Project:	Sensor 2185 (KITAS 4.0) , Release 1.0
DG-No.:	DG-041017
Status:	released
Filename:	2185R1.HOM.0486.SecurityTarget_Lite.docx
Revision:	Rev. 1.02
Revision Date:	21.11.2018
Designation:	-
Document key:	-

Sensor 2185 (KITAS 4.0)
Security Target Lite

History

Revision	Date	Maturity	Author, Editor	Reason
1.0	19.10.2018	released	Norbert Köhn	Initial Version
1.1	14.11.2018	released	Norbert Köhn	Added major and minor configuration options of the TOE in chapter 1.2.1 and chapter 1.2.2.
1.2	21.11.2018	released	Norbert Köhn	Added product documentation of Sensor 2185.20 (KITAS 4.0) in chapter 1.2.3

Table of content

List of figures

List of tables

1 ST Introduction

This document contains a description of the Sensor 2185 (KITAS 4.0) (the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the security requirements. It states the claimed minimum resistance against attacks of security functional requirements and the required level of assurance for the development and the evaluation.

This document is based on the 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) [9]

The document states the security objectives on the environment and describes how they are implemented in the Sensor 2185 (KITAS 4.0).

Requirements referred to in the document, are those of the body of Annex IC [5]. For clarity of reading, duplication sometimes arises between Annex IC body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex IC body requirement referred by this security target requirement, the Annex IC body requirement shall prevail.

Annex IC body requirements not referred by security targets are not the subject of TSF.

Unique labels have been assigned to threats, objectives, and procedural means and security requirements specifications for the purpose of traceability to development and evaluation documentation.

1.1 ST Reference

Title:	Sensor 2185 (KITAS 4.0) Security Target Lite
Revision:	Rev. 1.02
Author:	Norbert.Koehn@continental-corporation.com, I CVAM TTS VU HM
Publication date:	21.11.2018

1.2 TOE Reference

Developer name:	Continental Automotive GmbH
TOE name:	Sensor 2185 (KITAS 4.0)
TOE version number:	Release 1.0

1.2.1 Major configuration options

The evaluated major configuration option is the Sensor 2185.20 (KITAS 4.0) with an aluminum housing and a plastic connector housing. No other major configurations are in scope of this security target.

1.2.2 Minor configuration options of Sensor 2185.20 (KITAS 4.0)

The minor configuration options of the Sensor 2185.20 (KITAS 4.0) are described in this section. The minor configuration options for Sensor 2185.20 (KITAS 4.0) can be selected by the customer. Once the Sensor 2185.20 (KITAS 4.0) was delivered to the customer the configuration may not be changed. The following table shows all minor configurations:

2185. 20 xx xx x x xx									
Designation	Customer		Length Variant		Divider		Model		Change Index
2185.20 Intelligent pulse sensor with standard plug according to ISO 15170-B1 6.5 – 9V - unleaded	xx	variable	01	L = 18 mm	0	1 : 1	0	no Telma break	00
			02	L = 18.6 mm	1	4 : 1	1	Telma break	
			03	L = 19.8 mm					
			04	L = 23.8 mm					
			05	L = 25.0 mm					
			06	L = 33.8 mm					
			07	L = 62.0 mm					

			08	L = 63.2 mm					
			09	L = 88.8 mm					
			10	L = 113.8 mm					

Table 1-1: Minor configuration options of Sensor 2185.20 (KITAS 4.0)

1.2.3 Product documentation of Sensor 2185.20 (KITAS 4.0)

The product documentation includes a technical description of the Sensor 2185.20 (KITAS 4.0) which is a guidance for approved and certified workshops who carry out installations, checks and inspections of the Sensor 2185.20 (KITAS 4.0) and a guidance for law enforcement controls of the tachograph system which will be performed regularly and randomly, and must include security audits as well as visual inspections of the Sensor 2185.20 (KITAS 4.0).

The actual, certified version of both documents will be referenced in the certification report of this product.

1.3 TOE overview

1.3.1 TOE definition and operational usage

The Target of Evaluation (TOE) addressed by this security target is a second generation Tachograph Motion Sensor in the sense of Annex 1C [5], intended to be used in the smart tachograph system. The smart 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 smart 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. It may also be connected to specific equipment for management purposes, as defined by the manufacturer. Such connections are not addressed by this ST, but they must be defined and shown not to introduce exploitable vulnerabilities.

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

The functional requirements for a Motion Sensor are specified in Annex 1C [5], Chapter 3.2, and the common security mechanisms are specified in Appendix 11 of Annex 1C [5_2]. Aspects of the electrical interface between the motion sensor and vehicle unit are described in ISO 16844-3 [7].

It may also be connected to specific equipment for management diagnostic purposes. In the case of the Sensor 2185 (KITAS 4.0) motion sensor it will only be connected to specific equipment during the manufacturing process to initialise the device. In the field no specific equipment will be connected. Also workshops will not perform any management or repair operations but replace a faulty motion sensor by a new one.

The typical motion sensor is described in the following figure:

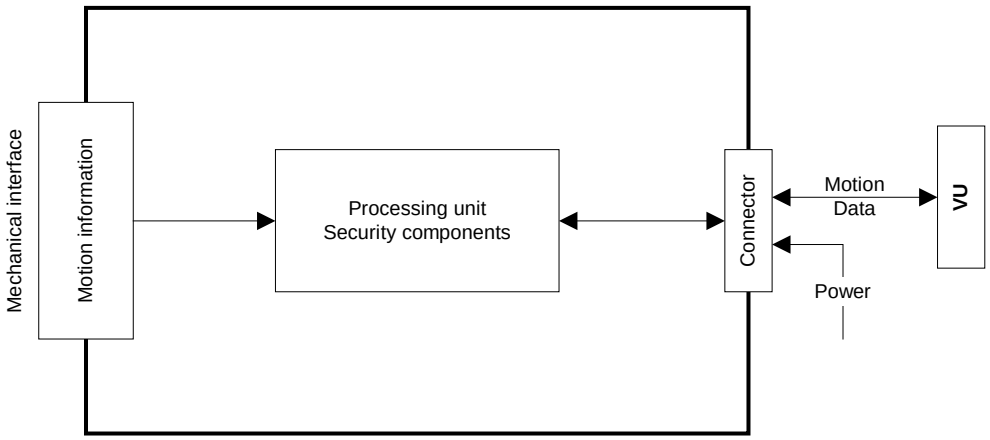

Figure 1-1: Typical motion sensor

1.3.2 TOE major security features for operational use

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:

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.

