1.1.5 Class FRU Resource utilization

6.1.1.5.1 FRU_PRS.1 Limited priority of service

Hierarchical to: -

Dependencies: -

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

FRU_PRS.1.2 The TSF shall ensure that each access to [assignment: *controlled resources*] shall be mediated on the basis of the subjects assigned priority.

Application note 11: The ST author lists the resources that are controlled in the assignment, and describes the basis of mediation in the TOE summary specification.

6.1.1.6 Class FTP Trusted path/channels

6.1.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1 The TSF shall provide a communications 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] 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 vehicle unit].

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

48 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

FCS_CKM.4 Cryptographic key destruction (1)

Hierarchical to: -

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(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*Fehler: Referenz nicht gefunden] that meets the following [

- Requirements in Table 15Fehler: Referenz nicht gefunden;
- 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[14];

- [assignment: *list of standards*]].

6.1.2.1.1 FCS_COP.1 Cryptographic operation (1: AES)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of 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)

Hierarchical to: -

Dependencies: FIA_UID.1 Identification before any action

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

Application note 12: 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)

Hierarchical to: -

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** .

[14] 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.

6.1.3 Security functional requirements for external communications (1st generation)

49 The following requirements shall be met only when the TOE is communicating with 1st generation vehicle units.

6.1.3.1 Class FCS Cryptographic support

6.1.3.1.1 FCS_CKM.4 Cryptographic key destruction (2)

Hierarchical to: -

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(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*Fehler: Referenz nicht gefunden] that meets the following [

- Requirements inFehler: Referenz nicht gefunden Table 14Fehler: Referenz nicht gefunden;
- 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[15];
- [assignment: *list of standards*]].

6.1.3.1.2 FCS_COP.1 Cryptographic operation (2:TDES)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of 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(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 [Triple DES 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)

Hierarchical to: -

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.

[15] 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.

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)

Hierarchical to: -
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**.

6.2 Security assurance requirements for the TOE

50 The assurance level for this protection profile is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [3].

51 These security assurance requirements are derived from [5] Annex 1C, Appendix 10 (SEC_006).

7 Rationale

7.1 Security objectives rationale

52 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.

	T.Access	T.Design	T.Environment	T.Hardware	T.Mechanical	T.Motion_Data	T.Securiy_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						
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

	T.Access	T.Design	T.Environment	T.Hardware	T.Mechanical	T.Motion_Data	T.Securiy_Data	T.Software	T.Tests	T.Power_Supply	A.Approved_Workshops	A.Controls	A.Type_Approved	P.Crypto
OE.Type_Approved_VU													x	
OE.EOL							x							

Table 9 - Security objectives rationale

53 A detailed justification required for suitability of the security objectives to address the security problem definition is given below.

54 **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.

55 **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.

56 **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.

57 **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.

58 **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.

59 **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.

60 **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. O.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.

61 **T.Software** is addressed by O.Sensor_Main, which requires that 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.

62 **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.

63 **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.

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

65 **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.

66 **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.

67 **P.Crypto i**s 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 SFRs' dependencies

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

SFR	Dependencies	Rationale
MS core		
FAU_GEN.1	FPT_STM.1	Not satisfied but justified. *See note 1 below*
FAU_STG.1	FAU_GEN.1	Satisfied by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Satisfied by FAU_STG.1
FDP_ACC.1	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.1 *See note 2 below*
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.1 *See note 3 below*
FDP_SDI.2	-	-
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2(1&2)
FIA_ATD.1	-	-
FIA_UAU.3	-	-
FIA_UID.2	-	-
FPT_FLS.1	-	-
FPT_PHP.2	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	Satisfied by FDP_ITC.1
FCS_COP.1(1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1 and FCS_CKM.4(1)
FIA_UAU.2(1)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(1)	-	-
1st generation specific		

SFR	Dependencies	Rationale
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1
FCS_COP.1(2:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1 and FCS_CKM.4(2)
FIA_UAU.2(2)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(2)	-	-

Table 10 - SFRs' dependencies

Note 1: Audit records are indicated to the vehicle unit as soon as they are available. The audit records are then transferred to the vehicle unit, which itself generates and stores motion sensor related events as defined by [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.

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.

7.2.2 Security functional requirements rationale

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

		O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
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.	Subset access control		x		x		x				x

		O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
1											
FDP_ACF.1	Security attribute based access control		x		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		
FCS_CKM.4	Cryptographic key destruction (1)				x				x	x	
FCS_COP.1	Cryptographic operation (1:AES)				x				x	x	
FIA_UAU.	User authentication	x	x		x				x		

		O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
2	before any action (1)										
FPT_TDC.1	Inter-TSF basic TSF data consistency (1)	x				x	x				
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 11 - Coverage of security objectives for the TOE by SFRs

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

Security 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.

Security Objective	SFR	Rationale
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&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

Security Objective	SFR	Rationale
		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.

Table 12 - Suitability of the SFRs

7.2.3 Security assurance requirements rationale

71 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.

72 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.

73 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

74 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.

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

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

– ATE_DPT.2 and
– AVA_VAN.5.

77 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 13 - SARs' dependencies (additional to EAL4 only)

7.2.4 Security requirements – internal consistency

78 This 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.

a) SFRs

79 The dependency analysis in section 7.2.1 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.

80 All subjects and objects addressed by more than one SFR in sec. 6.1 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 PP accurately reflects the requirements of Commission Implementing Regulation (EU) 2016/799 [5], Annex 1C, which is assumed to be internally consistent.

b) SARs

81 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.

82 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 7.2.1 and 7.2.3. Furthermore, as also discussed in section 7.2.3, 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 Glossary and Acronyms

8.1 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 identification data	Data identifying the motion sensor: name of manufacturer, serial number, approval number, embedded security component identifier and operating

Glossary Term	Definition
	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.

Glossary Term	Definition
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.

8.2 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
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VU	Vehicle Unit

9 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

10 Annex A – Key & Certificate Tables

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

84 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 15. Optionally, a motion sensor may also contain the first-generation session key K_S and pairing key K_P shown in Table 14.

85 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 15.

86 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 14.

87 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 14	Fehler: Referenz nicht gefunden– First-generation symmetric keys stored or used by a motion sensor
Table 15	- Second-generation symmetric keys stored or used by a motion sensor

Key Symbol	Description	*Purpose*	*Type*	Source	Generation Method	Destruction method and time	Stored in
K_S	Motion sensor session key[16]	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 PP	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 PP	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 14 – First-generation symmetric keys stored or used by a motion sensor

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

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and time	Stored in
K_S	Motion sensor session key[17]	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 PP	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 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 PP	Made unavailable when the motion sensor has reached end of life.	Motion sensor non-volatile memory.

Table 15 - Second-generation symmetric keys stored or used by a motion sensor

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