DATAKOM DTC-100 v1.1
VEHICLE UNIT
SECURITY TARGET

Document Name:	DATAKOM DTC-100 Vehicle Unit Security Target
Document ID:	DTC-100-ST
Dissemination Level:	Public
Status:	Published
Document Version:	1.2
Version Date:	02.03.2016
Author(s):	Keriman DEMİRAY

DOCUMENT HISTORY

Version	Date	Modification Reason	Modified By	Approved By
0.1	18.09.2013	First draft	Keriman DEMİRAY	Metin HEKİMOĞLU
0.2	20.09.2013	Functional requirements are justified	Keriman DEMİRAY	Metin HEKİMOĞLU
0.3	23.09.2013	TOE Summary Specification has been completed	Keriman DEMİRAY	Metin HEKİMOĞLU
0.4	18.12.2013	Differences between VU PP and Datakom DTC-100 life cycle have been added.	Keriman Demiray	Metin Hekimoğlu
0.5	24.12.2013	Updated according to OR1.	Keriman Demiray	Metin Hekimoğlu
0.6	06.01.2014	SHA1 COP SFR has been added	Keriman Demiray	Metin Hekimoğlu
0.7	25.02.2014	Software upgrade security function has been added	Keriman Demiray	Metin Hekimoğlu
0.8	01.04.2014	GPS functionality is removed from Security Target	Keriman Demiray	Metin Hekimoğlu
0.9	30/10/2014	Software version was upgraded.	Keriman Demiray	Metin Hekimoğlu
1.0	26/01/2016	GR21 requirements were added.	Keriman Demiray	Metin Hekimoğlu
1.1	12/02/2016	Version number was updated on page7	Keriman Demiray	Metin Hekimoğlu
1.2	02/03/2016	ST is sanitized for publication	Keriman Demiray	Metin Hekimoğlu

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. ST Reference

ST Title	DATAKOM DTC-100v1.1 Vehicle Unit Security Target
ST Reference	DTC-100-ST 1.2

1.2. TOE Reference

TOE Identification	DATAKOM DTC-100 v1.1
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 4)
PP Conformance	Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)' (BSI-CC-PP-0057), version 1.0, 13th July 2010
Assurance Level Evaluation	Assurance Level 4 augmented with ATE_DPT.2 and AVA_VAN.5

1.3. TOE Overview

1.3.1. TOE definition and operational usage

The Target of Evaluation (TOE) addressed by the current Security Target is a vehicle unit (VU) in the sense of Annex I B [6] intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards.

The physical scope of the TOE is a device[1] to be installed in a vehicle. The TOE consists of a hardware box (includes a processing unit, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration/downloading connector, facilities for entry of user's inputs, embedded software and of related user manuals. It must be connected to a motion sensor (MS) and to a power supply unit; it can temporarily be connected with other devices used for calibration, data export and diagnostics.

The TOE receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all these user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces.

The basic operational and security functions provided by TOE is listed below.

Monitoring cards insertions and withdrawals: The TOE is able to monitor the card interface devices to detect card insertions and withdrawals. Upon card insertion the TOE detects whether the card inserted is a valid tachograph card and in such a case identify the card type. The TOE is so designed

[1] single or physically distributed device

that the tachograph cards are locked in position on their proper insertion into the card interface devices. The release of tachograph cards may function only when the vehicle is stopped and after the relevant data have been stored on the cards. The release of the card shall require positive action by the user

Speed and distance measurement: This function shall continuously measure and be able to provide the odometer value corresponding to the total distance travelled by the vehicle. This function shall continuously measure and be able to provide the speed of the vehicle.

Time measurement: The time measurement function measures permanently and digitally provide UTC date and time. UTC date and time is used for dating throughout the recording equipment (recordings, printouts, data exchange, display, …). In order to visualise the local time, it is possible to change the offset of the time displayed, in half hour steps.

Monitoring driver activities: This function is permanently and separately monitor the activities of one driver and one co-driver. Driver activity shall be DRIVING, WORK, AVAILABILITY, or BREAK/REST. It is possible for the driver and/or the co-driver to manually select WORK, AVAILABILITY, or BREAK/REST. When the vehicle is moving, DRIVING is selected automatically for the driver and AVAILABILITY is selected automatically for the co-driver. When the vehicle stops, WORK is selected automatically for the driver.

Monitoring driving status: This function is permanently and automatically monitor the driving status. The driving status CREW is selected when two valid driver cards are inserted in the equipment, the driving status SINGLE is selected in any other case.

Drivers manual entries: This function allows for the entry of places where the daily work periods begin and/or end for a driver and/or a co-driver. Places are defined as the country and, in addition where applicable, the region.

Company locks management: This function is allow the management of the locks placed by a company to restrict data access in company mode to itself. Company locks consist in a start date/time (lock-in) and an end date/time (lock-out) associated with the identification of the company as denoted by the company card number (at lock-in). Locks may be turned “in” or “out” in real time only. Locking-out is only possible for the company whose lock is “in” (as identified by the first 13 digits of the company card number), or, locking-out shall be automatic if another company locks in.

Monitoring control activities: This function monitors DISPLAYING, PRINTING, VU and card DOWNLOADING activities carried while in control mode. This function also monitors OVER SPEEDING CONTROL activities while in control mode. An over speeding control is deemed to have happened when, in control mode, the over speeding printout has been sent to the printer or to the display, or when events and faults data have been downloaded from the VU data memory.

Detection of events and/or faults: This function detects "insertion of a non-valid card event", "card conflict event", "time overlap event", "driving without an appropriate card event", "last card session not correctly closed event", "over speeding event", "power supply interruption event", "motion data error event", "security breach event", "card fault event", "recording equipment event".

Built-in and self-tests: The TOE self-detects faults through self-tests and built-in-tests.

Reading from data memory: The TOE is able to read any data stored in its data memory.

Recording and storing in data memory: The TOE is able to store driver and co-driver activity data for 365 calendar days. Times are recorded with a resolution of one minute unless otherwise specified. The odometer values are recorded with a resolution of one kilometre. Speeds are recorded with a resolution of 1 km/h. Data stored into the data memory shall not be affected by an external power supply cut-off of less than twelve months in type approval conditions.

Reading from tachograph cards: The TOE is able to read from tachograph cards, where applicable, the necessary data. In case of a reading error, the recording equipment tries again, three times maximum, the same read command, and then if still unsuccessful, declare the card faulty and non-valid.

Recording and storing in tachograph cards: The TOE updates data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder.

Displaying: This function allows TOE to show default data, data related to warnings, data related to menu access, other data requested by a user.

Printing: The TOE is able to print information from its data memory and/or from tachograph cards in accordance with the six following printouts: driver activities from card daily printout, driver activities from Vehicle Unit daily printout, events and faults from card printout, events and faults from Vehicle Unit printout, technical data printout, over speeding printout.

Warning: The TOE warns the driver when detecting any event and/or fault. Warning of a power supply interruption event may be delayed until the power supply is reconnected.

Data downloading to external media: The TOE is able to download on request data from its data memory or from a driver card to external storage media via the calibration/downloading connector. The TOE updates data stored on the relevant card before starting downloading.

Output data to additional external devices: The TOE is able to output the "current UTC date and time", " speed of the vehicle", " total distance travelled by the vehicle (odometer)", "currently selected driver and co-driver activity", and " information if any tachograph card is currently inserted in the driver slot and in the co-driver slot" data using a CAN bus connection located at the rear panel, to allow their processing by other electronic units installed in the vehicle.

Calibration: This function allows "to automatically pair the motion sensor with the VU", "to digitally adapt the constant of the recording equipment (k) to the characteristic coefficient of the vehicle (w)", "to adjust (without limitation) the current time", "to adjust the current odometer value", " to update motion sensor identification data stored in the data memory" and "to update or confirm other parameters known to the VU: vehicle identification, w, l, tire size and speed limiting device setting if applicable".

Time adjustment: The time adjustment function allows for adjusting the current time in amounts of one minute maximum at intervals of not less than seven days. This function allows for adjusting the current time without limitation, in calibration mode.

Software Upgrade: This function allows update of software running on the processor in secured way. It can only be executed when the VU is in calibration mode and the special programming equipment is utilized.

1.3.2. TOE major security features for operational use

The main security feature of the TOE is as specified in [9][2]. The data to be measured[3] and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

It concretely means that security of the VU aims to protect

a) the data recorded and stored in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,

b) the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,

c) the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and

d) the integrity and authenticity of data downloaded.

The main security feature stated above is provided by the following major security services

a) Identification and authentication of motion sensor und tachograph cards,

b) Access control to functions and stored data,

c) Accountability of users,

d) Audit of events and faults,

e) Object reuse for secret data,

f) Accuracy of recorded and stored data,

g) Reliability of services,

h) Data exchange with motion sensor, tachograph cards and external media (download function).

‘identification and authentication’ as well as ‘data exchange’ require cryptographic support according to [9], sec. 4.9

1.3.3. TOE Type

The TOE type is the Vehicle Unit in the sense of Annex I B [6].

The life cycle of the TOE is described in the following figure:

[2] O.VU_Main

[3] in the sense ‘collected’; the physical data measurement is performed by the motion sensor being not part of the current TOE.

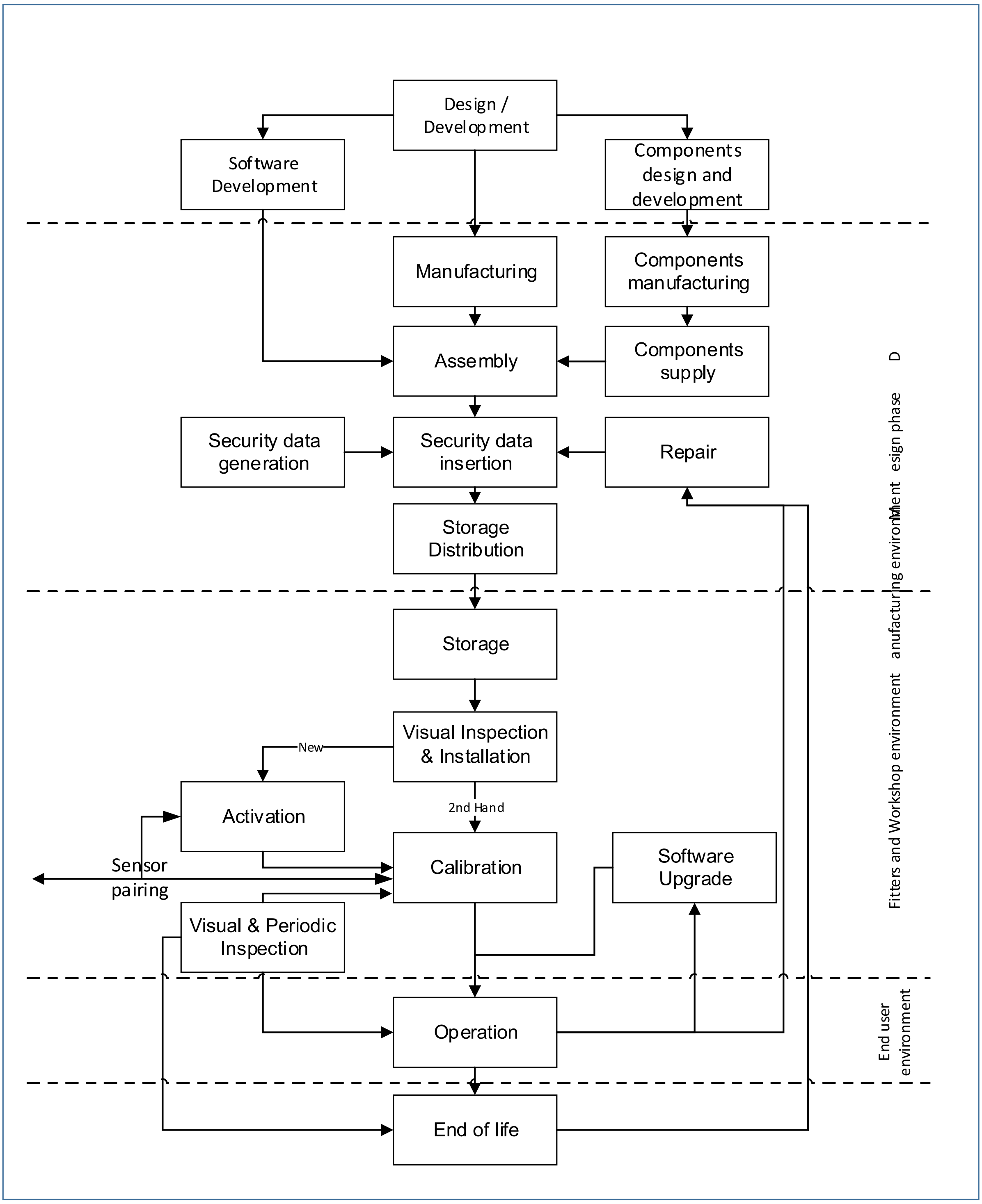

Figure 1 Vehicle Unit life cycle

Although the Protection Profile (Digital Tachograph – Vehicle Unit (VU PP)' (BSI-CC-PP-0057)) expresses that TOE can be repaired in Fitter or Workshop environment, Datakom DTC-100 can be repaired in only manufacturing environment.

1.3.4. Non-TOE hardware/software/firmware

The vehicle unit's operational environment while installed in a vehicle is depicted in the following figure:

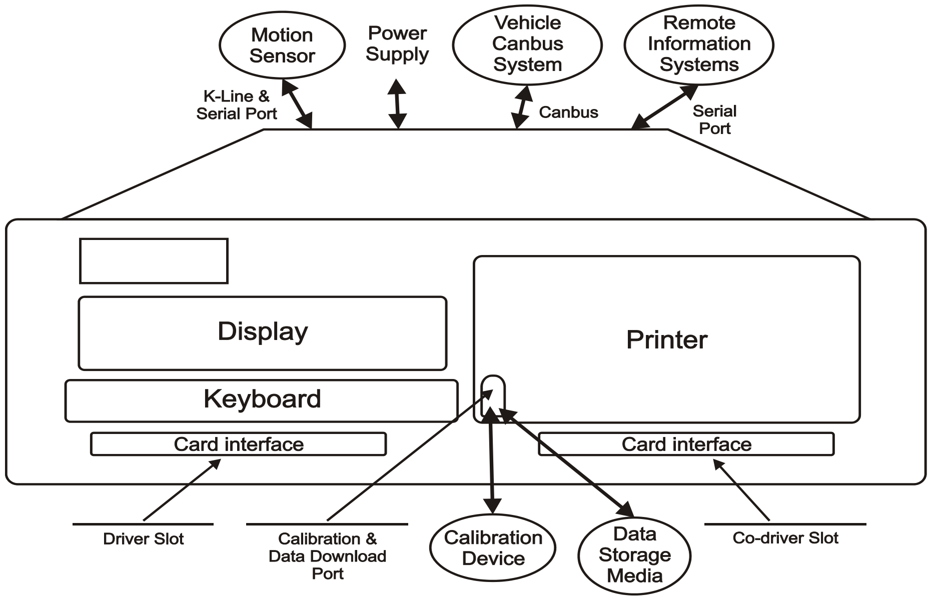

Figure 2 Vehicle Unit operational environment

The following TOE-external components are

a) Mandatory for a proper TOE operation:

- power supply e.g. from the vehicle, where the TOE is installed

- motion sensor;

b) functionally necessary for an Annex I B compliant operation:

- calibration device (fitters and workshops environment only)

- tachograph cards (four different types of them)

- printer paper

- external storage media for data download;

c) helpful for a convenient TOE operation:

- connection to the vehicle network e.g. CAN-connection.