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_2].

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_2], Parts A and B, respectively.

Motion sensors complying with this ST need to be interoperable with both first and second generation VUs. In both cases the appropriate security mechanisms will be used for communication.

There is a processing unit integrated in the Sensor 2185 (KITAS 4.0) motion sensor. One of the two signalling channels carries the sensor signal (speed, travelled distance) to the DTCO in real time. The other one acts as a bi-directional channel. The distance signal is added to an impulse counter in both the motion sensor and the DTCO.

The value of the impulse counter in the Sensor 2185 (KITAS 4.0) motion sensor is transmitted encrypted on a periodic request of the DTCO. It is decrypted and checked for equality in the DTCO. A deviation is interpreted as manipulation. The DTCO acts as master and controls the integrity/completeness of the plaintext signal – as described in [7].

The housing seal is part of the device. This housing seal ensures that the integrity and authenticity of the Sensor 2185 (KITAS 4.0) is given at installation of the Sensor 2185 (KITAS 4.0) and during the first pairing with a VU.

1.3.3 TOE type

The TOE is a motion sensor in accordance with Annex 1C [5], and Appendix 11 of that document ([5_2]).

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

The life cycle of the Sensor 2185 (KITAS 4.0) motion sensor is described in the following figure:

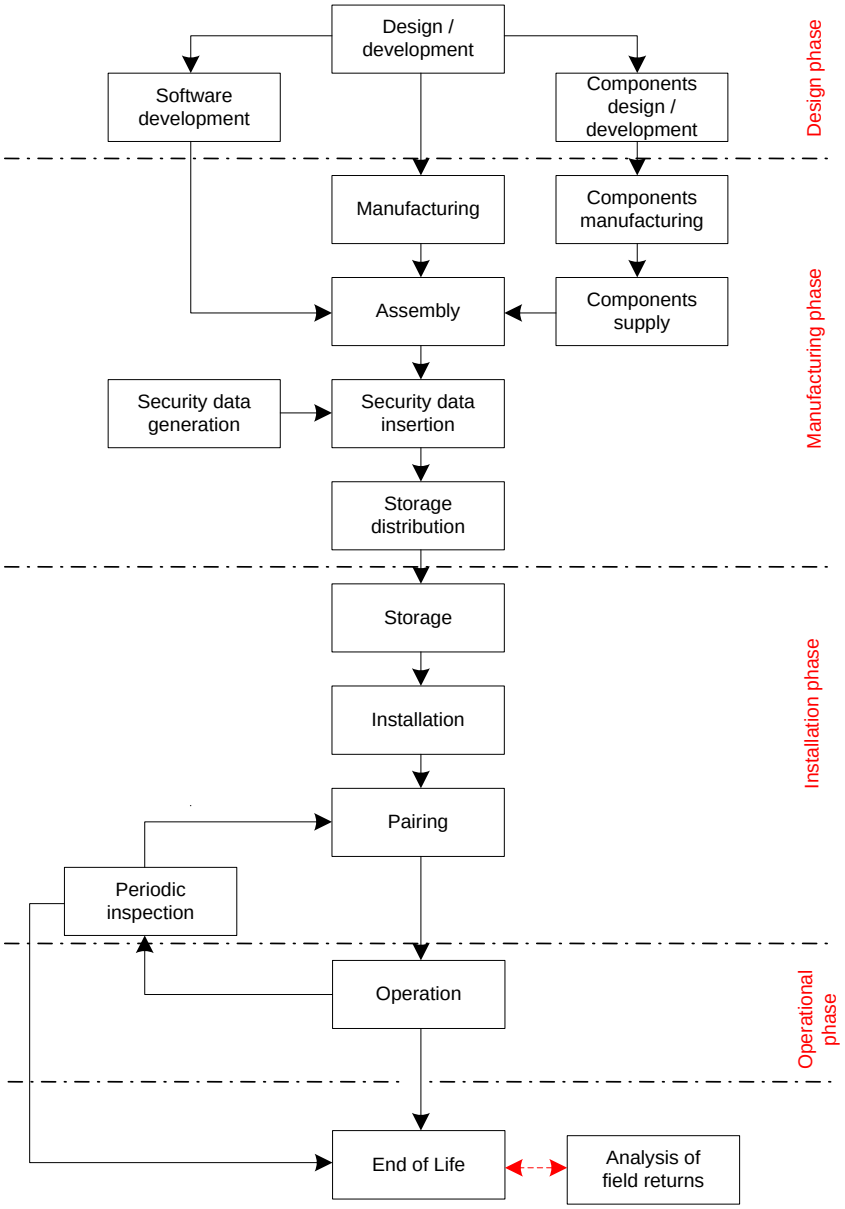

Figure 1-2: Sensor 2185 (KITAS 4.0) motion sensor life cycle

The repair of a Sensor 2185 (KITAS 4.0) motion sensor in the field is not possible. The fitters and workshops are only replacing a faulty Sensor 2185 (KITAS 4.0) by a functional Sensor 2185 (KITAS 4.0). If there is a suspicion of a manipulation at the Sensor 2185 (KITAS 4.0) it will be deeply analysed as field return by the manufacturer.

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

For the Sensor 2185 (KITAS 4.0) , “Design phase” and “Manufacturing phase” are part of the TOE development in the sense of the CC. The “Operational phase” is explicitly in focus of the current ST and is part of the operational use in the sense of the CC. The “Installation phase” is splitted between these CC phases. The “pairing” process and the installation of a mechanical

seal according to EN16882 [13] are belonging to the TOE operational use phase[1] in the sense of the CC. All other processes during the "Installation phase" are belonging to the TOE delivery phase in the sense of the CC. By this it is ensured that

a) All executable software in the TOE is covered by the evaluation;

b) The data structures and the access rights to these data as defined in the Annex 1C [5], in particular the generation, handling and loading of identification data and cryptographic material, are covered by the evaluation.

As mentioned above, the operational use of the TOE is explicitly the focus of the current ST. The TOE delivery takes place after the security data insertion by the TOE Manufacturer[2]. The exact procedure for TOE delivery will be part of the CC evaluation under the ALC activities. Depending on the TOE delivery procedure, the corresponding guidance for initialisation of data will be prepared and delivered for evaluation. All initialisation activities will take place in secure environments.

