Aselsan Digital Tachograph Vehicle Unit (v1.1) Security Target (Lite version)

26.04.2018

HBT-TGD-8250-01

Version 2.6

CONTENT

1. Overview

1.1 Abstract

This document provides the basis for an evaluation of a specific target of evaluation (TOE), Aselsan Digital Tachograph Vehicle Unit (v1.1). This security target (ST) defines a set of assumptions about the operational environment, a list of threats that the product intends to counter, a set of security objective, a set of security requirements and the IT security functions provided by the TOE, which meet the security objectives.

1.2 Document Organization

Section 1	Overview	General document formatting conventions, glossary of terms, tables
Section 2	ST Introduction	Includes an overview and description of the TOE, the hardware and software that make up the TOE, as well as the physical and logical boundaries of the TOE.
Section 3	Conformance Claims	Lists evaluation conformance to Common Criteria versions and applicable Protection Profile and Package.
Section 4	Security Problem Definition	Specifies the assets, threats, assumptions and organizational security policies that effect the TOE.
Section 5	Security Objectives	Defines the security objectives for the TOE and operational environment and rationale illustrating that the security objectives mitigate the threats.
Section 6	Extended Components Definition	Details any extended components used in this evaluation.
Section 7	Security Requirements	Describes the functional and assurance requirements for this TOE.
Section 8	TOE Summary Specification	Identifies the IT security functions provided by the TOE and how the assurance requirements are satisfied.

1.3 Document formatting conventions

In this Security Target some notations and conventions which are taken from the Common Criteria v3.1R4 have been used in order to guide the reader. The conventions used for the specification of the functional requirements under the Section 5 are defined in the Section 7.

1.4 List of acronyms and Glossary of terms

1.4.1 Acronyms

AETR	Accord Europeen sur les Transports
CA	Certification Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining (an operation mode of a block cipher; here of TDES)
CC	Common Criteria
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
EQTj.SK	Equipment Private Key
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
GST	Generic security target
K_{ID}	Identification key, manages the pairing between a motion sensor and the vehicle unit
Km	Master key, manages the pairing between a motion sensor and the vehicle unit
Km_{VU}	Part of the Master key stored in the VU, manages the pairing between a motion sensor and the vehicle unit
Km_{WC}	Part of the Master key stored in the workshop card, manages the pairing between a motion sensor and the vehicle unit
K_P	Pairing key, manages 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
MD	Management Device
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))

MSi.C	Member State Certificate
OSP	Organizational Security Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
REQxxx	A requirement from [6], whereby 'xxx' represents the requirement number.
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policies
VU	Vehicle Unit

1.4.2 Glossary of terms

The following terminology is used in this Security Target (ST).

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

Activity data are part of User Data.

Application note: Optional informative part of the PP containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.

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 level is signed with the private key corresponding to the public key in the certificate of the next higher level.

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 (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.

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.ec.europa.eu.

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.

European Authority: An organisation being responsible for the European Root Certification

Authority policy. It is represented by

European Commission

Directorate General for Mobility and Transport

B – 1049 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.

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

European Commission – Joint Research Centre,

Institute for the Protection and Security of the Citizen,

Digital Citizen Security Unit,

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 K_m results from XOR (exclusive OR) operation between Km_{wc} and Km_{vu}.

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 manufacturing life phase. The manufacturer of the VU within this Security Target is ASELSAN and unless it is explicitly stated the term manufacturer means “ASELSAN”.

Member State

Each Member State of the European Union establishes its own national

Authority (MSA): 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 K_m, 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.

Turkey implements the Digital Tachograph System as a non-EU AETR Contracting Party according to Digital Tachograph System Turkish Authority Policy (TR-A Policy) approved by ERCA. TR-A Policy is available from the web site http://staum.tobb.org.tr. AETR is European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport concluded at Geneva on 1 July 1970. The term Member State is used to refer to non-EU AETR Contracting Party along this document while the MSA policy refers to the TR-A Policy.