1.4. TOE Description

The target of evaluation (TOE) is the DATAKOM DTC-100 digital tachograph with software version 1.0 as developed by DATAKOM Electronics Engineering Ltd.

1.4.1. Physical Scope of TOE

The target of evaluation (TOE) is the DATAKOM DTC-100 digital tachograph is designed in accordance with Annex 1B of Commission Regulation (EC) on recording equipment in road transport. The following figure shows physical interfaces and internal components of DATAKOM DTC-100.

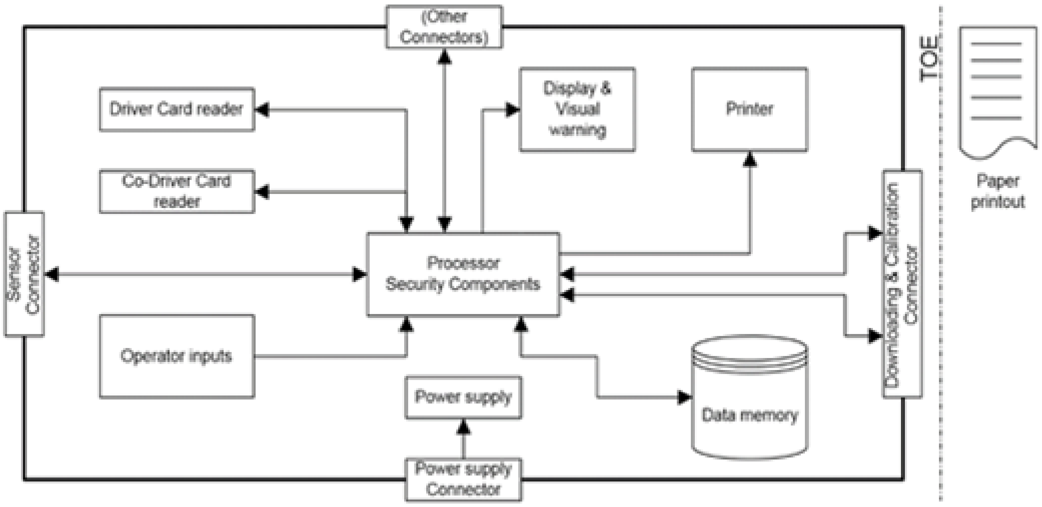

Figure 3Physical interfaces and internal components of TOE

The Hardware components are:

Display: Front display user interface to display necessary information (speed, errors etc.)

Printer: interface to print out reports and necessary information.

Operator interface: interface for user inputs.

Driver Card Reader Tachograph card interfaces.

Downloading&Calibration Connector (C): Interface for downloading VU records, calibration.

Data Memory: Component for storing software, VU records.

Processor Security Components: Controls all interfaces and executes all necessary process for VU.

Power Supply: The power supply module provides proper voltage levels to Vehicle Unit components

Power Supply (C): 12 or 24 Volt power interface.

Other Connectors (C): This is the connectors located at the back panel of the VU. It has an additional CAN BUS and some control signal input/outputs.

Motion Sensor Connector(C): Interface connecting MS that provides speed information to Vehicle Unit

Case Tempering Detection Circuit: Detects case opening while external power supply is connected or not.

1.4.2. TOE Software

TOE software is only one software which is called main software. The main software provides all functionality of necessary for digital tachograph operations (communication with Motion Sensor, recording, reporting etc.), tachograph card communication functions, control of all interfaces.

1.4.3. TOE Security Mechanisms

DATAKOM DTC-100 provides all security mechanisms required in Appendix 11 of Annex I B of Commission Regulation – Common Security Mechanisms.

1.4.4. TOE Environment

1.4.4.1. Development Environment

Necessary physical and logical security measures have been taken in development environment. Development environment is belongs to development company. 24 hours and 7 day physical security guard is deploy at the gate of development building. Research and development department is located at the highest floor of company building and unnecessary employee entrance is forbidden for development environment. Operating system access control mechanisms and configuration management software access control measures are used for logical security measures for the source code of TOE. Confidentiality and Integrity of source code and design documents are protected. Necessary backups are taken periodically for the availability of development results.

1.4.4.2. Manufacturing Environment

Software installation and security key insertion operations are processed in physically secured regions in manufacturing environment. Risk assessment has been made and all necessary physical and logical security measures have been taken. Systems used for software installation and security key insertion is accessible for authorised and trusted persons only.

1.4.4.3. Fitters and workshop environment

The fitters and workshop environment requirements are described in Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)' (BSI-CC-PP-0057), version 1.0, 13th July 2010

1.4.4.4. End user environment

The end user environment requirements are described in Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)' (BSI-CC-PP-0057), version 1.0, 13th July 2010

2. CONFORMANCE CLAIMS

2.1. CC Conformance Claims

This security target claims conformance to

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

as follows

- Part 2 conformant,

- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012,[4] has to be taken into account.

2.2. PP Conformance Claims

This security target claims conformance to the protection profile (PP) BSI-CC-PP-0057 “Protection Profile ‘Digital Tachograph – Vehicle Unit (VU PP)’“ as sponsored by “Bundesamt für Sicherheit in der Informationstechnik“, author Dr. Igor Furgel T-Systems GEI GmbH, SC Security Analysis & Testing, version 1.0 as of 13th July 2010.

2.3. Package Claim

The current ST is conformant to the following security requirements package:

– Assurance package E3hCC31_AP as defined in sec. 6.2 below. This assurance package is commensurate with JIL [11] defining an assurance package called E3hAP. This assurance package declares assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. 2.1) certification (in conjunction with the Digital Tachograph System).

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see sec. 6.2 below).

2.4. Conformance Rationale

Since this security target (ST) claims strict conformance with the protection profile (PP) BSI-CC-PP-0057 referenced in 2.2 “PP Claim”, no rationale is necessary here.

3. SECURITY PROBLEM DEFINITION

3.1. Introduction

Assets

The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap. 8 for the term definitions)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	user data (recorded or stored in the TOE)	Any data, other than security data (sec. III.12.2 of [6]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [6].	Integrity Authenticity

2	user data transferred between the TOE and an external device connected	All user data being transferred from or to the TOE. A TOE communication partner can be: - a motion sensor, - a tachograph card, or - an external medium for data download. Motion data are part of this asset. User data can be received and sent (exchange ↔ {receive, send}).	Confidentiality[4] Integrity Authenticity[5]

Table 1 Primary Assets

All these primary assets represent User Data in the sense of the CC.

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	**Asset**	**Definition**	**Generic security property to be maintained by the current security policy**
3	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
5	TOE immanent secret security data	Secret security elements used by the TOE in order to enforce its security functionality. There are the following security elements of this category: - equipment private key (EQT.SK), see [6], sec. III.12.2, - vehicle unit part of the symmetric master	Confidentiality Integrity

[4] Not each data element being transferred represents a secret. Whose data confidentiality shall be protected while transferring them (i) between the TOE and a MS, is specified in [12], sec. 7.6 (instruction #11); (ii) between the TOE and a tachograph card – in [8], chap. 4 (access condition = PRO SM). Confidentiality of data to be downloaded to an external medium is not required to be protected.

[5] Not each data element being transferred shall be protected for its integrity and authenticity. Whose data integrity and authenticity shall be protected while transferring them (i) between the TOE and a MS, is specified in [12], sec. 7.5 (instruction #80); (ii) between the TOE and a tachograph card – in [8], chap. 4 (access condition = AUT). Integrity and authenticity of data to be downloaded to en external medium shall always be protected.

		key for communication with MS (KmVU), see [10], sec. 3.1.3, - session key between motion sensor and vehicle unit KSm(see [12], sec. 7.4.5 (instruction 42)), - session key between tachograph cards and vehicle unit KSt(see [10], sec. 3.2)	
6	TOE immanent non-secret security data	Non-secret security elements used by the TOE in order to enforce its security functionality. There are the following security elements of this category: - European public key (EUR.PK), - Member State certificate (MS.C), - equipment certificate (EQT.C). see [6], sec. III.12.2.	Integrity Authenticity
7	TOE software components (upgrade package)	Updateable software components of the TOE (inclusive update credentials), such as TOE software and other software components	Confidentiality Authenticity Integrity

Table 2 Secondary Assets

The secondary assets represent TSF and TSF-data in the sense of the CC.

Subjects and external entities

This security target considers the following subjects:

External Entity No.	Subject No.	Role	Definition
1	1	User	Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card. There can also be Unknown User of the TOE and malicious user of the TOE – an attacker. User identity is kept by the VU in form of a concatenation of User group and User ID, cf. [9], UIA_208 representing security attributes of the role 'User'.

			An attacker is a threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. Due to constraints and definitions in [9], an attacker is an attribute of the role 'User' in the context of the current ST. Being a legal user is also an attribute of the role User.
2	2	Unknown User	not authenticated user.
3	4	Motion Sensor	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled. A MS possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are MS serial number encrypted with the identification key(Enc(KID|NS)) together with pairing key encrypted with the master key (Enc(KM|KP))
4	-	Tachograph Card	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: driver card, control card, workshop card, company card. A tachograph card possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK.
5	4	Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable. Valid credentials can be either a certified key pair for authentication of a device or MS serial number encrypted with the identification key (Enc(KID|NS)) together with pairing key encrypted with the master key (Enc(KM|KP)).
6	-	Attacker	see item User above.

Table 3 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 result from the assets protected by the TOE and the method of TOE's use in the operational environment.

The following threats are defined in the current ST (they are derived from [9], sec. 3.3):

Threats averted solely by the TOE:

T.Card_Data_Exchange Users could try to modify user data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).

T.Faults Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.[6]

T.Output_Data Users could try to modify data output (print, display or download)6

Threats averted by the TOE and its operational environment:

T.Access Users could try to access functions6 not allowed to them (e.g. drivers gaining access to calibration function).

T.Calibration_Parameters Users could try to use miscalibrated equipment6 (through calibration data modification, or through organisational weaknesses).

T.Clock Users could try to modify internal clock6.

T.Design Users could try to gain illicit knowledge of design[6] either from manufacturer's material (through theft, bribery …) or from reverse engineering

T.Environment Users could compromise the VU security[6] through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…)

T.Fake_Devices Users could try to connect fake devices (motion sensor, smart cards) to the VU[7]

T.Hardware Users could try to modify VU hardware[6]

T.Identification Users could try to use several identifications or no identification[8]

T.Motion_Data Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal)[9]

[6] The terms 'miscalibrated equipment', 'VU security', 'VU security objectives', 'data output', 'not allowed functions', 'VU in a well-defined state', 'VU design', 'correctness of the internal clock', 'integrity of VU hardware', 'integrity of the VU software', 'full activated security functionality of the VU' correspond with [9] and are covered by the assets 'Accessibility to the TOE functions and data only for authorised subjects' and 'Genuineness of the TOE'

[7] Communication with genuine/known equipment is a prerequisite for a secure data exchange and, hence, represents a partial aspect of the asset 'user data transferred between the TOE and an external device connected'

[8] Identification data are part of the asset 'User data', see Glossary

[9] Motion data transmitted are part of the asset 'user data transferred between the TOE and an external device connected'

T.Power_Supply — Users could try to defeat the VU security objectives[6] by modifying (cutting, reducing, increasing) its power supply

T.Security_Data — Users could try to gain illicit knowledge of security data[10] during security data generation or transport or storage in the equipment.

T.Software — Users could try to modify VU software[6] on the VU.

T.Stored_Data — Users could try to modify stored data (security[11] or user data)

T.Tests — The use of non-invalidated test modes or of existing back doors could compromise the VU security[6]

Threats averted solely by the TOE's operational environment:

T.Non_Activated — Users could use non activated equipment6

3.3. Organizational Security Policies

The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

They are defined here to reflect those security objectives from [9] for which there is no threat directly and fully associated.

OSPs related to the TOE:

OSP.Accountability — The VU must collect accurate accountability data.

OSP.Audit — The VU must audit attempts to undermine system security and should trace them to associated users.

OSP.Processing — The VU must ensure that processing of inputs to derive user data is accurate.

OSP.Test_Points — All commands, actions or test points, specific to the testing

needs of the manufacturing phase of the VU must be disabled

OSPs related to the TOE and its operational environment:

OSP.Type_Approved_MS[12] — The VU shall only be operated together with a motion sensor being type approved according to Annex I B

OSP.Software_Upgrade — In order to fulfill the software requirements RLB_204, RLB_205 of GST in [9], the software upgrade process must be carried out in a secure

[10] 'security data' are covered by the assets 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

[11] it means 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

[12] The identity data of the motion sensor (serial number NS) will be sent to the VU on request by the MS itself (see instruction #40 in [12]). The 'certificate' Enc(KID|NS) stored in the motion sensor is merely used by it for VU authentication, but not for verifying NS by the VU (see instruction #41 in [12]). Therefore, the VU accepts this data (serial number NS) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved

way.

OSPs related to the TOE's operational environment:

OSP.PKI

1) The European Authority shall establish a PKI according to [10], sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of the PKI.
2) The ERCA shall securely generate its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs.
3) The ERCA shall ensure that it issues MSi.C certificates only for the rightful MSCAs.
4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs shall securely generate their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
6) MSCAs shall ensure that they issue EQTj.C certificates only for the rightful equipment.

OSP.MS_Keys

1) The European Authority shall establish a special key infrastructure for management of the motion sensor keys according to [12] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure.
2) The ERCA shall securely generate both parts (K_{mVU} and K_{mWC}) of the master key (K_m).
3) The ERCA shall ensure that it securely convey this key material only to the rightful MSCAs.
4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs shall securely calculate the motion sensor identification key (K_{ID}) and the motion sensor's credentials: MS individual serial number encrypted with the identification key ($Enc(K_{ID}|N_S)$) and MS individual pairing key encrypted with the master key ($Enc(K_M|K_P)$).
6) MSCAs shall ensure that they issue these MS credentials[13], K_{mVU}[14] and K_{mWC}[15] only to the rightful equipment.