The specific production steps for data initialisation are of security relevance, and are 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.

The following remarks may show how some CC assurance activities apply to parts of the life-cycle[3]

a) The ALC class, which deals with security measures in the development environment of the TOE, applies to all development and production environments of "Design phase" and "Manufacturing phase", and to those parts of "Installation phase" belonging to TOE development, as defined in this ST. 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.
- Security measures for end-usage, which the installer/initialiser issuer needs to communicate to the end user.

1.3.4 Non-TOE hardware / software / firmware

The TOE is the Sensor 2185 (KITAS 4.0). 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] Since the control of the integrity of the mechanical seal according to EN16882 [13] shall take place in the trustworthy environment of the workshop, the belonging of the installation of the mechanical seal to the operational phase (as part of the pairing) was added by the ST author.

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

[3] 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 the TOE developer to understand the connection between the life-cycle model and some CC requirements.

2 Conformance claims

2.1 CC conformance claim

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2]
- Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [3]

.

as follows

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

2.2 PP conformance claim

This security target claims strict conformance to:

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

2.3 Package claim

This ST is conformant to the following security requirements package:

Standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

2.4 Conformance claim rationale

This security target claims strict conformance to only one PP that is referenced in [9]. The TOE is typical second generation Tachograph Motion Sensor in the sense of Annex 1C [5], intended to be used in the digital tachograph system as defined in PP chapter 1.2.3. Due to the fact that the TOE is not intend to be repairable the lifecycle of the TOE in was adapted accordingly (see Figure 1-3).

Since the security target claimed strict conformance to the PP [9] the security problem definition of this security target is consistent with the statement of the security problem definition in the PP [9].

Conformance Rationale:

- All treats in this security target are identical to the threats in the PP [9] to which conformance is being claimed.
- The assumptions in this security target are identical to the assumptions in the PP [9] to which conformance is being claimed.
- The organisational security policies in this security target are identical to the organisational security policies in the PP [9] to which conformance is being claimed.

Since the security target claimed strict conformance to the PP [9] the security objectives of this security target are consistent with the security objectives in the PP [9].

Conformance Rationale:

- All security objectives for the TOE are identical to the security objectives for the TOE in the PP [9] to which conformance is being claimed.
- All security objectives for the operational environment except OE.Delivery are identical to the security objectives for the operational environment in the PP [9] to which conformance is being claimed.
  OE.Delivery was extended by the ST author regarding the visual inspection of the housing seal before the Sensor 2185 (KITAS 4.0) is installed or paired with the VU.

The following paragraphs are demonstrating that the statement of security requirements in this security target is consistent with the statement of security requirements in the PP [9] for which conformance is being claimed.

All security functional requirements including their refinements defined in the PP [9] are included and completely defined in this security target. Selections having been made by the ST author are underlined and *italicised*. Assignments having been made by the ST author are double underlined and *italicised*.

Due to additional security functionality the following security functional requirements taken from Common Criteria CCMB-2017-04-002, Version 3.1, Revision 5 [2] are additionally included and completely defined in this security target:

- FAU_SAR.1 – Security audit review – for both generation of tachograph system (including the corresponding Application note 6-4)
- FPT_STM.1 – Reliable time stamps – for 2nd generation tachograph system (including its restricting Application note 6-18)

The assurance level for this security target is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 which is identical to the assurance level for the PP [9] to which conformance is being claimed (see also chapter 6.2). The Security assurance requirements rationale in chapter 7.2.3 demonstrates that this security target contains all SARs of the PP [9] and that all dependencies are met or exceeded in the EAL4 assurance package.

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 lifecycle are the application data defined in the tables below.

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

Table 3-1: 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 3-2: Secondary assets to be protected by the TOE and its environment

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 (Roles) and External Entities

The Security Target for the motion sensor Sensor 2185 (KITAS 4.0) considers the following subjects, who can interact with the TOE.

No.	Role	Definition
1	Vehicle Unit[4]	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.[5]
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

[4] The Sensor 2185 (KITAS 4.0) may be paired with 2nd generation vehicle units or 1st generation vehicle units

[5] The Sensor 2185 (KITAS 4.0) does not have any provisions to connect any management devices. Nevertheless with a control device it shall be possible to read the serial number and the audit records of the device.

No.	Role	Definition
		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.

Table 3-3: Subjects and external entities

Application note 3-1: 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.

The threats are defined in the following table. .

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.

Label	Threat
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).

Table 3-4: Threats addressed by the TOE

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.

Assumption	Definition
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[6].

Table 3-5: Assumptions

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.

OSP	Definition
P.Crypto	The cryptographic algorithms and keys described in [5_2] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

Table 3-6: Organisational security policy

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

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.

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_2] 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[7].

Table 4-1: Security Objectives for the TOE

[7] Implementation of a software update facility is optional. The Sensor 2185 (KITAS 4.0) does not implement any possibility to update the software.

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.

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 and checking of the integrity and authenticity of the Sensor 2185 (KITAS 4.0) before the first pairing (i.e. visual inspection of housing seal).
	OE.Data_Strong	**Strong crypto** – Security data inserted into the TOE must be as cryptographically strong as required by [5_2] 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[8].
	OE.Correct_Pairing	**Correct pairing** – Approved fitters and workshops must correctly pair the TOE with a vehicle unit during the installation phase.

[8] This means also that the installation plate contains the correct installation data and is placed in the vehicle in a proper way – i.e. seal number of mechanical seal.

Specific phase	Short name	Security objective for the environment
Operational phase	OE.Mechanical	**Protection of interface** – A means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)[9]
	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_2] 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 4-2: Security objectives for the TOE environment

Application note 4-1: The objective for the TOE environment OE.Delivery was extended compared to OE.Delivery in the Protection Profile [9] by the ST author to add the responsibility of fitters and workshops to do a visual inspection of the Sensor 2185 (KITAS 4.0) before the TOE is installed and the pairing[10] to the VU is performed.

[9] Provisions at the gear box of the vehicle may also needed to meet this objective.

[10] By performing a successful pairing with a VU fitters and workshops can additionally verify that they got delivered the certified Sensor 2185 (KITAS 4.0).