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 K_{id} as XOR of the master key K_m 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 K_m, respectively, and distributing them to the respective MSA component personalisation services.

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.

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 ($Enc(K_M|K_P)$).

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.

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).

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.

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.

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 or MS serial number encrypted with the identification key ($Enc(K_{ID}|N_S)$) together with pairing key encrypted with the master key ($Enc(K_M|K_P)$).

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'.

User Data: Any data, other than security data 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.

2. ST Introduction

This document contains a description of the TOE (ASELSAN STC-8250A v1.1), the threats it must be able to counteract and the security objectives it must achieve. It specifies the security requirements. It states the claimed minimum resistance against attacks of security functional requirements and the required level of assurance for the development and the evaluation.

This security target is based on the Vehicle Unit Generic Security Target [9].The document states the security objectives on the environment and describes how they are implemented in the TOE.

For clarity of reading, duplication sometimes arises between Annex IB [6] main body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex IB [6] main body requirement referred by this security target requirement, the Annex IB main body requirement shall prevail.

Annex IB [6] main body requirements not referred by this security target are not the subject of security certification.

The VU general characteristics, functions and mode of operations are described in Chapter II of Annex IB [6]. The VU functional requirements are specified in Chapter III of Annex IB [6].

2.1 ST Reference and TOE Reference

ST Title:	Aselsan Digital Tachograph Vehicle Unit (v1.1) Security Target (Lite Version)
ST Version:	v2.6
ST Release Date:	26.04.2018
TOE Developer	Aselsan A.Ş.
TOE Identification:	Aselsan STC-8250A
TOE Version	v1.1
TOE SW Version	0.8.3
OMAP SW file name	avu-omap-0_8_3_0dpl-0_0_102_signed
ARM SW file name	avu-arm-0_8_3_0dpl-svn2746-20171018
DSP SW file name	AVU_DSP_0_0_102
MSP SP SW file name	avu-msp-0_0_195_63_rls
MSP PP SW Version	avu-msp_pp-0_5_0
TOE HW Version	5820-8250-0001S_RevA
Base Card (TBK)	5999-9945-9002S_RevB
Processor Card (MPK_PRD)	5999-9945-9001_RevB
Processor Card Covers(CR TOP)	5999-0045-9004_RevB
Processor Card Covers(CR BOTTOM)	5999-0045-9005_RevB

Processor Frame Top (FRMT)	5999-0045-9006_RevB
Processor Card Frame Bottom (FRMB)	5999-0045-9007_RevB
Front Panel Card (OPK)	5999-9945-9003S_RevA
Mechanics (MEC)	6009-0045-9006_RevB (Front cover) 5999-9045-9008_RevB (Bottom cover) 5999-9045-9009_RevB (Top cover)

CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R4
Keywords:	Digital Tachograph, Vehicle Unit, Transport Vehicle, Security Target Lite

2.2 TOE Overview

2.2.1 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 IB [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 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 block diagram of the TOE is depicted in Figure 1 (it is noted that although the printer mechanism is part of the TOE, the paper document once produced is not).