[13] to the motion sensors

3.4. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

The GST in [9] does not define any dedicated assumption, but measures; these measures will be reflected in the current ST in form of the security objectives for the TOE environment below. Hence, it is to define some assumptions in the current ST being sensible and necessary from the formal point of view (to reflect those environmental measures from [9])

A.Activation Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.

A.Approved_Workshops The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.

A.Card_Availability Tachograph cards are available to the TOE users and delivered by Member State authorities to authorised persons only.

A.Card_Traceability Card delivery is traceable (white lists, black lists), and black lists are used during security audits.

A.Controls Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).

A.Driver_Card_Uniqueness Drivers possess, at one time, one valid driver card only.

A.Faithful_Calibration Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.

A.Faithful_Drivers Drivers play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …)[16]

A.Regular_Inspections Recording equipment will be periodically inspected and calibrated.

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1. Security Objectives for the TOE

[14] to the vehicle units

[15] to the workshop cards

[16] The assumption A.Faithful_Drivers taken from the Generic Security Target [9] seems not to be realistic and enforceable (from security point of view), because the driver is the person, who has to be controlled and surveyed (see the Commission Regulation [5]). This assumption is made in the current PP only for the sake of compatibility with the GST [9] and is necessary from functional point of view

The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.

They are derived from the security objectives as defined in GST [9], sec. 3.5.

O.Access The TOE must control user access to functions and data.

O.Accountability The TOE must collect accurate accountability data.

O.Audit The TOE must audit attempts to undermine system security and should trace them to associated users.

O.Authentication The TOE should authenticate users and connected entities (when a trusted path needs to be established between entities).

O.Integrity The TOE must maintain stored data integrity.

O.Output The TOE must ensure that data output reflects accurately data measured or stored.

O.Processing The TOE must ensure that processing of inputs to derive user data is accurate.

O.Reliability The TOE must provide a reliable service.

O.Secured_Data_Exchange The TOE must secure data exchanges with the motion sensor and with tachograph cards.

O.Software_Analysis[17] There shall be no way to analyse or debug software[18] in the field after the TOE activation.

O.Software_Upgrade The TOE must guarantee confidentiality, authenticity and integrity of the software packages that will be installed during a software upgrade.

4.2. Security Objectives for the Operational Environment

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment *independent* of the TOE itself.

They are derived from the security objectives as defined in GST [9], sec. 3.6, where they are represented as security measures.

a) Design environment (cf. the life cycle diagram in Figure 1above)

OE.Development VU developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security

b) Manufacturing environment

[17] This objective is added for the sake of a more clear description of the security policy: In the GST [9], this aspect is part of O.Reliability, what might be not self-evident. The special concern here is RLB_204 in [9].

[18] It is a matter of the decision by the certification body and the evaluation facility involved in a concrete certification process on a classification of the TOE (hard- and software) into security relevant and irrelevant parts.

OE.Manufacturing VU manufacturers shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

OE.Sec_Data_Generation Security data generation algorithms shall be accessible to authorised and trusted persons only.

OE.Sec_Data_Transport Security data shall be generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.

OE.Delivery VU manufacturers, vehicle manufacturers and fitters or workshops shall ensure that handling of the TOE is done in a manner which maintains IT security.

OE.Software_Upgrade Software revisions shall be granted security certification before they can be implemented in the TOE. The software update packages must be secured during the generation and transport to the TOE.

OE.Sec_Data_Strong[19] Security data inserted into the TOE shall be as cryptographically strong as required by [10].

OE.Test_Points[20] All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation by the VU manufacturer during the manufacturing process.

c) Workshops environment

OE.Activation Vehicle manufacturers and fitters or workshops shall activate the TOE after its installation before the vehicle leaves the premises where installation took place.

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

OE.Faithful_Calibration Approved fitters and workshops shall enter proper vehicle parameters in recording equipment during calibration.

d) End-user environment

OE.Card_Availability Tachograph cards shall be available to TOE users and delivered by

[19] The security objective OE.Sec_Data_Strong is defined in addition to [9] in order to reflect an aim of establishing the PKI and the symmetric key infrastructure (OSP.PKI and OSP.MS_Keys)

[20] This objective is added for the sake of a more clear description of the security policy: In the GST [9], this aspect is part of O.Reliability, what might be not self-evident: A TOE cannot achieve an objective depending on action of its manufacturer. The special concern here is RLB_201 in [9].

Member State Authorities to authorised persons only.

OE.Card_Traceability — Card delivery shall be traceable (white lists, black lists), and black lists must be used during security audits.

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

OE.Driver_Card_Uniqueness — Drivers shall possess, at one time, one valid driver card only.

OE.Faithful_Drivers[21] — Drivers shall play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …).

OE.Regular_Inspections — Recording equipment shall be periodically inspected and calibrated.

OE.Type_Approved_MS[22] — The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to Annex I B.

4.3. Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its 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.

This rationale covers the rationale part in GST [9], chap. 8 and in Corrigendum [7].

[21] The objective OE.Faithful_Drivers taken from the Generic Security Target [9] seems not to be realistic and enforceable (from security point of view), because the driver is the person, who has to be controlled and surveyed (see the Commission Regulation [5]). This objective is claimed in the current PP only for the sake of compatibility with the GST [9] and is necessary from functional point of view, see also A.Faithful_Drivers.

[22] The identity data of the motion sensor (serial number NS) will be sent to the VU on request by the MS itself (see instruction #40 in [12]). The 'certificate' Enc(KID|NS) stored in the motion sensor is merely used by it for VU authentication, but not for verifying NS by the VU (see instruction #41 in [12]). Therefore, the VU accepts this data (serial number NS) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved (-> UIA_202).

	Threats																		OSPs								Assumptions								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP_Software_Upgrade	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
O.Access	X					X		X		X						X		X																	
O.Accountability		X																	X																
O.Audit	X	X					X			X	X	X		X	X		X	X		X															
O.Authentication	X	X				X		X		X		X											X												
O.Integrity						X												X																	
O.Output					X						X			X			X	X																	
O.Processing						X	X	X	X	X	X					X	X				X														
O.Reliability			X	X	X		X		X	X	X	X			X	X	X	X				X													
O.Secured_Data_Exchange							X			X		X				X																			
O.Software_Analysis					X																														
O.Software_Upgrade																										X									
OE.Development					X												X																		
OE.Software_Upgrade																X	X	X								X									
OE.Delivery													X																						
OE.Manufacturing				X	X																														
OE.Sec_Data_Strong																X								X	X										
OE.Sec_Data_Generation																X								X	X										
OE.Sec_Data_Transport																X								X	X										
OE.Test_Points																						X													
OE.Activation	X												X														X						X		
OE.Approved_Workshops						X		X					X															X							
OE.Card_Availability		X																											X						
OE.Card_Traceability		X																												X					
OE.Controls						X		X	X	X	X		X		X	X	X	X													X				
OE.Driver_Card_Uniqueness		X																														X			
OE.Faithful_Calibration						X		X																									X		
OE.Faithful_Drivers																																		X	
OE.Management_Device																	X																		
OE.Regular_Inspections						X		X		X	X	X	X		X		X																		X
OE.Type_ Approved_ MS										X		X											X												

Table 4 Security Objective Rationale

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

T.Access is addressed by O.Authentication to ensure the identification of the user, O.Access to control access of the user to functions and O.Audit to trace attempts of unauthorised accesses. OE.Activation: The activation of the TOE after its installation ensures access of the user to functions.

T.Identification is addressed by O.Authentication to ensure the identification of the user, O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address this threat by storing all activity carried (even without an identification) with the VU. The OE.Driver_Card_Uniqueness, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.

T.Faults is addressed by O.Reliability for fault tolerance. Indeed, if the TOE provides a reliable service as required by O.Reliability, the TOE cannot experience uncontrollable internal states. Hence, also each possible fault of the TOE will be controllable, i.e. the TOE will be in a wellknown state at any time. Therefore, threats grounding in faults of the TOE will be eliminated.

T.Tests is addressed by O.Reliability and OE.Manufacturing. Indeed, if the TOE provides a reliable service as required by O.Reliability and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the TOE can neither enter any invalidated test mode nor have any back door. Hence, the related threat will be eliminated.

T.Design is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Software_Analysis to prevent reverse engineering and by O.Output (RLB_206) to ensure that data output reflects accurately data measured or store and O.Reliability (RLB_201, 204, 206).

T.Calibration_Parameters is addressed by O.Access to ensure that the calibration function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive calibration data is accurate, by O.Integrity to maintain the integrity of calibration parameters stored. Workshops are approved by Member States authorities and are therefore trusted to calibrate properly the equipment (OE.Approved_Workshops, OE.Faithful_Calibration). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the VU, which helps addressing the threat.

T.Card_Data_Exchange is addressed by O.Secured_Data_Exchange. O.Audit contributes to address the threat by recording events related to card data exchange integrity or authenticity errors. O.Reliability (ACR_201, 201a), O.Processing (ACR_201a).

T.Clock is addressed by O.Access to ensure that the full time adjustment function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive time adjustment data is accurate. Workshops are approved by Member States authorities and are therefore trusted to properly set the clock (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Faithful_Calibration), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.

T.Environment: is addressed by O.Processing to ensure that processing of inputs to derive user data is accurate and by O.Reliability to ensure that physical attacks are countered. OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.

T.Fake_Devices is addressed by O.Access (ACC_205) O.Authentication (UIA_201 – 205, 207 – 211, 213, UIA_221 – 223), O.Audit (UIA_206, 214, 220), O.Processing (ACR_201a), O.Reliability (ACR_201, 201a), O.Secured_Data_Exchange (CSP_201 - 205). OE.Type_Approved_MS ensures that only motion sensors with correct identification data have the credentials that are required to successfully authenticate themselves. OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the whole installation.

T.Hardware is mostly addressed in the user environment by O.Reliability, O.Output, O.Processing and by O.Audit contributes to address the threat by recording events related to hardware manipulation. The OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the installation.

T.Motion_Data is addressed by O.Authentication, O.Reliability (UIA_206, ACR_201, 201a), O.Secured_Data_Exchange and OE.Regular_Inspections, OE.Type_Approved_MS. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

T.Non_Activated is addressed by the OE.Activation and OE.Delivery. Workshops are approved by Member States authorities and are therefore trusted to activate properly the equipment (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Controls), also contribute to address the threat.

T.Output_Data is addressed by O.Output. O.Audit contributes to address the threat by recording events related to data display, print and download.

T.Power_Supply is mainly addressed by O.Reliability to ensure appropriate behaviour of the VU against the attack. O.Audit contributes to address the threat by keeping records of attempts to tamper with power supply. OE.Controls includes controls by law enforcement officers of power supply interruption records held in the VU, which helps addressing the threat. OE.Regular_Inspections helps addressing the threat through installations, calibrations, checks, inspections, repairs carried out by trusted fitters and workshops.

T.Security_Data is addressed by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport, OE.Software_Upgrade, OE.Controls. It is addressed by the O.Access, O.Processing, O.Secured_Data_Exchange to ensure appropriate protection while stored in the VU. O.Reliability (REU_201, RLB_206).

T.Software is addressed in the user environment by the O.Output, O.Processing, O.Reliability and O.Software_Upgrade as well as OE.Software_Upgrade to ensure the integrity of the code. O.Audit contributes to address the threat by recording events related to integrity errors. During design and manufacture, the threat is addressed by the OE.Development objectives. OE.Controls, OE.Regular_Inspections (checking for the audit records related).

T.Stored_Data is addressed mainly by O.Integrity, O.Access, O.Output and O.Reliability to ensure that no illicit access to data is possible. The O.Audit contributes to address the threat by recording data integrity errors. OE.Sofware_Upgrade included that software revisions shall be security certified before they can be implemented in the TOE to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU helping in addressing the threat.

OSP.Accountability is fulfilled by O.Accountability

OSP.Audit is fulfilled by O.Audit.

OSP.Software_Upgrade is fulfilled by O.Software_Upgrade and OE.Software_Upgrade,

OSP.Processing is fulfilled by O.Processing.

OSP.Test_Points is fulfilled by O.Reliability and OE.Test_Points

OSP.Type_Approved_MS is fulfilled by O.Authentication and OE.Type_Approved_MS

OSP.PKI is fulfilled by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport

OSP.MS_Keys is fulfilled by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport

A.Activation is upheld by OE.Activation.

A.Approved_Workshops is upheld by OE.Approved_Workshops.

A.Card_Availability is upheld by OE.Card_Availability.

A.Card_Traceability is upheld by OE.Card_Traceability.

A.Controls is upheld by OE.Controls.

A.Driver_Card_Uniqueness is upheld by OE.Driver_Card_Uniqueness.

A.Faithful_Calibration is upheld by OE.Faithful_Calibration and OE.Approved_Workshops.

A.Faithful_Drivers is upheld by OE.Faithful_Drivers.

A.Regular_Inspections is upheld by OE.Regular_Inspections.

5. EXTENDED COMPONENTS DEFINITION

This Security Target does not use any components defined as extensions to CC part 2.

6. 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 1 in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

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

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. In order to trace elements belonging to a component, the same slash "/" with iteration indicator is used behind the elements of a component.

For the sake of a better readability, the author uses an additional notation in order to indicate belonging of some SFRs to same functional cluster, namely a double slash "//" with the related functional group indicator after the component identifier. In order to trace elements belonging to a component, the same double slash "//" with functional cluster indicator is used behind the elements of a component.