5 Extended Components Definition

This security target does not use any components defined as extensions to CC part 2.

6 TOE Security Requirements

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define 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 having been made by the PP author are denoted as 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*.
- Selections having been made by the ST author are underlined and *italicised*.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password.

- Assignments having been made by the PP author are denoted by showing as 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*. Assignment having been made by the ST author are *double underlined and 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 for the TOE

The security functional requirements (SFRs) below are derived from the Protection Profile [9].

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 ST and others in the PP family. Section 6.1.3 addresses the communication requirements for 1st generation vehicle units to be used with the TOE. Section 6.1.2 addresses the communication requirements for 2nd 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 – Security audit data generation

FAU_GEN.1 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[11];

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

c) The following events:

i. Error in non volatile memory

ii. Error in controller RAM

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

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)

ix. Communication interruption

x. Security breach

xi. Successful pairing

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[12]; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no other audit relevant information*.

Application note 6-1: 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. As the motion sensor itself has no own date/time source, the paired vehicle unit may regularly send the actual date/time to the motion sensor. *If no date/time is provided by the paired vehicle unit, then the motion sensor internal time stamp will be an operating time counter over the whole lifetime of the motion sensor.*

Application note 6-2: The events ix Communication interruption and x Security breach were added by the ST author. The outcome of an event is always “failure” in this application. The subject identity is not applicable in this application.

Application note 6-3: The event “xi Successful pairing” was added by the ST author.

6.1.1.1.2 FAU_SAR – Security audit review

FAU_SAR.1 Audit review

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide all entities at their request with the capability to read all information from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application note 6-4: This SFR is an addition to the security requirements stated in [9] Protection Profile. The reason for this additional requirement is that the TOE is able to store audit records in its own memory. To interpret these information this SFR is needed.

6.1.1.1.3 FAU_STG – Security audit event storage

FAU_STG.1 Protected audit trail storage

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

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

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

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

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 *no other actions* if the audit trail is full.

6.1.1.2 Class FDP: User data protection

6.1.1.2.1 FDP_ACC – Access control policy

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 Table 11-1 and Table 11-2)
- 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 point, specific to the testing needs of the manufacturing phase
- *Pairing data from last pairing*
- *Specific motion sensor internal audit data*

Operations

Read, write, modify, delete.

Application note 6-5: The Protection Profile [9] requires only to enforce the access control SFP on the object “pairing data from the first pairing”. But the Annex 1C [5], Section 3.12.10, (122) requires to store pairing data of the first and of the last pairing. Therefore FDP_ACC.1.1 was adapted according to this requirement.

Application note 6-6: The object “Specific motion sensor internal audit data” was added because the TOE is able to store audit records in its own memory. The access to this data is to be controlled.

6.1.1.2.2 FDP_ACF – Access control functions

FDP_ACF.1 Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation (not relevant, see Application note 7-2)

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

Subjects:

- Vehicle unit
- Other device

Objects

- TOE symmetric keys (see Table 11-1 and Table 11-2)
- 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
- *Pairing data from last pairing*
- *Specific motion sensor internal audit data*

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.

i) Specific motion sensor internal audit data shall be externally readable – but not externally changeable/writeable.

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

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

Application note 6-7: The Protection Profile [9] requires only to enforce the access control SFP on the object "pairing data from the first pairing". But the Annex 1C [5], Section 3.12.10, (122) requires to store pairing data of the first and of the last pairing. Therefore FDP_ACF.1.1 was adapted according to this requirement.

Application note 6-8: The object "Specific motion sensor internal audit data" and the corresponding rules were added because the TOE is able to store audit records in its own memory. The access to this data is to be controlled.

6.1.1.2.3 FDP_ETC – Export from the TOE

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 6-9: FDP_ETC.1 covers the requirement to send motion data, including audit records, to the VU.

FDP_ETC.2 Export of user data with security attributes[13]

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control, or
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*: no additional exportation control rules.*

6.1.1.2.4 FDP_ITC – Import from outside of the TOE

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 (not relevant, see Application note 7-3)

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 6-10: FDP_ITC.1 covers the import of the motion sensor session key from the VU during pairing.

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

6.1.1.2.5 FDP_SDI – Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: -

FDP_SDI.2.1 The TSF shall monitor user data stored in the TOE's data memory containers controlled by the TSF for *integrity errors* on all objects, based on the following attributes: *no 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 – Authentication failures

FIA_AFL.1 Authentication failure handling

Hierarchical to: -

Dependencies: FIA_UAU.1(1), FIA_UAU.1(2) Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *one* 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 – User attribute definition

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 – User authentication

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 6-11: "User" in FIA_UAU.3 includes any attacker.

6.1.1.3.4 FIA_UID – User identification

FIA_UID.2 User authentication 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 6-12: 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 – Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -

Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state[14] 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[15].

6.1.1.4.2 FPT_PHP – TSF physical protection

FPT_PHP.2(1) Notification of physical attack (1:seal)

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

Dependencies: FMT_MOF.1 Management of security functions behaviour (not relevant see Application note 7-4)

FPT_PHP.2.1(1) The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2(1) 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(1) 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.

FPT_PHP.2(2) Notification of physical attack (2:marker)

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

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

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

Dependencies: FMT_MOF.1 Management of security functions behaviour (not relevant see Application note 7-4)

FPT_PHP.2.1(2) The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2(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(2) 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 6-13: 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(1) and FPT_PHP.2.3(2) are not relevant (penetration of the case by other means is addressed by FPT_PHP.2.2(1) and FPT_PHP.2.2(2)).

FPT_PHP.3(1) 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 6-14: 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.

FPT_PHP.3(2) 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.

6.1.1.4.3 FPT_TST – TSF self test

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 6-15: The strategy for running self-tests is specified in the TOE summary specification. A justification why this is appropriate is also done in the TOE summary specification.

6.1.1.5 Class FRU: Resource utilization

6.1.1.5.1 FRU_PRS – Priority of service

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 *processing time of real time pulses* shall be mediated on the basis of the subjects assigned priority.

Application note 6-16: The resources that are controlled are listed with the description of 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 – Inter-TSF trusted channel

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)

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 – Cryptographic key management

FCS_CKM.4(1) 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 *as specified in Table 11-2* that meets the following:

- Requirements in Table 11-2;

- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[16];
- *no further standards*.