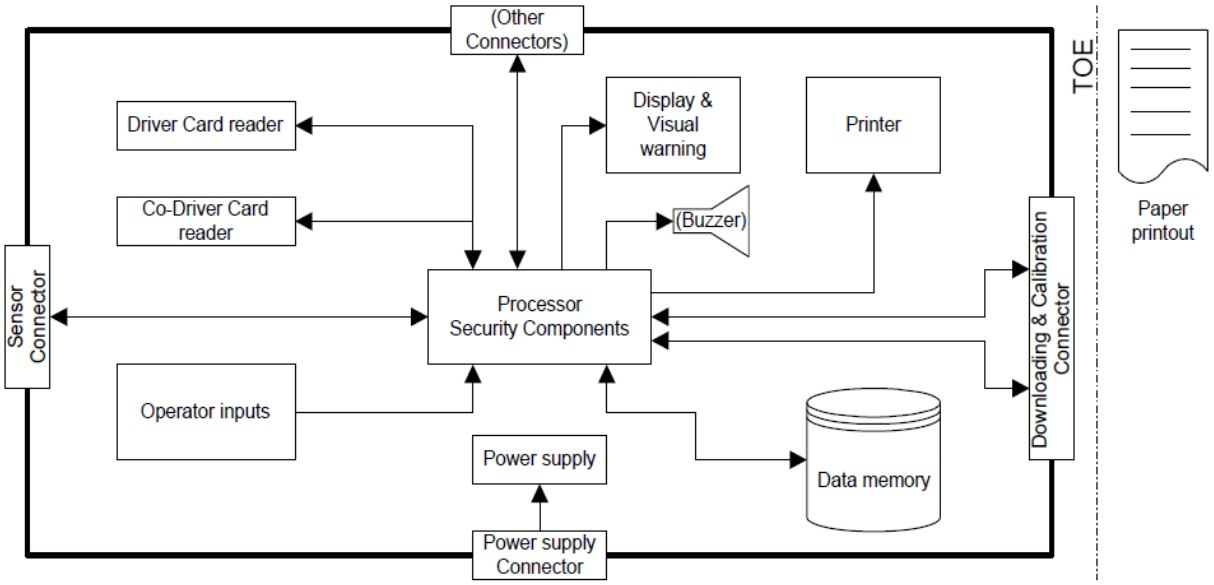

Figure 1: Block Diagram of the TOE

2.2.2 TOE Major Security Features for Operational Use

The main security feature of the TOE is as specified in [9][1]: The data to be measured[2] 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,

[1] O.VU_Main
[2] in the sense 'collected'; the physical data measurement is performed by the motion sensor and the motion sensor is not part of the current TOE.

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.
e) Integrity, authenticity and confidentiality of software upgrade.

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

(please refer to [9], chap.4)

a) Identification and authentication of motion sensor, and 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),
i) Secure software upgrade.

Application Note 1: At least two services listed above – "Identification and authentication" as well as "data exchange" require cryptographic support according to [10], sec.4.9.

2.2.3 TOE Type

The TOE type "ASELSAN STC-8250A v1.1" is a Vehicle Unit (VU) in the sense of Annex IB [6].