6.1. Security Functional Requirements for the TOE

The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in chap. 4 of the ITSEC vehicle unit GST in [9]. Each of the below SFRs includes in curly braces {…} a list of SEFs related. This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from [9]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

6.1.1. Overview

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the PP defined the security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Identification and authentication of motion sensor und tachograph cards (according to [9], sec. 4.1)	– FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_AFL.1/MS: Authentication failure: motion sensor

	– FIA_AFL.1/TC: Authentication failure: tachograph cards – (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE Supported by: – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards – (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1)
Access control to functions and stored data (according to [9], sec. 4.2)	– (FDP_ACC.1/FIL, FDP_ACF.1/FIL): file structures – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): functions – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): stored data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): user data export – (FDP_ACC.1/IS, FDP_ACF.1/IS): input sources – FDP_ACC.1/SW-Upgrade: authenticate the software upgrades as destined for a particular TOE – FDP_ACF.1/SW-Upgrade: capability to control access to the TSF software upgrade function Supported by: – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT

	– FMT_MSA.3/UDE – FMT_MSA.3/IS – (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)
Accountability of users (according to [9], sec. 4.3)	– FAU_GEN.1: Audit records: Generation – FAU_STG.1: Audit records: Protection against modification – FAU_STG.4: Audit records: Prevention of loss – FDP_ETC.2: Export of user data with security attributes Supported by: – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): VU identification data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): Data update on the TC – FPT_STM.1: time stamps – FCS_COP.1/TDES: for the motion sensor and the tachograph cards
Audit of events and faults (according to [9], sec. 4.4)	– FAU_GEN.1: Audit records: Generation – FAU_SAR.1: Audit records: Capability of reviewing Supported by: – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): Storing motion sensor's audit records – FDP_ETC.2 Export of user data with security attributes: Related audit records to the TC.
Object reuse for secret data (according to [9], sec. 4.5)	– FDP_RIP.1 Subset residual information protection Supported by: – FCS_CKM.4: Cryptographic key destruction
Accuracy of recorded and stored data (according to [9], sec. 4.6)and of SW-upgrade data	– FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC) – FDP_ITC.2//IS: right input sources with sec. attributes (MS and TC) – FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC) – FDP_SDI.2: Stored data integrity

	Supported by: – (FDP_ACC.1/IS, FDP_ACF.1/IS): right input sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): limited manual entry – FAU_GEN.1: Audit records: Generation – FPT_STM.1: Reliable time stamps – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FPT_TDC.1/SW-Upgrade: capability to ensure the consistency of data for the update – FCS_COP.1/TDES: for decryption of the software update data – FCS_COP.1/SHA1: for integrity control of the software update data, VU code memory and data memory
Reliability of services (according to [9], sec. 4.7)	– FDP_ITC.2//IS: no executable code from external sources – FDP_ITC.2/SW-Upgrade: definition of conditions for update acceptance – FPR_UNO.1: Unobservability of leaked data – FPT_FLS.1: Failure with preservation of secure state – FPT_PHP.2//Power_Deviation: Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services Supported by: – FAU_GEN.1: Audit records: Generation – (FDP_ACC.1/IS, FDP_ACF.1/IS): no executable code from external sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): Tachograph Card withdrawal – FMT_MOF.1: No test entry points
Data exchange with motion sensor, tachograph cards and external media (download function) (according to [9], sec. 4.8)	– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media – FDP_ETC.2 Export of user data with security attributes: to the TC and to external media – FDP_ITC.2//IS Import of user data with security attributes: from the MS

	and the TC Supported by: – FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) – FCS_COP.1/RSA: for data downloading to external media (signing) – (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media – (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC – FAU_GEN.1: Audit records: Generation
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification/authentication

Table 5 Security functional groups vs. SFRs

6.1.2. Class FAU Security Audit

6.1.2.1. FAU_GEN Security audit data generation

FAU_GEN.1Audit data generation {UIA_206,UIA_214, ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_202, AUD_203, ACR_205, RLB_203, RLB_206, RLB_210, RLB_214, DEX_202, DEX_204}

Hierarchical to:

Dependencies: FPT_STM.1 Reliable time stamps: is fulfilled by FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following

auditable events:

a) Start-up and shutdown of the audit functions;

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

c) the activities and auditable events specified in REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, and 105a [23] and {UIA 206, UIA 214, AUD 202,ACR 205, RLB 203, RLB 206,

[23] all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_203}

RLB_210, RLB_214[24], DEX_202, DEX_204};

none.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the information specified in {REQ 081,084, 087, 090, 093, 094, 096, 098, 101, 102, 103, 105a[25]};

none

6.1.2.2. FAU_SAR Security audit review

FAU_SAR.1 Audit review {AUD_205}

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1

FAU_SAR.1.1 The TSF shall provide everybody with the capability to read the recorded information according to REQ011 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.

6.1.2.3. FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage {ACT_206}[26]

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1

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

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

FAU_STG.4 Prevention of audit data loss {ACT_206}[27]

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage: is fulfilled by FAU_STG.1

[24] Last card session not correctly closed

[25] all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_203}

[26] REQ081 to 093 and REQ102 to 105a

[27] REQ 083, 086, 089, 092, 105b; REQ105b is completely covered by ACT_206

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and behave according to REQ 083, 086, 089, 092 and 105b, if the audit trail is full.

6.1.3. Class FCO Communication

6.1.3.1. FCO_NRO Non-repudiation of origin

FCO_NRO.1 Selective proof of origin {DEX_206, DEX_207}

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification: not fulfilled, but **justified** the components FIA_UID.2/MS, FIA_UID.2/TC being present in the PP do not fulfil this dependency, because they are not affine to DEX_206, DEX_207 (data download).

The sense of the current dependency would be to attach the VU identity (ACT_202) to the data to be downloaded; the VU identification data are permanently stored in the VU, so that the VU always 'knows' its own identity.

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted data to be downloaded to external media at the request of the originator.

FCO_NRO.1.2 The TSF shall be able to relate the VU identity ~~of the originator~~ of the information, and the data to be downloaded to external media ~~of the information~~ to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to the recipient given

- according to specification [10], sec. 6.1,

limited to the scope as required in {DEX_207} and {DEX_208}

6.1.4. Class FCS Cryptographic Support

6.1.4.1. FCS_CKM Cryptographic key management

FCS_CKM.1 Cryptographic key generation {CSP_202}

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

FCS_COP.1 Cryptographic operation]: is fulfilled by FCS_CKM.2;

FCS_CKM.4 Cryptographic key destruction: is fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm cryptographic key derivation algorithms (for the session keys KSM and KST as well as for the temporarily stored keys K_m, K_P and K_{ID}) and specified cryptographic key sizes 112 bits that meet the following: list of standards:

a) K_m, K_P, K_{ID} and K_{SM}: two-keys TDES as specified in [12];

b) K_{ST}: two-keys TDES as specified in [10].

FCS_CKM.2 Cryptographic key distribution {CSP_203}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: is fulfilled by FCS_CKM.1

FCS_CKM.4: is fulfilled by FCS_CKM.4

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the list below that meets the following list of standards:

a) K_{SM}: as specified in [12], sec. 7.4.5;

b) K_{ST}: as specified in [10], CSM_020.

FCS_CKM.3 Cryptographic key access {CSP_204}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]:

a) fulfilled by FCS_CKM.1 for the session keys KSM and KST as well as for the temporarily stored keys K_m, K_P and K_{ID};

b) fulfilled by FDP_ITC.2//IS for the temporarily stored key Km_{wc}(entry DEX_203); fulfilled by FDP_ITC.2/SW-Upgrade for the temporarily stored key $KENC_{update}$

c) not fulfilled, but **justified** for EUR.PK, EQT.SK, Km_{vu},: The persistently stored keys (EUR.PK, EQT_j.SK, Km_{vu}) will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

FCS_CKM.4: is fulfilled by FCS_CKM.4

FCS_CKM.3.1 The TSF shall perform cryptographic key access and storage in accordance with a specified cryptographic key access method as specified below that meets the following list of standards:

a) Km_{wc}: part of the Master key read out from the workshop card and temporarily stored in the TOE (calibration phase);

b) K_m: temporarily reconstructed from part of the Master key Km_{vu} and part of the Master key Km_{wc} as specified in [12], sec. 7.2 and in [10], sec. 3.1.3, CSM_036, CSM_037 (calibration phase);

c) K_{ID}: temporarily reconstructed from the Master key K_m as specified in [12], sec. 7.2, 7.4.3 (calibration phase);

d) K_P: temporarily reconstructed from $Enc(K_m|K_P)$ as specified in [12], sec. 7.2, 7.4.3 (calibration phase);

e) K_{SM}: internally generated and temporarily stored during a session between the TOE and the motion sensor connected (calibration and operational phases);

f) K_{ST}: internally generated and temporarily stored during a session between the TOE and the tachograph card connected (calibration and operational phases);

g) EUR.PK: stored during manufacturing of the TOE (calibration and operational phases);

h) EQT_j.SK: stored during manufacturing of the TOE (calibration and operational phases);

i) part of the Master key Km_{vu}: stored during manufacturing of the TOE (calibration and operational phases);

j) *SW-Update Keys – DK_EQT.SK, DK.$C_{1,2}$: stored during manufacturing of the TOE; $KENC_{update}$: stored during the software upgrade process*.

FCS_CKM.4 Cryptographic key destruction {CSP_205}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: see explanation for FCS_CKM.3 above

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified

cryptographic key destruction method as specified below that meets the following list of standards:

a) Km_{wc}: delete after use (at most by the end of the calibration phase);

b) K_m: delete after use (at most by the end of the calibration phase);

c) K_{ID}: delete after use (at most by the end of the calibration phase);

d) K_P: delete after use (at most by the end of the calibration phase);

e) K_{SM}: delete by replacement (by closing a motion sensor communication session during the next pairing process);

f) K_{ST}: delete by replacement (by closing a card communication session);

g) EUR.PK: this public key does not represent any secret and, hence, needn't to be deleted;

h) EQT_j.SK: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational;

i) part of the Master key Km_{vu}: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational;

j) *SW-Update Keys – DK_EQT.SK, DK.$C_{1,2}$: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx, and must not be destroyed as long as the TOE is operational; $KENC_{update}$: will be deleted after use (at the end of the software upgrade process);*

6.1.4.2. FCS_COP Cryptographic operation

FCS_COP.1/TDES Cryptographic operation {CSP_201}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: is fulfilled by FCS_CKM.1 FCS_CKM.4: is fulfilled by FCS_CKM.4

a) fulfilled by FDP_ITC.2/SW-Upgrade for the temporarily stored keys $KENC_{update}$;
b) not fulfilled, but **justified** for DK_EQT.SK, DK.$C_{1,2}$: The permanently stored DK_EQT.SK, DK.$C_{1,2}$ keys will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

FCS_COP.1.1/TDES The TSF shall perform the cryptographic operations (encryption, decryption, Retail-MAC) in accordance with a specified cryptographic algorithm Triple DES in CBC and ECB modes and cryptographic key size 112 bits that meet the following: [12] for the Motion Sensor, [10]for the Tachograph Cards and 168 bits that meet the following: software upgrade.

FCS_COP.1/RSA Cryptographic operation {CSP_201}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: not fulfilled, but **justified** It is a matter of RSA decrypting and verifying in the context of CSM_020 (VU<->TC authentication) and of RSA signing according to CSM_034 using static keys imported outside of the VU’s operational phase (OE.Sec_Data_xx).

FCS_CKM.4: is fulfilled by FCS_CKM.4

FCS_COP.1.1/RSA The TSF shall perform the cryptographic operations (decryption, verifying for the Tachograph Cards authentication and signing for downloading to external media) in accordance with a specified cryptographic algorithm RSA and cryptographic key size 1024 bits that meet the following: [10], CSM_020 for the Tachograph Cards authentication and [10], CSM_034 for downloading to external media and software upgrade respectively.

FCS_COP.1/SHA1 Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4: not fulfilled, but **justified**SHA1 do not use keys for hashing, so there is no need for key insertion and key destruction method.

FCS_COP.1.1/SHA1 The TSF shall perform *the cryptographic operations (integrity detection and protection)* in accordance with a specified cryptographic algorithm, namely *SHA1* with a cryptographic key size of *none* that meet the following: *FIPS 180-1.*

6.1.5. Class FDP User Data Protection

6.1.5.1. FDP_ACC Access control policy

FDP_ACC.1/FIL Subset access control {ACC_211}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/FIL

FDP_ACC.1.1/FIL The TSF shall enforce the File Structure SFP on *tachograph application and data files structure as required by ACC_211.*

FDP_ACC.1/FUN Subset access control {ACC_201}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/FUN

FDP_ACC.1.1/FUN The TSF shall enforce the SFP FUNCTION on *subjects, objects, and operations as referred to in*

- operational modes {ACC_202} and the related restrictions on access rights {ACC_203},

- calibration functions {ACC_206} and time adjustment {ACC_208},

- limited manual entry {ACR_201a}, and

- Tachograph Card withdrawal {RLB_213} as required by ACC_201.

FDP_ACC.1/DAT Subset access control {ACC_201}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/DAT

FDP_ACC.1.1/DAT The TSF shall enforce the SFP DATA on *subjects, objects, and operations as referred to in:*

- VU identification data: REQ075 (structure) {ACT_202} and REQ076

(once recorded) {ACC_204},

- MS identification data: REQ079 (Manufacturing-ID) and REQ155 (pairing) {ACC_205},

- Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209},

- Security Data: REQ080 {ACC_210},

- MS Audit Records: {AUD_204}[28] as required by ACC_201.

FDP_ACC.1/UDE Subset access control {ACT_201, ACT_203, ACT_204}: REQ 109 and 109a

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/UDE
FDP_ACC.1.1/UDE	The TSF shall enforce the SFP User_Data_Export on *subjects, objects, and operations as required by REQ 109 and 109a*

FDP_ACC.1/IS Subset access control {ACR_201, RLB_205}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/IS
FDP_ACC.1.1/IS	The TSF shall enforce the SFP Input_Sources on *subjects, objects, and operations as required by ACR_201 (right input sources) and RLB_205 (no external executable code)*

FDP_ACC.1/SW-Upgrade Subset access control {ACC_201}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/SW-Upgrade
FDP_ACC.1.1/SW-Upgrade	The TSF shall enforce the SFP SW_Upgrade on *upgradeable software component and User identity for upgrades of software components*

6.1.5.2. FDP_ACF Access control functions

FDP_ACF.1/FIL Security attribute based access control {ACC_211}

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/FIL FMT_MSA.3: is fulfilled by FMT_MSA.3/FIL
FDP_ACF.1.1/FIL	The TSF shall enforce the File_Structure SFP to objects based on the following: *the entire files structure of the TOE-application as required by {ACC_211}.*
FDP_ACF.1.2/FIL	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: none.

[28] These data are generated not by the TOE, but by the Motion Sensor. Hence, they represent - from the point of view of the TOE - just a kind of data to be stored.

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

FDP_ACF.1.4/FIL The TSF shall explicitly deny access of subjects to objects based on the following additional rules as required by {ACC_211}.

FDP_ACF.1/FUN Security attribute based access control {ACC_202, ACC_203, ACC_206, ACC_208, ACR_201a, RLB_213}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/FUN

FMT_MSA.3: is fulfilled by FMT_MSA.3/FUN

FDP_ACF.1.1/FUN The TSF shall enforce the SFP FUNCTION to objects based on the following: *subjects, objects, and their attributes as referred to in:*

- operational modes {ACC_202} and the related restrictions on access rights {ACC_203},

- calibration functions {ACC_206} and time adjustment {ACC_208},

- limited manual entry {ACR_201a}, and

- Tachograph Card withdrawal {RLB_213}.

FDP_ACF.1.2/FUN The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in {ACC_202, ACC_203, ACC_206, ACC_208, ACR_201a, RLB_213}.

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

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

FDP_ACF.1/DAT Security attribute based access control {ACC_204, ACC_205, ACC_207, ACC_209, ACC_210, ACT_202, AUD_204}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/DAT

FMT_MSA.3: is fulfilled by FMT_MSA.3/DAT

FDP_ACF.1.1/DAT The TSF shall enforce the SFP DATA to objects based on the following: *subjects, objects, and their attributes as referred to in:*

- VU identification data: REQ075 (structure) {ACT_202} and REQ076 (once recorded) {ACC_204},

- MS identification data: REQ079 (Manufacturing-ID)and REQ155 (pairing) {ACC_205},

- Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209},

- Security Data: REQ080 {ACC_210},

- MS Audit Records: {AUD_204}.