6.1.2.1.2 FCS_COP – Cryptographic operation

FCS_COP.1(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(1) Cryptographic key destruction

FCS_COP.1.1(1) 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_2] Annex 1C Appendix 11, Part B.

6.1.2.2 Class FIA: Identification and authentication

6.1.2.2.1 FIA_UAU – User authentication

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

Hierarchical to: FIA_UAU.1(1) Timing of authentication

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_2] Annex 1C Appendix 11, Part B, Chapter 12 before allowing any other TSF-mediated actions on behalf of that user.

Application note 6-17: 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_DTC – Inter-TSF TSF data consistency

FPT_TDC.1(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_2] 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_2] Annex 1C, Appendix 11 Part B when interpreting the TSF data from ~~another trusted IT product~~ a vehicle unit.

6.1.2.3.2 FPT_STM – Time stamps

FPT_STM.1 Reliable time stamps

[16] 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: -

Dependencies: -

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note 6-18: The actual time equivalent is given by the vehicle unit by an additional command, that is based on but actually not included in ISO 16844-3 [7]. By this and an internal timer the actual date and time (reliable time stamp) will be calculated by the TOE. This SFR is an addition to the security requirements stated in [9] Protection Profile and supports only communications specifically with 2nd generation vehicle units. It was added to support the recording of specific motion sensor internal audit data inside the motion sensor.

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

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 – Cryptographic key management

FCS_CKM.4(2) 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 *as specified in Table 11-1* that meets the following:

- Requirements in Table 11-1;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[17];
- *no further standards*.

6.1.3.1.2 FCS_COP – Cryptographic operation

FCS_COP.1(2) 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(2) Cryptographic key destruction

FCS_COP.1.1(2) 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_2] Annex 1C, Appendix 11 Part A, Chapter 3.

6.1.3.1.3 FIA_UAU – User authentication

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

Hierarchical to: FIA_UAU.1(2) Timing of authentication

[17] 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.

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_2] Annex 1C, Appendix 11, Part A, Chapter 3 before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.2 Class FPT: Protection of the TSF

6.1.3.2.1 FPT_DTC – Inter-TSF TSF data consistency

FPT_TDC.1(2) 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_2] Annex 1C, Appendix 11 Part A 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_2] 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

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].

These security assurance requirements are derived from [5_1] Annex 1C, Appendix 10 (SEC_006).

Assurance Class	Assurance Family	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements

Assurance Class	Assurance Family	Description
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability testing

Table 6-1: TOE Security Assurance Requirements

7 Rationale

7.1 Security Objectives Rationale

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

	Treats, Assumptions and OSPs													
	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						

	Treats, Assumptions and OSPs													
	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
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 7-1: Security Objectives Rationale

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

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

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

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

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

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

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 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 SFRs' dependencies

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 for communication with 1st generation vehicle units.

SFR	Dependencies	Rationale
		Satisfied by FPT_STM.1 for communication with 2nd generation vehicle units; See Application note 7-1 below
FAU_SAR.1	FAU_GEN.1	Satisfied by FAU_GEN.1
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 Application note 7-2 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 Application note 7-3 below
FDP_SDI.2	-	-
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2(1) and FIA_UAU.2(2) (hierarchical to FIA_UAU.1(1) and FIA_UAU.1(2))
FIA_ATD.1	-	-
FIA_UAU.3	-	-
FIA_UID.2	-	-
FPT_FLS.1	-	-
FPT_PHP.2(1)	FMT_MOF.1	See Application note 7-4 below
FPT_PHP.2(2)	FMT_MOF.1	See Application note 7-4 below
FPT_PHP.3(1)	-	-
FPT_PHP.3(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)	[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 (hierarchical to FIA_UID.1)

SFR	Dependencies	Rationale
FPT_TDC.1(1)	-	-
FPT_STM.1	-	-
1st generation specific		
FCS_CKM.4(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by FDP_ITC.1
FCS_COP.1(2)	[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 (hierarchical to FIA_UID.1)
FPT_TDC.1(2)	-	-

Table 7-2: SFRs' dependencies

Application note 7-1: 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 for the communication with (1st or 2nd generation vehicle units).
Nevertheless the actual time equivalent shall be given by an additional command from the 2nd generation vehicle unit (Command is based on but actually not included in ISO 16844-3 [7]). By this and an internal timer the actual date and time (reliable time stamp) will be calculated by the TOE. This SFR is an addition to the security requirements stated in [9] Protection Profile and supports only communications specifically with 2nd generation vehicle units. It was added to support the recording of specific motion sensor internal audit data inside the motion sensor.

Application note 7-2: 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.

Application note 7-3: 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.

Application note 7-4: 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

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

		Security objectives for the TOE									
		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	Audit data generation			X				X			
FAU_SAR.1	Audit review			X							
FAU_STG.1	Protected audit trail storage			X							
FAU_STG.4	Prevention of audit data loss			X							
FDP_ACC.1	Subset access control		X		X		X				X
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(1)	Notification of physical attack (1:seal)	X					X	X			

		Security objectives for the TOE									
		O.Sensor_Main	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Physical	O.Secure_Communication	O.Crypto_Implement	O.Software_Update
FPT_PHP.2(2)	Notification of physical attack (2:marker)	X					X	X			
FPT_PHP.3(1)	Resistance to physical attack (1)	X					X	X			
FPT_PHP.3(2)	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(1)	Cryptographic key destruction (1)				X				X	X	
FCS_COP.1(1)	Cryptographic operation (1: AES)				X				X	X	
FIA_UAU.2(1)	User authentication before any action (1)	X	X		X				X		
FPT_TDC.1(1)	Inter-TSF basic TSF data consistency (1)	X				X	X				
FPT_STM.1	Reliable time stamps			X							
FCS_CKM.4(2)	Cryptographic key destruction (2)				X				X	X	
FCS_COP.1(2)	Cryptographic operation (2:TDES)				X				X	X	
FIA_UAU.2(2)	User authentication before any action (2)	X	X		X				X		
FPT_TDC.1(2)	Inter-TSF basic TSF data consistency (2)	X				X	X				

Table 7-3: Coverage of security objectives for the TOE by SFRs

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), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
	FPT_PHP.2(1), FPT_PHP.2(2)	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1), FPT_PHP.3(2)	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.
	FPT_TDC.1(1), FPT_TDC.1(2)	Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.
O.Access	FDP_ACC.1, FDP_ACF.1	Defines the access control policy for the TOE.
	FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
O.Audit	FAU_GEN.1	Specifies what must be audited.
	FAU_SAR.1	Ensures that all audit records can be provided to interpret the information
	FAU_STG.1	Requires that the audit records are protected against 42nauthorized 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.
	FPT_STM.1	Requires that the TSF provide reliable time stamps for TSF functions.