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

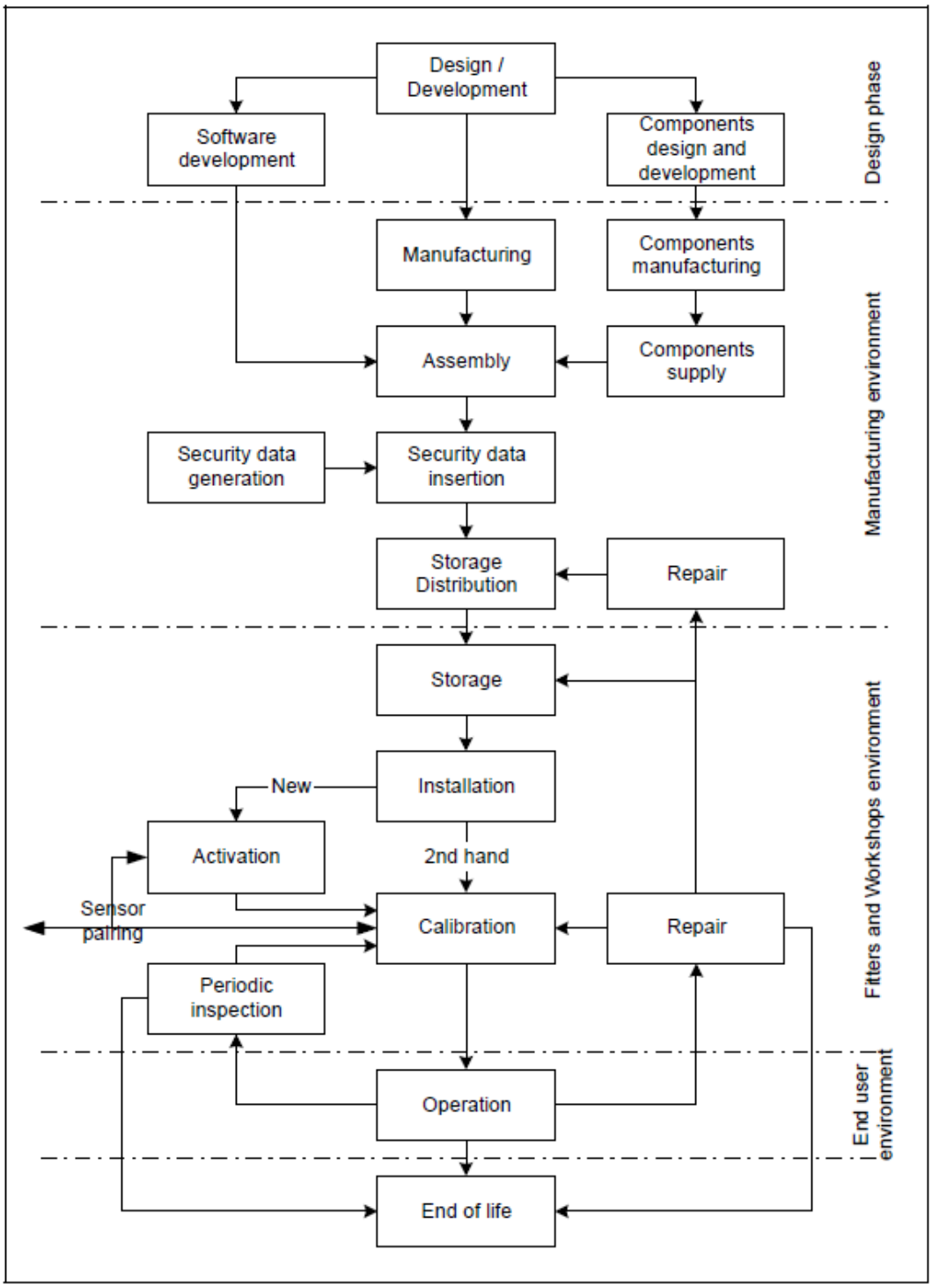

Figure 2: TOE Life Cycle

Application Note 2: The security requirements in sec. 4 of [9] limit the scope of the security examination of the TOE to the *operational phase* in the end user environment. Therefore, the security policy defined by the current ST also focuses on the operational phase of the VU in the end user environment. Some single properties of the *calibration phase*[3] being significant for the security of the TOE in its *operational phase* are also considered by the current ST as required by [9]. The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [6], REQ007 and REQ010: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU.

A security evaluation/certification involves all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 3.2.2 'Package Claim' below). The TOE delivery from its manufacturer to the first customer (approved workshops) exactly happens at the transition from the manufacturing to the calibration phase.

There is no plan for repairing or changing components of the TOE in the fitters or the workshops. The only exceptions that can be executed in the workshops are;

- battery replacement,
- printer drawer replacement,
- approved software upgrade

for the TOE.

[3] *calibration phase* comprises all operations within the fitters and workshops environment