FDP_ACF.1.2/DAT The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the access rules as required by {ACC_204, ACC_205, ACC_207, ACC_209, ACC_210, ACT_202, AUD_204}

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

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

FDP_ACF.1/UDE Security attribute based access control {ACT_201, ACT_203, ACT_204} (REQ109 and 109a)

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/UDE

FMT_MSA.3: is fulfilled by FMT_MSA.3/UDE

FDP_ACF.1.1/UDE The TSF shall enforce the SFP User Data Export to objects based on the following: *subjects, objects, and their attributes as required by REQ 109 and 109a*

FDP_ACF.1.2/UDE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in REQ109 and 109a.

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

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

FDP_ACF.1/IS Security attribute based access control {ACR_201, RLB_205}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/IS

FMT_MSA.3: is fulfilled by FMT_MSA.3/IS

FDP_ACF.1.1/IS The TSF shall enforce SFP Input Sources to objects based on the following: *subjects, objects, and their attributes as required by ACR_201 (right input sources) and RLB_205 (no external executable code).*

FDP_ACF.1.2/IS The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in {ACR_201[29]}.

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

FDP_ACF.1.4/IS The TSF shall explicitly deny access of subjects to objects based on the following additional rules as required by {RLB_205}.

FDP_ACF.1/SW-Upgrade Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/SW-Upgrade
FMT_MSA.3: not fulfilled but **justified**:
In the case of a software upgrade, the upgrade packages are accepted only if the corresponding credentials which contain all the information required for the verification are also available,. Thus, it is not necessary to initialize any static attributes.

FDP_ACF.1.1/SW-Upgrade The TSF shall enforce SFP SW_Upgrade to objects based on the following: upgradeable software packages can be replaced if the integrity and the authenticity of the package is guaranteed by virtue of the upgrade credentials

FDP_ACF.1.2/SW-Upgrade The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
- Software upgrade is only possible after workshop card authentication,
- Software upgrade is only acceptable if the integrity and the authenticity of the upgrade software package were confirmed by virtue of the upgrade credentials.

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

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

6.1.5.3. FDP_ETC Export from the TOE

FDP_ETC.2 Export of user data with security attributes {ACT_201, ACT_203, ACT_204, ACT_207, AUD_201, DEX_205, DEX_208} (REQ109 and 109a)

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/UDE

FDP_ETC.2.1 The TSF shall enforce the SFP User Data Export when exporting user data, controlled under the SFP(s), outside of 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

[29] Especially for MS and TC

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: REQ110, DEX_205, DEX_208.

6.1.5.4. FDP_ITC Import from outside of the TOE

FDP_ITC.1 Import of user data without security attributes {ACR_201}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS

FMT_MSA.3: is fulfilled by FMT_MSA.3/IS

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

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: as required by {ACR_201} for recording equipment calibration parameters and user's inputs.

FDP_ITC.2//IS Import of user data with security attributes {ACR_201, RLB_205, DEX_201, DEX_202, DEX_203, DEX_204}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS

[FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but **justified**:

Indeed, trusted channels VU<->MS and VU<->TC will be established. Since the component FTP_ITC.1 represents just a higher abstraction level integrative description of this property and does not define any additional properties comparing to {FDP_ITC.2//IS + FDP_ETC.2 + FIA_UAU.1/TC (and /MS)}, it can be dispensed with this dependency in the current context of the PP.

FPT_TDC.1: is fulfilled by FPT_TDC.1//IS

FDP_ITC.2.1//IS The TSF shall enforce the SFP Input_Sources when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2//IS The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3//IS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4//IS The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5//IS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE as required by:

- [12] for the Motion Sensor {ACR_201, DEX_201},

- DEX_202 (audit record and continue to use imported data),

- [10] for the Tachograph Cards {ACR_201, DEX_203},

- DEX_204 (audit record and not using of the data),

- RLB_205 (no executable code from external sources).

FDP_ITC.2/SW-Upgrade Import of user data with security attributes

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/SW-Upgrade
[FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but **justified**: In case of a software upgrade, the upgrade packages are accepted only if the corresponding credentials which contain all the information required for the verification are also available. Thus, it is not necessary to establish a trusted channel or trusted path.
FPT_TDC.1: is fulfilled by FPT_TDC.1/SW-Upgrade

FDP_ITC.2.1/SW-Upgrade The TSF shall enforce the SFP SW_Upgrade when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/SW-Upgrade The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/SW-Upgrade The TSF shall ensure that the used protocol provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/SW-Upgrade The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/SW-Upgrade The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE upgrade of the indicated software components only if the integrity and the authenticity of the upgrade software package is confirmed by virtue of the upgrade credentials
- [10] for the Tachograph Cards {ACR_201, DEX_203},
- DEX_204 (audit record and not using of the data),
- RLB_205 (no executable code from external sources).

6.1.5.5. FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {REU_201}

Hierarchical to: -

Dependencies: -

The TSF shall ensure that any previous information content of a **temporarily stored** resource is made unavailable upon the *allocation of the resource to* the following objects:

a) Km_{WC}: workshop card part of the motion sensor master key (at most by the end of the calibration phase);

b) K_m: motion sensor master key (at most by the end of the calibration phase);

c) K_{ID}: motion sensor identification key (at most by the end of the calibration phase);

d) K_P: motion sensor pairing key (at most by the end of the calibration phase);

e) K_{SM}: session key between motion sensor and vehicle unit (when its temporarily stored value shall not be used any more);

f) K_{ST}: session key between tachograph cards and vehicle unit (by closing a card communication session);

g) EQT_j.SK: equipment private key (when its temporarily stored value shall not be used any more);

h) Km_{VU}: VU part of the motion sensor master key (when its temporarily stored value shall not be used any more);

i) PIN: the verification value of the workshop card PIN temporarily stored in the TOE during its calibration (at most by the end of the calibration phase);

j) *SW-Update Keys – DK EQT.SK, DK.*$C_{1,2:,}$ *KENC*$_{update}$ *(when the temporarily stored values shall not be used any more, at most by the end of the software upgrade).*

6.1.5.6. FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity {ACR_204, ACR_205}

Hierarchical to: -
Dependencies:
FDP_SDI.2.1 The TSF shall monitor user data stored in the **TOE's data memory** ~~containers controlled by the TSF~~ for integrity errors ~~on all objects, based on the following attributes:[assignment: user data attributes].~~
FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall generate an audit record.

6.1.6. Class FIA Identification and Authentication

6.1.6.1. FIA_AFL Authentication failures

FIA_AFL.1/MS Authentication failure handling {UIA_206}

Hierarchical to: -

Dependencies: FIA_UAU.1: is fulfilled by FIA_UAU.2//MS

FIA_AFL.1.1/MS The TSF shall detect when *10* unsuccessful authentication attempts occur related to motion sensor authentication.

FIA_AFL.1.2/MS When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall

- generate an audit record of the event,
- warn the user,
- continue to accept and use non secured motion data sent by the motion sensor.

FIA_AFL.1/TC Authentication failure handling {UIA_214}

Hierarchical to: -

Dependencies: FIA_UAU.1: is fulfilled by FIA_UAU.1/TC

FIA_AFL.1.1/TC The TSF shall detect when 5 unsuccessful authentication attempts occur related to tachograph card authentication.

FIA_AFL.1.2/TC When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall

- generate an audit record of the event,
- warn the user,
- assume the user as Unknown User and the card as non valid[30] (definition (z) and REQ007).

6.1.6.2. FIA_ATD User attribute definition

FIA_ATD.1//TC User attribute definition {UIA_208}

Hierarchical to: -

Dependencies: -

FIA_ATD.1.1//TC The TSF shall maintain the following list of security attributes belonging to individual users: as defined in {UIA_208}.

6.1.6.3. FIA_UAU User authentication

FIA_UAU.1/TC Timing of authentication {UIA_209}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/TC

FIA_UAU.1.1/TC The TSF shall allow (i) TC identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by FAU_SAR.1 on behalf

[30] is commensurate with 'Unknown equipment' in the current ST

of the user to be performed before the user is authenticated[31]

FIA_UAU.1.2/TC The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PIN Timing of authentication {UIA_212}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/TC[32]

FIA_UAU.1.1/PIN The TSF shall allow (i) TC (Workshop Card) identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by FAU_SAR.1 on behalf of the user to be performed before the user is authenticated[33]

FIA_UAU.1.2/PIN The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2//MS User authentication before any action {UIA_203}[34]

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/MS

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

FIA_UAU.3/MS Unforgeable authentication {UIA_205}

Hierarchical to: -

Dependencies: -

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

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

FIA_UAU.3/TC Unforgeable authentication {UIA_213}

Hierarchical to: -

Dependencies: -

FIA_UAU.3.1/TC The TSF shall detect and prevent use of authentication data that has

[31] According to CSM_20 in [10] the TC identification (certificate exchange) is to perform strictly before the mutual authentication between the VU and the TC.

[32] the PIN-based authentication is applicable for the workshop cards, whose identification is ruled by FIA_UID.2/TC

[33] According to CSM_20 in [10] the TC identification (certificate exchange) is to perform strictly before the PIN authentication of the Workshop Card.

[34] Though MS identification happens before the MS authentication, they will be done within same command (80 or 11); hence, it is also plausible to choose here the functional component FIA_UAU.2.

been forged by any user of the TSF.

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

FIA_UAU.5//TC Multiple authentication mechanisms {UIA_211}

Hierarchical to: -

Dependencies:

FIA_UAU.5.1//TC The TSF shall provide multiple authentication mechanisms according to CSM_20 in [10] to support user authentication.

FIA_UAU.5.2//TC The TSF shall authenticate any user's claimed identity according to the

CSM_20 in [10].

FIA_UAU.6/MS Re-authenticating {UIA_204}.

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1/MS The TSF shall re-authenticate the user under the conditions *more frequently than once per hour, cf. UIA_204 in [9].*

FIA_UAU.6/TC Re-authenticating {UIA_210}

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1/TC The TSF shall re-authenticate the user under the conditions *more frequently than once per day, cf. UIA_210 in [9].*

6.1.6.4. FIA_UID User identification

FIA_UID.2/MS User identification before any action {UIA_201}

Hierarchical to: -

Dependencies: -

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

FIA_UID.2/TC User identification before any action {UIA_207}

Hierarchical to: FIA_UID.1

Dependencies: -

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

6.1.7. Class FPR Privacy

6.1.7.1. FPR_UNO Unobservability

FPR_UNO.1 Unobservability {RLB_204 for leaked data}

Hierarchical to: -

Dependencies: -

FPR_UNO.1.1 The TSF shall ensure that all users are unable to observe the **cryptographic** operations as required by FCS_COP.1/TDES and FCS_COP.1/RSA on cryptographic keys being to keep secret (as listed in FCS_CKM.3 excepting EUR.PK) by **the TSF**~~[assignment: list of protected users and/or subjects]~~.

6.1.8. Class FPT Protection of the TSF

6.1.8.1. 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 when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}.

6.1.8.2. FPT_PHP TSF physical protection

FPT_PHP.2//Power_Deviation Notification of physical attack {RLB_209}

Hierarchical to: FPT_PHP.1

Dependencies: FMT_MOF.1: not fulfilled, but **justified**:

It is a matter of RLB_209: this function (detection of deviation) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a not applicable way for RLB_209

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

FPT_PHP.2.2//Power_Deviation 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//Power_Deviation For the devices/elements for which active detection is required in {RLB_209}, the TSF shall monitor the devices and elements and notify the user and audit record generation when physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3Resistance to physical attack {RLB_204 for stored data}

Hierarchical to: -

Dependencies:

FPT_PHP.3.1 The TSF shall resist physical tampering attacks to the TOE security enforcing part of the software in the field after the TOE activation by responding automatically such that the SFRs are always enforced.

6.1.8.3. FPT_STM Time stamps

FPT_STM.1Reliable time stamps {ACR_201}

Hierarchical to: -

Dependencies:

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

6.1.8.4. FPT_TDC Inter-TSF TSF Data Consistency

FPT_TDC.1//ISInter-TSF basic TSF data consistency {ACR_201}

Hierarchical to: -

Dependencies:

FPT_TDC.1.1//IS The TSF shall provide the capability to consistently interpret secure messaging attributes as defined by [12] for the Motion Sensor and by [10] for the Tachograph Cards when shared between the TSF and another trusted IT product.

FPT_TDC.1.2//IS The TSF shall use the interpretation rules (communication protocols) as defined by [12] for the Motion Sensor and by [10] for the Tachograph Cards when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/SW-Upgrade Inter-TSF basic TSF data consistency

Hierarchical to: -

Dependencies:

FPT_TDC.1.1/SW-Upgrade The TSF shall provide the capability to consistently interpret SW upgrade package and upgrade credentials when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SW-Upgrade The TSF shall use the credentials which belong to software upgrade package and particular VU when interpreting the TSF data from another trusted IT product.

6.1.8.5. FPT_TST TSF self test

FPT_TST.1 TSF testing {RLB_202}

Hierarchical to: -

Dependencies:

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate the **integrity of security data and the integrity of stored executable code (if not in ROM)**~~ the correct operation of [selection: *[assignment: parts of TSF]*, *the TSF*~~].

FPT_TST.1.2 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of security data.

FPT_TST.1.3 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of stored TSF executable code.

6.1.9. Class FRU Resource Utilisation

6.1.9.1. FRU_PRS Priority of service

FRU_PRS.1 Limited priority of service {RLB_212}

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 functions and data covered by the current set of SFRs shall be mediated on the basis of the subjects' assigned priority.

6.1.10. Class FMT Security Management

6.1.10.1. FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes {UIA_208}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/FUN

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_SMF.1: is fulfilled by FMT_SMF.1

FMT_MSA.1.1 The TSF shall enforce the SFP FUNCTION to restrict the ability to change default the security attributes User Group, User ID[35] to nobody.

FMT_MSA.3/FUN Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/FUN The TSF shall enforce the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/FUN The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is

[35] see definition of the role 'User' in Table 3 above.

created.

FMT_MSA.3/FIL Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/FIL The TSF shall enforce the File_Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/FIL The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/DAT Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/DAT The TSF shall enforce the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/DAT The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/UDE Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/UDE The TSF shall enforce the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/UDE The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/IS Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/IS The TSF shall enforce the SFP Input Sources to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IS The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

6.1.10.2. FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour {RLB_201}

Hierarchical to: -

Dependencies: FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_SMF.1: is fulfilled by FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to enable the functions specified in {RLB_201} to nobody.