Security Objective	SFR	Rationale
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), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
	FIA_AFL.1	Defines the actions to be taken when there is an authentication failure with the VU.
	FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.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), 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 prioritized 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(1), FPT_PHP.2(2)	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1), FPT_PHP.3(2)	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), FPT_TDC.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
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
	FRU_PRS.1	Ensuring that access to resources is correctly prioritized 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(1), FPT_PHP.2(2)	Requires that attempts at physical tampering are detected, and that, if the case is designed to be opened, an audit record is generated.
	FPT_PHP.3(1), FPT_PHP.3(2)	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), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.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), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2	These requirements are concerned with establishing and maintaining the credentials of the entities using the secure channel.
	FTP_ITC.1	Requires use of a secure channel for communication with the VU.
O.Crypto_Implement	FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.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 7-4: Suitability of the SFRs

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_1] 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 predefined 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 predefined 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 3-3: Subjects, entry 'Attacker'). This decision represents a part of the conscious security policy for the recording equipment required by the regulations, and reflected by the current PP.

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

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

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

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

Table 7-5: SARs' dependencies (additional to EAL4 only)

7.2.4 Security requirements – internal consistency

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

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.

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

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.

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 TOE Summary Specification

The TOE provides the following security services:

8.1 TOE_SS.Integrity_Authenticity

The TOE provides this security service of ensuring integrity and authenticity of the TOE

TOE_SS.Integrity_Authenticity is supported and ensured by cryptographic operations (see TOE_SS.Cryptographic_Support), by limited availability (see TOE_SS.Access) and by audit services (see TOE_SS.Audit).

Security functional requirements concerned:

FDP_ETC.1 -	export of motion data in compliance with policy.
FDP_ETC.2 -	motion sensor serial number is exported to support verification of motion data authenticity
FDP_SDI.2 -	monitor stored data for integrity errors
FPT_PHP.2(1), FPT_PHP.2(2) -	physical tampering attempts are detected. FPT_PHP.2.3(1) and FPT_PHP.2.3(2) are not relevant because the motion sensor is designed so that it cannot be opened.
FPT_PHP.3(1), FPT_PHP.3(2) -	resistance to or reaction to magnetic physical attack that may interfere with motion data supply and resistance to physical attacks designed to access TSF software.
FPT_TST.1 -	Self-tests help to ensure that the TOE is operating correctly.
FPT_TDC.1(1), FPT_TDC.1(2) -	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 prioritized assists in ensuring that the TOE processes motion data correctly.

8.2 TOE_SS.Identification_Authentication

The TOE provides this security service of identification and authentication of the vehicle unit before access to data and functions is allowed.

TOE_SS.Identification_Authentication is supported and ensured by cryptographic operations (see TOE_SS.Cryptographic_Support).

Security functional requirements concerned:

FDP_ACC.1, FDP_ACF.1 -	policy for protection of TOE identification data
FDP_ITC.1 -	the import of cryptographic session keys from the VU.
FIA_ATD.1, FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2 -	establishing and maintaining the credentials of the entities using the secure channel.
FIA_AFL.1 -	Defines the actions to be taken when there is an authentication failure with the VU
FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.1(2) -	Define the required cryptography to be used by the TOE for authentication

8.3 TOE_SS.Accuracy

The TOE provides this security service of accuracy of stored, processed and outputted data.

Security functional requirements concerned:

FDP_ETC.2 -	motion sensor serial number is exported to support verification of motion data authenticity.
FDP_SDI.2 -	monitor stored data for integrity errors.
FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2 -	establishing and maintaining the credentials of the entities using the secure channel.
FPT_PHP.3(1), FPT_PHP.3(2) -	resistance to or reaction to magnetic physical attack that may interfere with motion data supply and 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 -	use of a secure channel for communication with the VU – to ensure that the motion data are not manipulated or changed unintentionally during the transport to the vehicle unit
FPT_TDC.1(1), FPT_TDC.1(2) -	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 prioritized assists in ensuring that the TOE processes motion data correctly.

8.4 TOE_SS.Access

The TOE provides this security service of access control for access to functions and data of the TOE according to the mode of operation selection rules.

TOE_SS.Access is supported and ensured by security service of ensuring integrity and authenticity (see TOE_SS.Integrity_Authenticity).

Security functional requirements concerned:

FDP_ACC.1, FDP_ACF.1 -	Defines the access control policy for the TOE.
FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2 -	establishing and maintaining the credentials of the entities using the secure channel.
FCS_CKM.4(1), FCS_CKM.4(2) -	Defines that the permanently stored motion sensor keys are made unavailable when the motion sensor has reached end of life (see also Table 11-1 and Table 11-2).

8.5 TOE_SS.Audit

The TOE provides this security service of audit service to ensure proper audit data generation. The TOE generates audit records for events impairing its security.

Security functional requirements concerned:

FAU_GEN.1 -	Specifies what must be audited.
FAU_SAR.1 -	Ensures that all audit records can be provided to interpret the information
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 -	Recorded audit records are transmitted to the vehicle unit for storage

FPT_STM.1 -	The TSF provides reliable time stamps for TSF functions (Audit record generation).
FDP_ACC.1, FDP_ACF.1 -	Storing motion sensor's audit records – and access to it

8.6 TOE_SS.Reliability

The TOE provides this security service of reliability of service to ensure proper operation.

TOE_SS.Reliability will be supported by TOE_SS.Audit for the generation and storage of audit records.