2.2.4 Non-TOE hardware/software/firmware

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

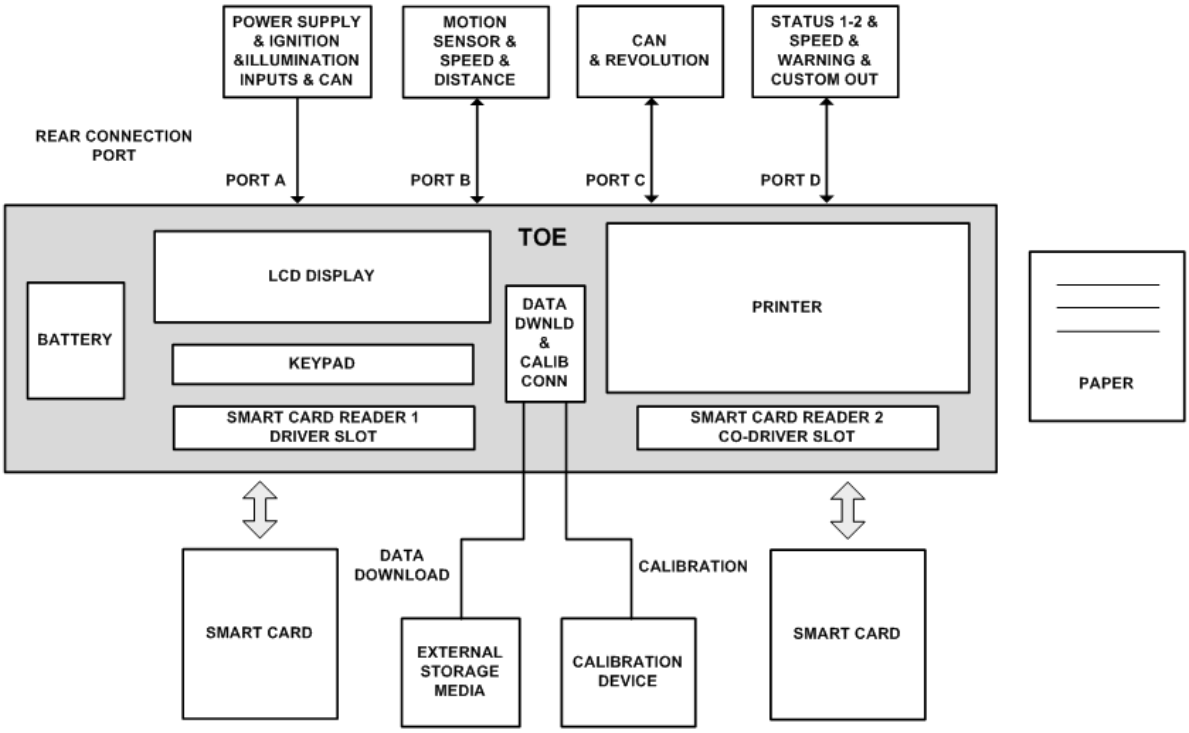

Figure 3: TOE Operational Enviroment

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 IB [6] compliant operation:

- calibration device (fitters and workshops environment only),
- tachograph cards (four different types of them, driver card, workshop card, company card, control card),
- printer paper,
- external storage media for data download.

c) helpful for a convenient TOE operation:

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

Application Note 3: While operating, the TOE will verify, whether the motion sensor and tachograph cards connected possess appropriate credentials showing their belonging to the digital tachograph system. A security certification according to [9] is a prerequisite for the type approval of a motion sensor and tachograph cards.

2.3 TOE Description

2.3.1 Physical Scope

The physical scope of the TOE is Aselsan Digital Tachograph Vehicle Unit (Aselsan STC-8250A v1.1) which is a device 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 manuals.

The TOE 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, software upgrade and diagnostics.

The TOE is delivered to authorized Digital Tachograph workshops and Vehicle Manufacturers together with related manuals according to delivery procedures described in AVU-DEL document. The manuals include a Quick User Guide, a Preparation Manual and an Operation Manual for users, workshops and vehicle manufacturers.

Quick User Guide

This is the printed (hardcopy) document describing summary usage information for all users of the TOE (AVU-QUI-RevA).

Preparation Manual

This is the electronic document (pdf format) describing TOE installation details for workshops (AVU-PRE v0.8.pdf).

Operation Manual

This is the electronic document (pdf format) describing TOE operation for users, workshops and vehicle manufacturers (AVU-OPE v0.7.pdf).

Below figure is a block diagram of the main components and the interfaces of the TOE.