6.1.10.3. FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions {UIA_208}

Hierarchical to: -

Dependencies:

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: all operations being allowed only in the calibration mode as specified in REQ010.

FMT_SMF.1/SW-Upgrade Specification of Management Functions

Hierarchical to: -

Dependencies:

FMT_SMF.1.1/SW-Upgrade The TSF shall be capable of performing the following management functions: upgrade of upgradeable software components if the rights and conditions are fulfilled as specified in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade.

6.1.10.4. FMT_SMR Security management roles

FMT_SMR.1//TC Security roles {UIA_208}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/TC

FMT_SMR.1.1//TC The TSF shall maintain the roles as defined in {UIA_208} as UserGroups:

- DRIVER (driver card),
- CONTROLLER (control card),
- WORKSHOP (workshop card),
- COMPANY (company card),
- UNKNOWN (no card inserted),

- Motion Sensor,
- Unknown equipment.

FMT_SMR.1.2//TC The TSF shall be able to associate users with roles.

6.2. Security Assurance Requirements for the TOE

The European Regulation [6] requires for a vehicle unit the assurance level ITSEC E3, high as specified in [9], chap. 6 and 7.

JIL [11] defines an assurance package called E3hAP declaring assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. 2.1) certification (in conjunction with the Digital Tachograph System).

The current official CCMB version of Common Criteria is Version 3.1, Revision 3. This version defines in its part 3 assurance requirements components partially differing from the respective requirements of CC v2.x.

The CC community acts on the presumption that the assurance components of CCv3.1 and CCv2.x are equivalent to each other.

Due to this fact, the author of this PP compiled and defined an appropriate assurance package **E3hCC31_AP** as shown below (validity of this proposal is confined to the Digital Tachograph System):

Assurance Classes	**Assurance Family**	**E3hCC31_AP** (based on EAL4)
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_INT	-
	ADV_TDS	3
	ADV_SPM	-
Guidance Documents	AGD_OPE	1
	AGD_PRE	1
Life Cycle Support	ALC_CMC	4
	ALC_CMS	4
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1

Assurance Classes	**Assurance Family**	**E3hCC31_AP** (based on EAL4)
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	ATE_FUN	1
	ATE_IND	2
Vulnerability Assessment	AVA_VAN	5

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

The requirement {RLB_215} is covered by ADV_ARC (security domain separation); the requirement {RLB_204} is partially covered by ADV_ARC (self-protection).

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

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

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FAU_GEN.1	Audit data generation		X	X								
FAU_SAR.1	Audit review		X	X								
FAU_STG.1	Protected audit trail storage		X	X		X						
FAU_STG.4	Prevention of audit data loss		X	X								
FCO_NRO.1	Selective proof of origin						X			X		
FCS_CKM.1	Cryptographic key generation									X		
FCS_CKM.2	Cryptographic key distribution									X		
FCS_CKM.3	Cryptographic key access									X		

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FCS_CKM.4	Cryptographic key destruction									X		
FCS_COP.1/TDES	Cryptographic operation									X		X
FCS_COP.1/RSA	Cryptographic operation									X		
FCS_COP.1/SHA1	Cryptographic operation					X						X
FDP_ACC.1/FIL	Subset access control	X										
FDP_ACC.1/FUN	Subset access control	X						X	X	X	X	
FDP_ACC.1/DAT	Subset access control	X										
FDP_ACC.1/UDE	Subset access control	X										
FDP_ACC.1/IS	Subset access control	X						X	X			
FDP_ACC.1/SW-Upgrade	Subset access control	X							X			X
FDP_ACF.1/FIL	Security attribute based access control	X										
FDP_ACF.1/FUN	Security attribute based access control	X						X	X	X	X	
FDP_ACF.1/DAT	Security attribute based access control	X										
FDP_ACF.1/UDE	Security attribute based access control	X										
FDP_ACF.1/IS	Security attribute based access control	X						X	X			
FDP_ACF.1/ SW-Upgrade	Security attribute based access control	X							X			X
FDP_ETC.2	Export of user data with security attributes		X			X	X			X		
FDP_ITC.1	Import of user data without security attributes							X	X			
FDP_ITC.2//IS	Import of user data with security attributes							X	X	X		
FDP_ITC.2/ SW-Upgrade	Import of user data with security attributes								X			X

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FDP_RIP.1	Subset residual information protection	X						X	X			
FDP_SDI.2	Stored data integrity monitoring and action			X		X	X		X			
FIA_AFL.1/MS	Authentication failure handling			X	X				X			
FIA_AFL.1/TC	Authentication failure handling			X	X				X			
FIA_ATD.1//TC	User attribute definition			X						X		
FIA_UAU.1/TC	Timing of authentication				X					X		
FIA_UAU.1/PIN	Timing of authentication				X							
FIA_UAU.2//MS	User authentication before any action				X					X		
FIA_UAU.3/MS	Unforgeable authentication				X							
FIA_UAU.3/TC	Unforgeable authentication				X							
FIA_UAU.5//TC	Multiple authentication mechanisms	X			X					X		
FIA_UAU.6/MS	Re-authenticating				X					X		
FIA_UAU.6/TC	Re-authenticating				X					X		
FIA_UID.2/MS	User identification before any action	X	X	X	X					X		
FIA_UID.2/TC	User identification before any action	X	X	X	X					X		
FMT_MSA.1	Management of security attributes	X								X		
FMT_MSA.3/FUN	Static attribute initialisation	X						X	X	X	X	
FMT_MSA.3/FIL	Static attribute initialisation	X										
FMT_MSA.3/DAT	Static attribute initialisation	X										
FMT_MSA.3/IS	Static attribute initialisation	X						X	X			
FMT_MSA.3/UDE	Static attribute initialisation	X										
FMT_MOF.1	Management of security functions	X							X			
FMT_SMF.1	Specification of Management Functions	X								X		

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FMT_SMF.1/SW-Upgrade	Specification of Management Functions											X
FMT_SMR.1//TC	Security roles	X								X		
FPR_UNO.1	Unobservability						X	X	X		X	
FPT_FLS.1	Failure with preservation of secure state.			X					X			
FPT_PHP.2//Power_ Deviation	Notification of physical attack								X			
FPT_PHP.3	Resistance to physical attack						X	X	X		X	
FPT_STM.1	Reliable time stamps		X	X				X	X			
FPT_TDC.1//IS	Inter-TSF basic TSF data consistency							X	X			
FPT_TDC.1/ SW-Upgrade	Inter-TSF basic TSF data consistency								X			X
FPT_TST.1	TSF testing			X					X			
FRU_PRS.1	Limited priority of service								X			

Table 6 Coverage of Security Objectives for the TOE by SFR

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

security objectives	Security functional requirement	
O.Access	FDP_ACC.1/FIL	File structure SFP on application and data files structure
	FDP_ACC.1/FUN	SFP FUNCTION on the functions of the TOE
	FDP_ACC.1/DAT	SFP DATA on user data of the TOE
	FDP_ACC.1/UDE	SFP User_Data_Export for the export of user data
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACC.1/SW-	Guarantees the rights for software updates

security objectives	Security functional requirement	
	Upgrade	
	FDP_ACF.1/FIL	Entire files structure of the TOE-application
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/DAT	Defines security attributes for SFP DATA on user
	FDP_ACF.1/UDE	Defines security attributes for SFP User_Data_Export
	FDP_ACF.1/IS	Defines security attributes for SFP Input Sources.
	FDP_ACF.1/SW-Upgrade	Guarantees the conditions for software updates
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation of resource
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [10] to support user authentication.
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FMT_MSA.1	Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody.
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/FIL	Provides the File_Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/DAT	Provides the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created

security objectives	Security functional requirement	
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/UDE	Provides the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MOF.1	Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, prevents an unintended access to data in the operational phase.
	FMT_SMF.1	Performing all operations being allowed only in the calibration mode.
	FMT_SMR.1//TC	Maintain the roles as defined in {UIA_208} as User Groups.
O.Accountability	FAU_GEN.1	Generates correct audit records
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FPT_STM.1	Provides accurate time
O.Audit	FAU_GEN.1	Generates correct audit records
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion.
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)

security objectives	Security functional requirement	
	FDP_SDI.2	monitors user data stored for integrity error
	FIA_AFL.1/MS	Detects and records authentication failure events for the motion sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FIA_ATD.1//TC	Defines user attributes for tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FPT_FLS.1	Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}
	FPT_STM.1	Provides accurate time
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
O.Authentication	FIA_AFL.1/MS	Detects and records authentication failure events for the motion sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FIA_UAU.1/TC	Allows TC identification before authentication
	FIA_UAU.1/PIN	Allows TC (Workshop Card) identification before authentication
	FIA_UAU.2//MS	Motion sensor has to be successfully authenticated before allowing any action
	FIA_UAU.3/MS	Provides unforgeable authentication for the motion sensor
	FIA_UAU.3/TC	Provides unforgeable authentication for the tachograph cards
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [10] to support user authentication.
	FIA_UAU.6/MS	Periodically re-authenticate the motion sensor
	FIA_UAU.6/TC	Periodically re-authenticate the tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action

security objectives	Security functional requirement	
O.Integrity	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FCS_COP.1/SHA1	Provides stored data integrity
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_SDI.2	monitors user data stored for integrity error
O.Output	FCO_NRO.1	Generates an evidence of origin for the data to be downloaded to external media.
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_SDI.2	monitors user data stored for integrity error
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_PHP.3	Ensures resistance to physical attack to the TOE software in the field after the TOE activation
O.Processing	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/IS	Defines security attributes for SFP User_Data_Export
	FDP_ITC.1	Provides import of user data from outside of the TOE using the SFP Input Sources
	FDP_ITC.2//IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation of resource
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.

security objectives		Security functional requirement
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_PHP.3	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1//IS	Provides the capability to consistently interpret secure messaging attributes as defined by [12] for the Motion Sensor and by [10] for the Tachograph Cards.
O.Reliability	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACC.1/SW-Upgrade	Guarantees the rights for software upgrades
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/IS	Defines security attributes for SFP User_Data_Export
	FDP_ACF.1/SW-Upgrade	Guarantees the conditions for software upgrades
	FDP_ITC.1	Provides import of user data from outside of the TOE using the SFP Input Sources
	FDP_ITC.2//IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards
	FDP_ITC.2/SW-Upgrade	Provides import of SW upgrade data from outside of the TOE, using the defined conditions for the update acceptance
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation of resource
	FDP_SDI.2	monitors user data stored for integrity error
	FIA_AFL.1/MS	Detects and records authentication failure events for the motion

security objectives	Security functional requirement	
		sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FMT_MOF.1	Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, increases TOE reliability in the operational phase.
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_FLS.1	Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}
	FPT_PHP.2//Power_ Deviati on	Detection of physical tampering (Power_Deviation) and generation of an audit record
	FPT_PHP.3	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1//IS	Provides the capability to consistently interpret secure messaging attributes as defined by [12] for the Motion Sensor and by [10] for the Tachograph Cards
	FPT_TDC.1/SW-Upgrade	Provides the capability to consistently interpret the software update data and the corresponding credentials.
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
	FRU_PRS.1	Ensures that resources will be available when needed
O.Secured_Data_Exchange	FCO_NRO.1 FCS_CKM.1	Generates an evidence of origin for the data to be downloaded to external media. Generates of session keys for the motion sensor and the

security objectives		Security functional requirement
		tachograph cards
	FCS_CKM.2	Controls distribution of cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the table below that meets the following list of standards.
	FCS_CKM.3	Controls cryptographic key access and storage in the TOE
	FCS_CKM.4	Destroys cryptographic keys in the TOE
	FCS_COP.1/TDES	Provides the cryptographic operation TDES
	FCS_COP.1/RSA	Provides the cryptographic operation RSA
	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_ITC.2//IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards
	FIA_ATD.1//TC	Defines user attributes for tachograph cards
	FIA_UAU.1/TC	Allows TC identification before authentication
	FIA_UAU.2//MS	Motion sensor has to be successfully authenticated before allowing any action
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [10] to support user authentication.
	FIA_UAU.6/MS	Periodically re-authenticate the motion sensor
	FIA_UAU.6/TC	Periodically re-authenticate the tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action

security objectives	Security functional requirement	
	FMT_MSA.1	Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created
	FMT_SMF.1	Performing all operations being allowed only in the calibration mode
	FMT_SMR.1//TC	Maintain the roles as defined in {UIA_208} as User Groups
O.Software_Analysis	FPT_PHP.3	Ensures resistance to physical attack to the TOE software in the field after the TOE activation
	FPR_UNO.1	Ensures unobservability of secrets
	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
O.Software_Upgrade	FDP_ACC.1/SW-Upgrade	Guarantees the rights for software updates
	FDP_ACF.1/SW-Upgrade	Guarantees the conditions for software updates
	FDP_ITC.2/SW-Upgrade	Provides import of SW upgrade data inclusive the corresponding credentials from outside of the TOE.
	FPT_TDC.1/SW-Upgrade	Provides the capability to consistently interpret the software upgrade package and the corresponding credentials.
	FCS_COP.1/RSA	Provides the cryptographic operation RSA
	FCS_COP.1/TDES	Provides the cryptographic operation TDES
	FCS_COP.1/SHA1	Provides the cryptographic operation SHA1 for integrity

security objectives		Security functional requirement
		protection
	FMT_SMF.1/SW-Upgrade	Performs the upgrade only if the rights and conditions allow it.

Table 7Suitability of the SFRs

6.3.2. Rationale for SFR's Dependencies

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The dependency analysis has directly been made within the description of each SFR in sec. 6.1 above. All dependencies being expected by CC part 2 are either fulfilled or their non-fulfilment is justified.

6.3.3. Security Assurance Requirements Rationale

The current protection profile is claimed to be conformant with the assurance package E3hCC31_AP (cf. sec. 2.3 above). As already noticed there in sec. 6.2, the assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

The main reason for choosing made is the legislative framework [11], where the assurance level required is defined in form of the assurance package E3hAP (for CCv2.1). The author translated this assurance package E3hAP into the assurance package E3hCC31_AP. These packages are commensurate with each other.

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects, entry 'Attacker'). This decision represents a part of the conscious security policy for the recording equipment required by the legislative [6] 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 component, all dependencies are met or exceeded in the EAL4 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
	TOE security assurance requirements (only additional to EAL4)	
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 8 SAR Dependencies

6.3.4. Security Requirements – Internal Consistency

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

6.3.4.1. SFRs

The dependency analysis in section 6.3.2 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in 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 and completely reflects the Generic Security Target [9]. Since the GST [9] is part of the related legislation, it is assumed to be internally consistent. Therefore, due to conformity between the current PP and [9], also subjects and objects being used in the current PP are used in a consistent way.