Security functional requirements concerned:

FDP_ACC.1, FDP_ACF.1 -	Testing commands, actions and test points are disabled to prevent their use by an attacker.
FDP_SDI.2 -	monitor stored data for integrity errors.
FPT_FLS.1 -	preserve a secure state in the event of certain failure events.
FPT_PHP.2(1), FPT_PHP.2(2) -	physical tampering attempts are detected. FPT_PHP.2.3(1) and FPT_PHP.2.3(2) are not relevant because the motion sensor is designed so that it cannot be opened.
FPT_PHP.3(1), FPT_PHP.3(2) -	resistance to or reaction to magnetic physical attack that may interfere with motion data supply, and resistance to physical attacks designed to access TSF software.
FPT_TDC.1(1), FPT_TDC.1(2) -	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 prioritized assists in ensuring that the TOE operates reliably.
FAU_GEN.1 -	Audit records are generated and stored when unexpected events occur

8.7 TOE_SS.Secured_Data_Exchange

The TOE provides this security service of secured data exchange with the vehicle unit.

Detailed properties of this security service are described in [5_2] Appendix 11 of Annex IC (CSM_216 to CSM_222) for use in a 2nd-generation tachograph system – and in [7] for use in a 1st generation tachograph system.

The TOE is interoperable with both 1st generation vehicle units and 2nd generation vehicle units. This is in compliance with Appendix 15 of [5] Annex 1C (section 2.3).

TOE_SS.Secured_Data_Exchange is supported and ensured by cryptographic operations (see TOE_SS.Cryptographic_Support).

Security functional requirements concerned:

FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.1(2) -	Define the required cryptography to be used by the TOE for authentication, data protection and key destruction.
FDP_ITC.1 -	concerns the import of cryptographic session keys from the VU.
FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.3, FIA_UID.2 -	concerned with establishing and maintaining the credentials of the entities using the secure channel.
FTP_ITC.1 -	use of a secure channel for communication with the VU

8.8 TOE_SS.Cryptographic_Support

The TOE provides this security service of cryptographic support using standard cryptographic algorithms and procedures.

Any cryptographic operation performed by the TOE is in accordance with a specified algorithm and a specified key size described in [5_2] Appendix 11 of Annex IC (CSM_216 to CSM_222) for use a 2nd-generation tachograph system.

Any cryptographic operation performed by the TOE is in accordance with a specified algorithm and a specified key size described in [7] for use a 1st generation tachograph system.

A list of all cryptographic methods that are provided by the Sensor 2185 (KITAS 4.0) at its external interfaces can be found in Annex B – List of used cryptographic methods.

The destruction method and time of the motion sensor keys is in accordance with Table 11-1 and Table 11-2 (column "Destruction method and time") and with [10] NIST Special Publication 800-57.

Security functional requirements concerned:

FCS_CKM.4(1), FCS_CKM.4(2), FCS_COP.1(1), FCS_COP.1(2) - defines the required cryptography to be used by the TOE for authentication, data protection and key destruction.

FDP_ITC.1 - defines the import of cryptographic session keys from the VU.

8.9 TOE_SS.Software_Update

A software update is not supported by the TOE. If a software change is required, a new security certification of the complete TOE is needed. Old motion sensors must be replaced as required.

Security functional requirements concerned:

FDP_ACC.1, FDP_ACF.1 – Require that unauthenticated software is not accepted. No software update is possible on the TOE.

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.
Authenticity	Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer
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.
Digital Tachograph	Recording Equipment
Entity	A device connected to the motion sensor.
Equipment Level	At the equipment level the final master key K_m and the identification key K_{ID} are used for authentication between the vehicle unit and the motion sensor as well as for an encrypted transfer of the motion sensor individual pairing key K_P from the motion sensor to the vehicle unit. The master key K_m, the pairing key K_P and the identification key K_{ID} are used merely during the pairing of a motion sensor with a vehicle unit (see [7] for further details). K_m and K_{ID} are permanently stored neither in the motion sensor nor in the vehicle unit; K_P is permanently stored in the motion sensor and temporarily – in the vehicle unit.
ERCA Policy	The ERCA policy is not a part of the Commission Regulation 1360/2002 [6] and represents an important additional contribution. It was approved by the European Authority. The ERCA policy is available from the web site http://dtc.jrc.it. Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
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.
Housing seal	Until the pairing with a VU housing seals provide the possibility of detection physical tampering of the Sensor 2185 (KITAS 4.0). Housing seals which are part of the motion sensor are conformant to security level 1 of BSI–TL03415 [12].
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.
Mechanical (security) seal	At the end of the installation after the pairing, the workshop installs a mechanical seal according to EN16882 [13]. Mechanical seals provide the possibility of detecting physical tampering with the mechanical interface during the operational phase of the Sensor 2185 (KITAS 4.0).

Glossary Term	Definition
Member State Authority (MSA)	Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA). The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself. MSA is also responsible for inserting data containing $K_{m\text{-}wc}$, $K_{m\text{-}vu}$, motion sensor identification and authentication data encrypted with K_m and K_{ID} into respective equipment (workshop card, vehicle unit and motion sensor). Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
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
Motion Sensor	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.
Motion sensor identification data	Data identifying the motion sensor: name of manufacturer, serial number, approval number, embedded security component identifier and operating system identifier. Motion sensor identification data are part of security data. These are stored in clear in the motion sensor's permanent memory.
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 (like identification data or serial numbers and pairing keys for MS) are stored in and unambiguously, inseparably associated with the related equipment.
Physically separated parts	Physical components of the motion sensor that are distributed in the vehicle as opposed to physical components gathered into the motion sensor casing.
Recording Equipment	The total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers.
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	See Digital Tachograph Smart Tachograph is the definition according the new regulation and their appendixes [5]
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.
Specific motion sensor internal audit data	Data that are not part of definitions in the new regulation and their appendixes [5] and not defined in ISO 16844-3 [7]. These data provide information about the last 20 (re-)parings including information about the used workshop cards.

Glossary Term	Definition
System	Equipment, people or organisations, involved in any way with the recording equipment.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]). In this ST TSF data the term security data is also used.
User	A legitimate user of the TOE, being a paired vehicle unit
User Data	Any data, other than security data, recorded or stored by the motion sensor. User data include motion sensor identification data and motion data. The CC gives the following generic definitions for user data: - Data 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.