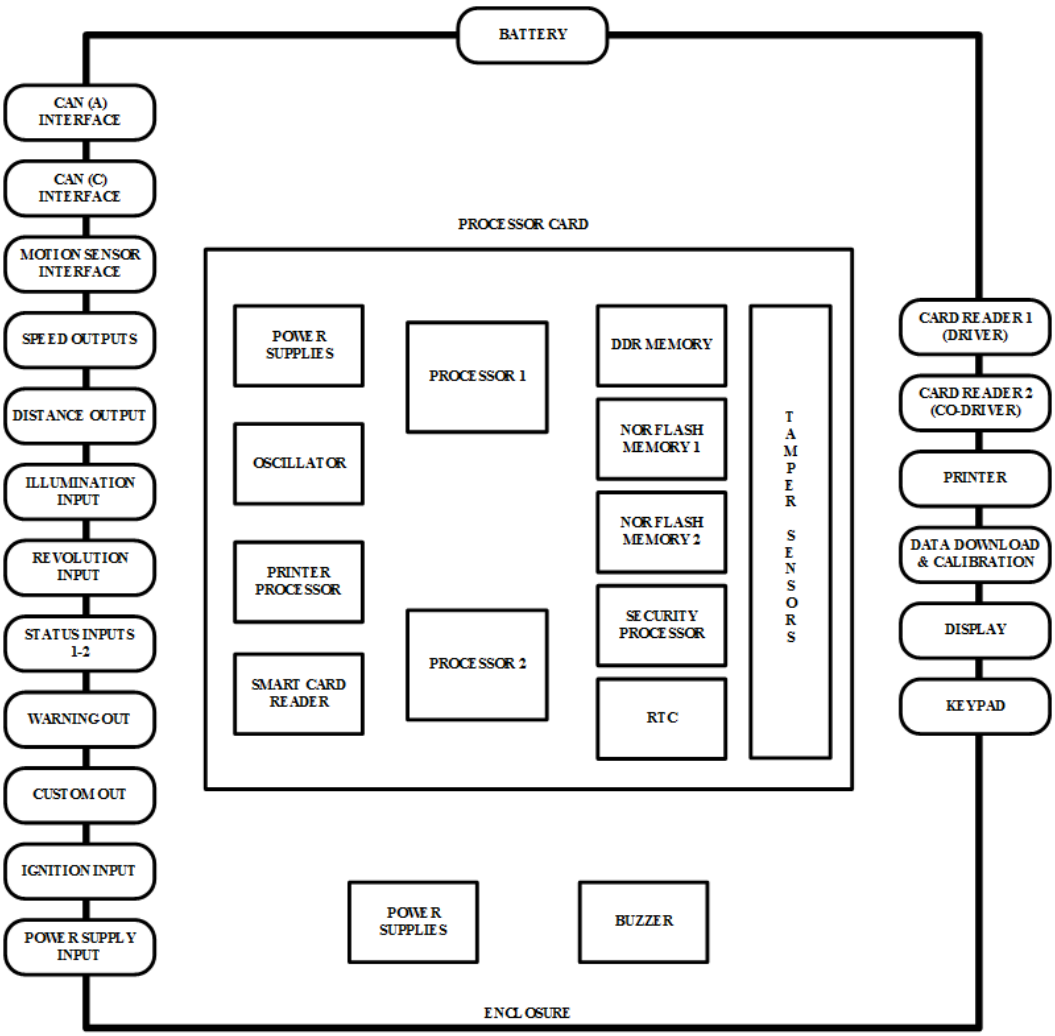

Figure 4: Aselsan Digital Tachograph Vehicle Unit

The following components are in the physical scope of the TOE;

Processor Card is the main processing unit of the TOE. All processors and the peripheral units are on this card. Processor Card is used as the system main controller. Main Processor on this card has System On Chip (SOC) architecture.

Processor1 executes general TOE control and interfacing functions.

Processor2 supports the Security Processor.

Security Processor executes tamper detection functions.

RTC (Real Time Clock) keeps the time information as the reference time source for the operation of the TOE.

Tamper Sensors are the detectors. These electronic circuits are connected to the Security Processor.

Oscillator supplies the clock signal for the operation of the Processors.