6.3.4.2. SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance

Requirements Rationale 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 6.3.2 Rationale for SFR's Dependencies and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements

7. TOE SUMMARY SPECIFICATION

7.1. TOE Security Functions

7.1.1. Identification and Authentication

The TOE provides this security function of identification and authentication of the motion sensor and users by monitoring the tachograph cards. Detailed properties of this security function are described below.

Motion sensor identification and authentication:

Requirement, Appendix 10	Related SFR used in the current ST	Security Function Description
UIA_201	FIA_UID.2/MS	The TOE is able to establish, for every interaction, the identity of the motion sensor it is connected to.
UIA_202	OSP.Type_Approved_MS	The identity of the motion sensor consists of the sensor approval number and the sensor serial number.
UIA_203	FIA_UAU.2//MS	The TOE authenticates the motion sensor it is connected to: • at motion sensor connection, • at each calibration of the recording equipment, • at power supply recovery Authentication is mutual and triggered by the TOE.
UIA_204	FIA_UAU.6/MS	The TOE periodically (*in 15 minutes*) re-identifies and re-authenticates the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.
UIA_205	FIA_UAU.3/MS	The TOE detects and prevents use of authentication data that has been copied and replayed.

UIA_206	FIA_AFL.1/MS, FAU_GEN.1	After 5 consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the TSF: - generates an audit record of the event, - warns the user, - continues to accept and use non secured motion data sent by the motion sensor.

User identification and authentication

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
UIA_207	FIA_UID.2/TC	The TOE permanently and selectively tracks the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.
UIA_208	FIA_ATD.1//TC for User Identity FMT_MSA.3/FUN for the default value UNKNOWN (no valid card) FDP_ACC.1/FUN for functions (for UNKNOWN) FMT_MSA.1 FMT_SMF.1 FMT_SMR.1//TC for five different User Groups	The user identity consists of: • a user group: ○ DRIVER (driver card), ○ CONTROLLER (control card), ○ WORKSHOP (workshop card), ○ COMPANY (company card), ○ UNKNOWN (no card inserted), • a user ID, composed of : ○ the card issuing Member State code and of the card number, ○ UNKNOWN if user group is UNKNOWN. UNKNOWN identities may be implicitly or explicitly.
UIA_209	FIA_UAU.1/TC	The TOE authenticates its users at card insertion.
UIA_210	FIA_UAU.6/TC	The TOE re-authenticates its users: - at power supply recovery, - periodically or after occurrence of specific

		events (*every 4 hours*).
UIA_211	FIA_UAU.5//TC	Authentication is performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication is mutual and triggered by the TOE.
UIA_212	FIA_UAU.1/PIN	In addition to the above, workshops are required to be successfully authenticated through a PIN check. PINs are at least 4 characters long. Note: In the case the PIN is transferred to the TOE from an outside equipment located in the vicinity of the TOE, PIN confidentiality is protected during the transfer.
UIA_213	FIA_UAU.3/TC	The TOE detects and prevents use of authentication data that has been copied and replayed.
UIA_214	FIA_AFL.1/TC, FAU_GEN.1	After 5 consecutive unsuccessful authentication attempts have been detected, the TSF: - generates an audit record of the event, - warns the user, assume the user as UNKNOWN, and the card as non valid (definition (z) and requirement 007).

7.1.2. Access Control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

It must be noted that the user data recorded by the TOE, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011) is not the subject of a security enforcing function.

Access control policy:

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**

ACC_201	FDP_ACC.1/FUN for functions FMT_MSA.3/FUN FDP_ACC.1/DAT for data FMT_MSA.3/DAT	The TOE manages and check access control rights to functions and to data.

Access rights to functions

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
ACC_202	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for choosing an operation mode according to REQ006 to 009.	The TOE enforces the mode of operation selection rules (requirements 006 to 009).
ACC_203	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for accessible functions in each mode of operation (REQ010)	The TOE uses the mode of operation to enforce the functions access control rules (requirement 010).

Access rights to data:

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
ACC_204	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ076 FMT_MSA.3/DAT	The TOE enforces the TOE identification data write access rules (requirement 076)
ACC_205	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ079 and 155 FMT_MSA.3/DAT FMT_MSA.3/IS	The TOE enforces the paired motion sensor identification data write access rules (requirements 079 and 155)

ACC_206	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for REQ154 and 156.	After the TOE activation, the TOE ensures that only in calibration mode, may calibration data be input into the TOE and stored into its data memory (requirements 154 and 156).
ACC_207	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ097 FMT_MSA.3/DAT	After the TOE activation, the TOE enforces calibration data write and delete access rules (requirement 097).
ACC_208	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for ACC_208	After the TOE activation, the TOE ensures that only in calibration mode, may time adjustment data be input into the TOE and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).
ACC_209	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for ACC_209 FMT_MSA.3/DAT	After the TOE activation, the TOE enforces time adjustment data write and delete access rules (requirement 100).
ACC_210	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ080 FMT_MSA.3/DAT	The TOE enforces appropriate read and write access rights to security data (requirement 080).

File structure and access conditions:

Requirement, **Appendix 10**	**Related SFR used in the current ST**	**Security Function Description**
ACC_211	FDP_ACC.1/FIL and FDP_ACF.1/FIL with only one rule as stated in ACC_211 for file structure FMT_MSA.3/FIL	Application and data files structure and access conditions is created during the manufacturing process, and then locked from any future modification or deletion.

7.1.3. Accountability

Requirement, Appendix 10	Related SFR used in the current ST	Security Function Description
ACT_201	FAU_GEN.1 with an entry for REQ081, 084, 087, 105a REQ105b is completely covered by ACT_206 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109, 109a FMT_MSA.3/UDE	The TOE ensures that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).
ACT_202	FDP_ACC.1/DAT, FDP_ACF.1/DAT FMT_MSA.3/DAT	The TOE holds permanent identification data (requirement 075).
ACT_203	FAU_GEN.1 with an entry for REQ098, 101 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE	The TOE ensures that workshops are accountable for their activities (requirements 098, 101 and 109).
ACT_204	FAU_GEN.1 with an entry for REQ102, 103 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE	The TOE ensures that controllers are accountable for their activities (requirements 102, 103 and 109).
ACT_205	FAU_GEN.1 with an entry for REQ 090, 093	The TOE records odometer data (requirement 090) and detailed speed data (requirement 093).
ACT_206	FAU_STG.1 with *detection* for 081 to 093 and 102 to 105a FAU_STG.4 for REQ083, 086, 089, 092,	The TOE ensures that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.

	105b (replacing oldest data)	
ACT_207	FDP_ETC.2 for REQ109, 109a and 110	The TOE ensures that it does not modify data already stored in a tachograph card (requirement 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1.Note.

7.1.4. Audit

Audit capabilities are required only for events that may indicate a manipulation or a security breach attempt. It is not required for the normal exercising of rights even if relevant to security.

Requirement, **Appendix 10**	**Related SFR used in the current ST**	**Security Function Description**
AUD_201	FAU_GEN.1 for REQ094, 096 FDP_ETC.2	The TOE, for events impairing the security of the TOE, records those events with associated data (requirements 094, 096 and 109).
AUD_202	FAU_GEN.1 for AUD_202	The events affecting the security of the TOE are the following: – Security breach attempts: - motion sensor authentication failure, - tachograph card authentication failure, - unauthorised change of motion sensor, - card data input integrity error, - stored user data integrity error, - internal data transfer error, - unauthorised case opening, - hardware sabotage, – Last card session not correctly closed, – Motion data error event, – Power supply interruption event, – TOE internal fault.

AUD_203	FAU_GEN.1	The TOE enforces audit records storage rules (requirement 094 and 096).
AUD_204	FDP_ACC.1/DAT FDP_ACF.1/DAT FMT_MSA.3/DAT	The TOE stores audit records generated by the motion sensor in its data memory.
AUD_205	FAU_SAR.1	TOE is able to print, display and download audit records.

7.1.5. Object re-use

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
REU_201	FDP_RIP.1	The TOE ensures that temporary storage objects can be reused without this involving inadmissible information flow.

7.1.6. Accuracy

Information flow control policy

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
ACR_201	FDP_ACC.1/IS FDP_ACF.1/IS FPT_STM.1 for - TOE's real time clock, FDP_ITC.1 for - recording equipment calibration parameters, - user's inputs; FDP_ITC.2//IS for - vehicle motion data; - tachograph cards.	The TOE ensures that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources: – vehicle motion data, – TOE's real time clock, – recording equipment calibration parameters, – tachograph cards, – user's inputs.

	FPT_TDC.1//IS	
ACR_201a	FDP_ACC.1/FUN FDP_ACF.1/FUN	The TOE ensures that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).

Stored data integrity

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
ACR_204	FDP_SDI.2 FCS_COP/SHA1 FCS_COP/TDES	The TOE checks user data stored in the data memory for integrity errors. Provides stored data integrity.
ACR_205	FDP_SDI.2, FAU_GEN.1	Upon detection of a stored user data integrity error, the TSF generates an audit record.

7.1.7. Reliability of Service

Test

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
RLB_201	The property a) is formulated as OSP.Test_Points FMT_MOF.1 for the property b)	a) Organisational part by manufacturer All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE is disabled or removed before the TOE activation. b) TOE cares: It is not possible to restore them for later use.
RLB_202	FPT_TST.1	The TOE runs self tests, during initial start-up, and during normal operation to verify its correct operation. The TOE self tests includes a verification of the integrity of security data and a verification of the integrity of stored executable code
RLB_203	FAU_GEN.1 for an audit record FPT_FLS.1 for preserving	Upon detection of an internal fault during self test, the TSF : • generates an audit record (except in

	the stored data integrity	calibration mode), - preserves the stored data integrity.

Software

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
RLB_204	FPT_PHP.3 and ADV_ARC (self- protection for stored data) FPR_UNO.1 (no successful analysis of leaked data)	There is no way to analyse or debug software in the field after the TOE activation.
RLB_205	FDP_ITC.2//IS with FDP_ACC.1/IS, FDP_ACF.1/IS	Inputs from external sources is not accepted as executable code.

Physical protection

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
RLB_206	FAU_GEN.1 for auditing,	The TOE detects any case opening, except in calibration mode, even without external power supply for a minimum of 6 months. In such a case, the TSF generates an audit record (The audit record is generated and stored after power supply reconnection). TOE is designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).

Power supply interruptions

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
RLB_209	FPT_PHP.2//Power_Deviation for detection	The TOE detects deviations from the specified values of the power supply, including cut-off.

RLB_210	FAU_GEN.1 for auditing FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset (cf. also RLB_203 and RLB_211)	In the case described above, the TSF: • generates an audit record (except in calibration mode), • preserves the secure state of the TOE, • maintains the security functions, related to components or processes still operational, • preserves the stored data integrity

Reset conditions

Requirement, Appendix 10	Related SFR used in the current ST	Security Function Description
RLB_211	FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset	In case of a power supply interruption, or when a transaction is stopped before completion, or on any other reset conditions, the TOE is reset cleanly.

Data availability

Requirement, Appendix 10	Related SFR used in the current ST	Security Function Description
RLB_212	FRU_PRS.1	The TOE ensures that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.
RLB_213	FDP_ACC.1/FUN FDP_ACF.1/FUN with a rule for REQ015 and 016	The TOE ensures that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).
RLB_214	FAU_GEN.1 (Last card session not correctly closed)	In the case described above, the TSF generates an audit record of the event.

Multiple applications

Requirement, Appendix 10	Related SFR used in the current ST	Security Function Description
RLB_215	ADV_ARC (domain separation)	TOE does not provide applications other than the tachograph application. So that there is no need for

		physically and/or logically separation.

7.1.8. Data Exchange

Data exchange with motion sensor

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
DEX_201	FDP_ITC.2//IS for – vehicle motion data	The TOE verifies the integrity and authenticity of motion data imported from the motion sensor.
DEX_202	FAU_GEN.1. FDP_ITC.2//IS for – vehicle motion data	Upon detection of a motion data integrity or authenticity error, the TSF shall: • generates an audit record, • continues to use imported data.

Data exchange with tachograph cards

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
DEX_203	FDP_ITC.2//IS for – tachograph cards.	The TOE verifies the integrity and authenticity of data imported from tachograph cards.
DEX_204	FAU_GEN.1 FDP_ITC.2//IS for – tachograph cards	Upon detection of a card data integrity or authenticity error, the TSF: • generates an audit record, • do not use the data.
DEX_205	FDP_ETC.2	The TOE exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

Data exchange with external storage media (downloading function)

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
DEX_206	FCO_NRO.1	The TOE generates an evidence of origin for data downloaded to external media.

DEX_207	FCO_NRO.1	The TOE provides a capability to verify the evidence of origin of downloaded data to the recipient.
DEX_208	FDP_ETC.2	The TOE downloads data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.

7.1.9. Cryptographic support

Requirement, Appendix 10	**Related SFR used in the current ST**	**Security Function Description**
CSP_201	FCS_COP.1/TDES FCS_COP.1/RSA	Any cryptographic operation performed by the TOE is in accordance with a specified algorithm and a specified key size.
CSP_202	FCS_CKM.1	TOE generates 112 bits cryptographic TDES session keys for securing communication between VU and MS
CSP_203	FCS_CKM.2	TOE distributes KSM and KST cryptographic keys to MS
CSP_204	FCS_CKM.3	TOE accesses cryptographic keys in following ways: a) Kmwc: part of the Master key read out from the workshop card and temporarily stored in the TOE (calibration phase); b) Km: temporarily reconstructed from part of the Master key Kmvu and part of the Master key Kmwc as specified in [12], sec. 7.2 and in [10], sec. 3.1.3, CSM_036, CSM_037 (calibration phase); c) KID: temporarily reconstructed from the Master key Km as specified in [12], sec. 7.2, 7.4.3 (calibration phase); d) KP: temporarily reconstructed from Enc(Km|KP) as specified in [12], sec. 7.2, 7.4.3 (calibration phase); e) KSM: internally generated and temporarily stored during a session between the TOE and the motion sensor connected (calibration and operational phases); f) KST: internally generated and temporarily stored during a session between the TOE and the tachograph card connected (calibration and operational phases); g) EUR.PK: stored during manufacturing of the TOE (calibration and operational phases); h) EQTj.SK: stored during manufacturing of the TOE (calibration and operational phases); i) part of the Master key Kmvu: stored during manufacturing of the TOE (calibration and operational

		phases);
CSP_205	FCS_CKM.4	TOE destroys cryptographic keys as specified below: a) Kmwc: delete after use (at most by the end of the calibration phase); b) Km: delete after use (at most by the end of the calibration phase); c) KID: delete after use (at most by the end of the calibration phase); d) KP: delete after use (at most by the end of the calibration phase); e) KSM: delete by replacement (by closing a motion sensor communication session during the next pairing process); f) KST: delete by replacement (by closing a card communication session); g) EUR.PK: this public key does not represent any secret and, hence, needn't to be deleted; h) EQTj.SK: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational; i) part of the Master key Kmvu: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational;

7.1.10. Software Upgrade

DATAKOM DTC-100 performs updates of software in a secure way. If software of TOE have to be updated an authentication with the workshop card is required to allow the update. If the needed authentication was not successfully (FDP_ACC.1/SW-Upgrade) no further checks take place.