Table 9-1: Glossary

9.2 Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard (see FIPS PUB 197)
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)
DTCO	Digital Tachograph or Smart Tachograph
e	encrypted
EAL	Evaluation Assurance Level (a pre-defined package in CC)
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES
EGF	External GNSS Facility
ERCA	European Root Certification Authority
GNSS	Global Navigation Satellite System
K_m	Master key
K_{m_VU}	Part of the Master key stored in the VU, will manage the pairing between a motion sensor and the vehicle unit
K_{m_WC}	Part of the Master key stored in the workshop card, will manage the pairing between a motion sensor and the vehicle unit
K_p	sensor-specific pairing key
K_s	session key
MAC	Message Authentication Code

MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
n.a.	Not applicable
Ns	Extended Serial-Number
OSP	Organisational security policy
PP	Protection profile
ROM	Read Only Memory
SAR	Security assurance requirements
SEF	Security Enforcing Function
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TBD	To Be Defined
TC	Tachograph Card
TDES	Triple Data Encryption Standard (see FIPS PUB 46-3)
TOE	Target Of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy
VU	Vehicle Unit

Table 9-2: Acronyms

10 Bibliography

Common Criteria

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

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

[3] Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

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

[5_1] Appendix 10 of Annex IC of Council Regulation (EEC) No. 165/2014 [5] - Security Requirements

[5_2] Appendix 11 of Annex IC of Council Regulation (EEC) No. 165/2014 [5] - Common security mechanisms

[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, Road vehicles, Tachograph systems, Part 3: Motion sensor interface, First edition, 2004-11-01, Corrigendum 1, 2006-03-01

[8] Joint Interpretation Library. Security Evaluation and Certification of Digital Tachographs. JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1B, Version 1.12, June 2003

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

[10] NIST Special Publication 800-57 – Recommendation for Key Management

[11] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques , National Institute of Standards and Technology, U.S Department of Commerce, 2001

[12] BSI TL-03415, Version 1.4, Juli 2011 – Anforderungen und Prüfbedingungen für Sicherheitsetiketten

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

[14] FIPS PUB 46-3 – Federal Information Processing Standards Publication Data Encryption Standard (DES) Reaffirmed 1999 October 25

[15] FIPS PUB 197 – U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES)

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 1st and 2nd 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 11-2. Optionally, a motion sensor may also contain the first-generation session key K_S and pairing key K_P shown in Table 11-1.

Additionally, as explained in section 9.2.1 of [5_2] 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 11-2.

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 11-1.

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. Therefore, for the purposes of these tables 'end of life' is defined as when circumstances necessitate the decommissioning of a motion sensor. Making unavailable the permanently stored keys mentioned in these tables, if feasible, is a matter of organisational policy.

Table 11-1: First-generation symmetric keys stored or used by a motion sensor

Table 11-2: 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[18]	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 nonvolatile 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 nonvolatile memory (conditional, only if the motion sensor supports pairing to a first-generation VU)

Table 11-1: First-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[19]	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 nonvolatile 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_2] Annex 1C, Appendix 11, section 9.2.1.2) that a motion sensor may contain up to 3 keys K_P, of consecutive generations.	AES	Generated by the motion sensor manufacturer; stored in motion sensor at the end of the manufacturing phase	Out of scope for this ST	Made unavailable when the motion sensor has reached end of life.	Motion sensor nonvolatile memory

Table 11-2: Second-generation symmetric keys stored or used by a motion sensor

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

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

12 Annex B – List of used cryptographic methods

12.1 Annex B.1 - General

This annex lists the cryptographic methods that are provided by the Sensor 2185 (KITAS 4.0) at its external interfaces.

The description of the cryptographic methods is based on the requirements in the application for a German IT security certificate according to the Common Criteria for an IT product by the Federal Office for Information Security (BSI), version CC-Zert-001-V3.0, chapter point 5: Listing of the cryptographic methods (algorithms and communication protocols) offered via the external interfaces.

12.2 Annex B.2 – List of cryptographic methods

Nr.	Use case	Crpyptographic algorithm	Implementing standard	Key length	Application standard	Validity period
1	Secure messaging Digital Tachograph of 1st generation tachograph system ←→ Sensor 2185 (KITAS 4.0) TOE_SS.Identification_Authentication, TOE_SS.Secured_Data_Exchange, TOE_SS.Crypto-graphic_support	Triple-DES in CBC mode	FIPS PUB 46-3 [14], NIST 800-38A [11]	112	ISO 16844-3 [7], sec. 7.6	Valid until ‚End of Life' of Sensor 2185 (KITAS 4.0) and/or. ‚End of Life' of connected Digital Tachograph
2	Authentication of Digital Tachograph of 1st generation tachograph system ←→ Sensor 2185 (KITAS 4.0) TOE_SS.Identification_Authentication, TOE_SS.Secured_Data_Exchange, TOE_SS.Crypto-graphic_support	Triple-DES in CBC mode	FIPS PUB 46-3 [14], NIST 800-38A [11]	112	ISO 16844-3 [7], sec. 7.4; sec. 7.5	Valid until ‚End of Life' of Sensor 2185 (KITAS 4.0) and/or. ‚End of Life' of connected Digital Tachograph
3	Secure messaging Smart Tachograph of 2nd generation tachograph system ←→ Sensor 2185 (KITAS 4.0) TOE_SS.Identification_Authentication, TOE_SS.Secured_Data_Exchange, TOE_SS.Crypto-graphic_support	AES in CBC mode	FIPS PUB 197 [15], NIST 800-38A [11]	128, 192, 256 (depending on cipher suite according [5_2] of connected Digital Tachograph).	ISO 16844-3 [7], sec. 7.6 with adaptions defined in Appendix 11 of Annex IC [5_2]	Valid until ‚End of Life' of Sensor 2185 (KITAS 4.0) and/or. ‚End of Life' of connected Digital Tachograph
4	Authentication of Smart Tachograph of 2nd generation tachograph system ←→ Sensor 2185 (KITAS 4.0) TOE_SS.Identification_Authentication, TOE_SS.Secured_Data_Exchange, TOE_SS.Crypto-graphic_support	AES in CBC mode	FIPS PUB 197 [15], NIST 800-38A [11]	128, 192, 256 (depending on cipher suite according [5_2] of connected Digital Tachograph).	ISO 16844-3 [7], sec. 7.4; sec. 7.5 with adaptions defined in Appendix 11 of Annex IC [5_2]	Valid until ‚End of Life' of Sensor 2185 (KITAS 4.0) and/or. ‚End of Life' of connected Digital Tachograph

Table 12-1: List of cryptographic methods of Sensor 2185 (KITAS 4.0)