Power Supplies on the Processor Card generates local voltages necessary for the operation of the electronics.

DDR Memory is the storage medium for the Processor1.

NOR Flash Memory1 is used for the code storage.

NOR Flash Memory2 is used as the mass storage medium.

Printer Processor serves as a slave to the Processor1. Any data that will be printed is transferred to the Printer Processor which controls the printer interface and the illumination input.

Battery supplies energy for the operation. Battery is replacable and placed in a slot on the enclosure of the VU.

Smart Card Reader is an integrated circuit providing electrical interface between Processor1 and card readers (Card Reader 1 and Card Reader 2).

CAN A Interface is for the interconnection of the TOE to a CAN bus in the vehicle.

CAN C Interface is for the interconnection of the TOE to another CAN bus in the vehicle.

Motion Sensor Interface is the connection port for the Motion Sensor to detect vehicle speed.

Speed Outputs are the indicators of vehicle speed in a pulse width modulated format.

Distance Output is the pulse output to indicate the distance of the vehicle to external cluster displays.

Illumination Input is for acquiring the cabin illumination level.

Revolution Input supplies revolution information of the vehicle to the TOE. This input is nonfunctional.

Status Input 1 and 2 are for the determination of the level for the external contacts. These inputs are non-functional.

Warning Output is for sharing any warning with the external equipments.

Custom Out is a serial output line for communicating with the external equipments.

Ignition Input is for the detection of vehicle ignition status.

Power Supply Input provides the voltage for the operation of the TOE.

Power Supplies generate various level of internal voltages for the correct operation of the TOE.

Card Reader 1 (Driver) is the first connection port for the tachograph cards.

Card Reader 2 (Co-Driver) is the second connection port for the tachograph cards.

Printer is the interface to print reports.

Data Download & Calibration is the interface for calibration and data downloading.

Display is a built in visual output indicator for the user interaction.

Keypad is the input interface for the user interaction.

Buzzer is the sound source to warn user about the situational changes and the events.

Enclosure provides casing to the TOE.

2.3.2 Logical Scope

This section describes the logical security features of the TOE.

The logical boundary of the TOE is broken down into the following security classes which are further described in sections 7.1 (Security Functional Requirements) and 8 (TOE Summary Specification) of this ST.

TOE Security Function	Description
Security Audit	The TOE records 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, hardware sabotage), last card session not correctly closed error, motion data error event, power supply interruption event and the TOE internal fault which affect the security of the TOE. The TOE enforces audit records storage rules and also stores audit records generated by the motion sensor in its data memory. The audit records can be reviewed on TOE display, printed by the TOE printer and downloaded to an external media.
Cryptographic Support	The TOE performs cryptographic operations and supports functions for the generation, distribution, access and destruction of cryptographic keys
User Data Protection	The TOE manages and checks access control rights to functions and to data. It enforces mode of operation selection rules. After the TOE activation, only in calibration mode, may calibration and time adjustment functions be accessed. The TOE checks user data in the data memory for integrity errors. Tachograph cards can not be released before relevant data stored to them. The TOE verifies the integrity and authenticity of data imported from the tachograph cards. The TOE exports data to tachograph cards and to external media with associated security attributes such that the card or the external media is able to verify its integrity and authenticity.
Identification & Authentication of Motion Sensor and Tachograph Cards	The TOE enforces identification and authentication of the motion sensor and the tachograph cards.The TOE requires workshops to be authenticated through a PIN check. Before allowing any interaction, the TOE authenticates the management device.
Security Management	All commands, actions or test points, specific to the testing needs of the manufacturing phase is disabled and removed before the TOE activation. It is not possible to restore them for later use. There is no way to analyze or debug the software in the field after the TOE activation. All processors are protected by a hardware implementation, and any attempt to reach them is detected as hardware sabotage. Moreover, all inputs from external sources are not accepted as executable code. Only the program upgrade is accepted to upgrade the software after checking its signature.
Protection of the TSF	The TSF preserves a secure state upon detection of an internal fault during self test. The VU detects deviations from the specified values of the power supply, including cut-off. In case of a power supply interruption, or if a transaction is stopped before completion, or on any