The software update mechanism which is implemented in accordance with the SFR FMT_SMF.1/SW-Upgrade ensures that the upgrade is performed only if the integrity and the authenticity of the update package data is confirmed by means of update credentials. TOE can detect manipulated upgrade package and prevent itself for malicious or manipulated upgrade packages.

Further information about Software Upgrade security function is not given in public version of this Security Target.

7.2. Assurance Measures

The section providing a general mapping from the documentation or evidence the developer intends to provide to the appropriate assurance measures is not available in the public version of this Security Target.

7.3. TOE Summary Specification Rationale

7.3.1. Security Functions Rationale

Security Functional Requirements (SFR)- TOE SECURITY FUNCTIONS		Identification and Authentication	Access Control	Accountability	Audit	Object re-use	Accuracy	Reliability of service	Data Exchange	Cryptographic Support	Software Upgrade
FAU_GEN.1	Audit data generation	x		x	x		x	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							
FCO_NRO.1	Selective proof of origin								x		
FCS_CKM.1	Cryptographic key generation									x	
FCS_CKM.2	Cryptographic key distribution									x	
FCS_CKM.3	Cryptographic key access									x	x
FCS_CKM.4	Cryptographic key destruction									x	x
FCS_COP.1/TDES	Cryptographic operation						x			x	x
FCS_COP.1/RSA	Cryptographic operation									x	x
FCS_COP.1/SHA1	Cryptographic operation						x			x	x
FDP_ACC.1/FIL	Subset access control		X								
FDP_ACC.1/FUN	Subset access control	x	x				x	x			
FDP_ACC.1/DAT	Subset access control		x	x	x						
FDP_ACC.1/UDE	Subset access control			x							
FDP_ACC.1/IS	Subset access control						x	x			
FDP_ACC.1/SW_Upgrade	Subset access control							x			x
FDP_ACF.1/FIL	Security attribute based access control		x								
FDP_ACF.1/FUN	Security attribute based access control		x				x	x			
FDP_ACF.1/DAT	Security attribute based access control		x	x	x						

Security Functional Requirements (SFR)- TOE SECURITY FUNCTIONS		Identification and Authentication	Access Control	Accountability	Audit	Object re-use	Accuracy	Reliability of service	Data Exchange	Cryptographic Support	Software Upgrade
FDP_ACF.1/UDE	Security attribute based access control			x							
FDP_ACF.1/IS	Security attribute based access control						x	x			
FDP_ACF.1/SW_Upgrade	Security attribute based access control							x			x
FDP_ETC.2	Export of user data with security attributes			x	x				x		
FDP_ITC.1	Import of user data without security attributes						x				
FDP_ITC.2//IS	Import of user data with security attributes						x	x	x		
FDP_ITC.2/SW Upgrade	Import of user data with security attributes							x			x
FDP_RIP.1	Subset residual information protection					x					
FDP_SDI.2	Stored data integrity monitoring and action						x				
FIA_AFL.1/MS	Authentication failure handling	x									
FIA_AFL.1/TC	Authentication failure handling	x									
FIA_ATD.1//TC	User attribute definition	x									
FIA_UAU.1/TC	Timing of authentication	x									
FIA_UAU.1/PIN	Timing of authentication	x									
FIA_UAU.2//MS	User authentication before any action	x									
FIA_UAU.3/MS	Unforgeable authentication	x									
FIA_UAU.3/TC	Unforgeable authentication	x									
FIA_UAU.5//TC	Multiple authentication mechanisms	x									

Security Functional Requirements (SFR)- TOE SECURITY FUNCTIONS		Identification and Authentication	Access Control	Accountability	Audit	Object re-use	Accuracy	Reliability of service	Data Exchange	Cryptographic Support	Software Upgrade
FIA_UAU.6/MS	Re-authenticating	x									
FIA_UAU.6/TC	Re-authenticating	x									
FIA_UID.2/MS	User identification before any action	x									
FIA_UID.2/TC	User identification before any action	x									
FMT_MSA.1	Management of security attributes	x									
FMT_MSA.3/FUN	Static attribute initialisation	x	x								
FMT_MSA.3/FIL	Static attribute initialisation		x								
FMT_MSA.3/DAT	Static attribute initialisation		x	x	x						
FMT_MSA.3/IS	Static attribute initialisation		x								
FMT_MSA.3/UDE	Static attribute initialisation			x							
FMT_MOF.1	Management of security functions							x			
FMT_SMF.1	Specification of Management Functions	x									
FMT_SMF.1/SW_ Upgrade	Specification of Management Functions										x
FMT_SMR.1//TC	Security roles	x									
FPR_UNO.1	Unobservability							x			
FPT_FLS.1	Failure with preservation of secure state.							x			
FPT_PHP.2//Power_Deviation	Notification of physical attack							x			
FPT_PHP.3	Resistance to physical attack							x			
FPT_STM.1	Reliable time stamps						x				
FPT_TDC.1//IS	Inter-TSF basic TSF data consistency						x				

Security Functional Requirements (SFR)- TOE SECURITY FUNCTIONS		Identification and Authentication	Access Control	Accountability	Audit	Object re-use	Accuracy	Reliability of service	Data Exchange	Cryptographic Support	Software Upgrade
FPT_TDC.1/SW_Upgrade	Inter-TSF basic TSF data consistency							x			x
FPT_TST.1	TSF testing							x			
FRU_PRS.1	Limited priority of service							x			

Table 9Coverage of Security Functional Requirements by TOE Security Functionality

7.3.2. Assurance Measures Rationale

The assurance measures of the developer as referred in sections 6.2 and 7.1.10 are suitable and sufficient to meet the CC assurance level EAL4 augmented by AVA_VAN.5 and ATE_DPT.2 as claimed in section 6.2. In particular, the deliverables listed in chapter 7.1.10 are suitable and sufficient to document that the assurance requirements are met.

8. GLOSSARY AND ACRONYMS

Glossary

Term **Definition**

Activity data Activity data include user activities data, events and faults data and control activity data.

Activity data are part of User Data.

Approved Workshops Fitters and workshops installing, calibrating and (optionally) repairing VU and being under such agreement with a VU manufacturer, so that the assumption A.Approved_Workshops is fulfilled.

Authenticity Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer

Certificate chain Hierarchical sequence of Equipment Certificate (lowest level), Member State Certificate and European Public Key (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level.

Term	Definition
Certification authority	A natural or legal person who certifies the assignment of public keys (for example PK.EQT) to serial number of equipment and to this end holds the licence.
Digital Signature	A digital signature is a seal affixed to digital data which is generated by the private signature key of an entity (a private signature key) and establishes the owner of the signature key (the entity) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.
Digital Tachograph	Recording equipment including a vehicle unit and a motion sensor connected to it.
Digital Tachograph System	Equipment, people or organisations, involved in any way with the recording equipment and tachograph cards.
Equipment Level	At the equipment level, one single key pair (EQTj.SK and EQTj.PK) is generated and inserted in each equipment unit (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQTj.C). This key pair is used for (i) authentication between vehicle units and tachograph cards, (ii) enciphering services: transport of session keys between vehicle units and tachograph cards, and (iii) digital signature of data downloaded from vehicle units or tachograph cards to external media.
	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 ISO 16844-3 [12] 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. See also [14], sec. 5.3.
ERCA policy	The ERCA policy is not a part of the Commission Regulation 1360/2002 and represents an important additional contribution. It was approved by the European Authority on 9 July 2004. 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. See also [14], sec. 5.3.

Term	Definition
European Authority	An organisation being responsible for the European Root Certification Authority policy. It is represented by European Commission Directorate General for Transport and Energy Unit E.1 – Land Transport Policy Rue J.-A. Demot, 24 B-1040 Brussels. The entire Digital Tachograph System is operated in the frame and on the base of the Digital Tachograph System European Root Policy (Administrative Agreement TREN-E1-08-M-ST-SI2.503224) defining the general conditions for the PKI concerned and contains accordingly more detailed information. See also [14], sec. 5.3.
European Root Certification Authority (ERCA)	An organisation being responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment (TP.360) Via E. Fermi, 1 I-21020 Ispra (VA) At the European level, ERCA generates a single European key pair (EUR.SK and EUR.PK). It uses the European private key to certify the Member States` public keys and keeps the records of all certified keys. A change of the European (root) key pair is currently not intended. ERCA also generates two symmetric partial master keys for the motion sensor: Km_{wc} and Km_{vu}. The first partial key Km_{wc} is intended to be stored in each workshop tachograph card; the second partial key Km_{vu} is inserted into each vehicle unit. The final master key Km results from XOR (exclusive OR) operation between Km_{wc} and Km_{vu}. See also [14], sec. 5.3.
Identification data	Identification data include VU identification data. Identification data are part of User data.
Manufacturer	The generic term for a VU Manufacturer producing and completing the VU to the TOE. The Manufacturer is the default user of the TOE during the

Term	Definition
	manufacturing life phase.
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 Km_{wc}, Km_{vu}, motion sensor identification (N_S) and authentication data (K_P) encrypted with K_{ID} and Km, resp., 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. See also [14], sec. 5.3.
Member State *Certification* *Authority (MSCA)*	At the Member State level, each MSCA generates a Member State key pair (MSi.SK and MSi.PK). Member States' public keys are certified by the ERCA (MSi.C). MSCAs use their Member State private key to certify public keys to be inserted in equipment (vehicle unit or tachograph card) and keep the records of all certified public keys with the identification of the equipment concerned. MSCA is allowed to change its Member State key pair. MSCA also calculates an additional identification key Kid as XOR of the master key Km with a constant control vector CV. MSCA is responsible for managing Km_{wc}, Km_{vu}, encrypting motion sensor identification (N_S) and authentication data (K_P) with K_{ID} and Km, respectively, and distributing them to the respective MSA component personalisation services. See also [14], sec. 5.3.
Motion data	The data exchanged with the VU, representative of speed and distance travelled.
Motion Sensor	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled. A MS possesses valid credentials for its authentication and their validity is verifiable.

Term	Definition
	Valid credentials are MS serial number encrypted with the identification key ($Enc(K_{ID}\|N_S)$) together with pairing key encrypted with the master key ($Enc(K_M\|K_P)$)[36]. See also [14], sec. 5.3.
Personal Identification Number (PIN)	A short secret password being only known to the approved workshops.
Personalisation	The process by which the equipment-individual data (like identification data and authentication key pairs for VU and TC 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 vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys), see sec. III.12.2 of [6]. Security data are part of sensitive data.
Sensitive data	Data stored by the recording equipment and by the tachograph cards that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data.

[36] for motion sensor, cf. [12]

Term	Definition
Tachograph cards	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: driver card, control card, workshop card, company card. A tachograph card possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK[37]. See also [14], chap. 2.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable. Valid credentials can be either a certified key pair for authentication of a device[38] or MS serial number encrypted with the identification key ($\mathrm{Enc}(K_{ID}\|N_{S})$) together with pairing key encrypted with the master key ($\mathrm{Enc}(K_{M}\|K_{P})$)[39].
Unknown User	not authenticated user.
Update issuer	An organisation issuing the completed update data of the tachograph application
User	Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card. There can also be Unknown User of the TOE and malicious user of the TOE – an attacker. User identity is kept by the VU in form of a concatenation of User group and User ID, cf. [9], UIA_208 representing security attributes of the role 'User'.

[37] for tachograph cards, cf. [10], sec. 3.1

[38] for tachograph cards, cf. [10], sec. 3.1

[39] for motion sensor, cf. [12]

Term	Definition
User Data	Any data, other than security data (sec. III.12.2 of [6]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [6]. User data are part of sensitive data. User data include identification data and activity data. CC give 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 recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.
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.

Acronyms

Acronym	Term
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher; here of TDES)
CC	Common Criteria
CCMB	Common Criteria Management Board
DES	Data Encryption Standard (see FIPS PUB 46-3)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES)
EQTj.C	equipment certificate
EQTj.PK	equipment public key
$EQT_j.SK$	equipment private key
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
EUR.PK	European public key
GST	Generic Security Target for VU as defined in [9]
K_{ID}	Identification key, will manage the pairing between a motion sensor and the vehicle unit
K_m	Master key, will manage the pairing between a motion sensor and the vehicle unit
K_{mVU}	Part of the Master key stored in the VU, will manage the pairing between a motion sensor and the vehicle unit
K_{mWC}	Part of the Master key stored in the workshop card, will manage the pairing between a motion sensor and the vehicle unit
K_P	Pairing key, will manage the pairing between a motion sensor and the vehicle unit
K_{SM}	Session key between motion sensor and vehicle unit
K_{ST}	Session key between tachograph cards and vehicle unit
MAC	Message Authentication Code
MD	Management Device as defined in [9]
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-

Acronym	Term
	00-12 (DG-TREN))
MSi.C	Member State certificate
n.a.	Not applicable
NCA	National Certification Authority
OSP	Organisational security policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
RAD	Reference Authentication Data
REQxxx	A requirement from [6], whereby ‘xxx’ represents the requirement number.
RTC	Real time clock
SAR	Security assurance requirements
SFP	Security Function Policy (see CC part 2)
SFR	Security functional requirement
ST	Security Target
TC	Tachograph card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
ToSS	TOE Security Service
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
UDI.PK	public key of the update issuer
UDI.SK	private key of the update issuer
VAD	Verification Authentication Data
VU	Vehicle Unit

9. BIBLIOGRAPHY

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance

Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

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

Digital Tachograph: Directives and Standards

[5] Commission Regulation (EC) No 1360/2002 of 13 June 2002adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport

[6] Annex I B of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 77)

[7] Corrigendum to Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Official Journal of the European Communities L 77/71-86,

13.03.2004

[8] Appendix 2 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Tachograph Cards Specification

[9] Appendix 10 of Annex I B of Commission Regulation (EEC) No. 1360/2002 - Generic Security Targets

[10] Appendix 11 of Annex I B of Commission Regulation (EEC) No. 1360/2002 - Common Security Mechanisms

[11] Joint Interpretation Library (JIL): 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

[12] ISO 16844-3:2004 with Technical Corrigendum 1:2006, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface

[13] Digital Tachograph, Specification for remote company card authentication and remote data downloading, Index H, Heavy Truck Electronic Interfaces Working Group – DTCO,

31.01.2008

Additional Sources

[14] Igor Furgel, Kerstin Lemke 'A Review of the Digital Tachograph System', in: Embedded Security in Cars, Springer-Verlag, 2006, ISBN-13 978-3-540-28384-3