TOE Security Function	Description
	other reset conditions, the VU resets cleanly.
Communication	An evidence of origin is generated for data downloaded to external media. The TOE provides a capability to verify the evidence of origin of downloaded data to the recipient by relating the TOE identity of the information and the data to be downloaded to external media to which the evidence applies. Data signature is generated for the verification of the evidence of origin of information to the recipient by following PKCS1.
Privacy	TOE is designed so that its users are unable to observe the cryptographic operations using any TOE external interface in order to gain the values of cryptographic keys being to keep secret.
Resource utilization	TOE is designed so as to ensure that its resources required for the functions and data covered by the SFRs is obtained when required and that resources are not requested nor retained unnecessarily.

3. Conformance Claims

3.1 CC Conformance Claim

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 Components; 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.

3.2 PP and Package Claim

3.2.1 Protection Profile (PP) Claim

This Security Target claims conformance to 'Protection Profile Digital Tachograph-Vehicle Unit (VU-PP)', BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik [13].

> *Application Note 4:* This vehicle unit ST covers all requirements of the vehicle unit generic ITSEC ST as contained in [9]. The coverage of the requirements of [9] by the security functional requirements of the current ST is stated in Annex A, chap. 11 of this security target.

3.2.2 Package Claim

This Security Target is conformant to the following security requirements package:

- Assurance package E3hCC31_AP as defined in section 7.3.3.

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. 7.3.3).

3.3 Conformance Rationale

The type of TOE defined in this ST is a Vehicle Unit in the sense of Annex IB [6] and strictly compliant with the TOE type defined in the PP [13] which is claimed in the section 3.2.1.

4. Security Problem Definition

4.1 Assets

4.1.1 Primary Assets

The primary assets to be protected by the TOE are described in the following table. Please refer to the sec. 1.6 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 TOE, 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.

[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 an external medium shall always be protected.

4.1.2 Secondary Assets

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

Object No.	Secondary Asset	Description	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 key for communication with MS (K_{mVU}), see [10], sec.3.1.3, -session key between motion sensor and vehicle unit K_{SM} (see [12], sec. 7.4.5 (instruction 42)), -session key between tachograph cards and vehicle unit K_{ST} (see [10], sec 3.2) **-Software upgrade keys** **-Secure boot keys**	Confidentiality Integrity
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	**Main Processor Software**	**Upgradable software components**	**Confidentiality** **Integrity** **Authenticity**

Table 2: Secondary Assets

Application Note 5: The workshop tachograph card requires an additional human user authentication by presenting a correct PIN value to the card. The vehicle unit (i) transmits the PIN verification value input by the user to the card and (ii) receives the card response to this verification attempt. A workshop tachograph card can only be used within the fitters and workshops environment (see A.Card_Availability below), which is presumed to be trustworthy (see A.Approved_Workshops below). Hence, no threat agent is presumed while using a workshop tachograph card. In this context, the VU is not required to secure a PIN verification value and any card response to a verification attempt, cf. [10], chap. 4.

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

4.2 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	3	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 ($Enc(K_{ID}\|N_S)$) together with pairing key encrypted with the master key ($Enc(K_m\|K_P)$)
4	-	Tachograph	Smart cards intended for use with the recording equipment.

External Entity No.	Subject No.	Role	Definition
		Card	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 ($Enc(K_{ID}\|N_S)$) together with pairing key encrypted with the master key ($Enc(K_m\|K_P)$)
6	-	Attacker	see item User above.

Table 3: Subjects and External Entities

*Application Note 6:*This table defines the subjects in the sense of [1] which can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

4.3 Subjects, objects, and access rights

In this section access rights of TOE users and its external entities on the objects described for TOE are summarised below.

4.3.1 Subjects

S1 entities:

S1.1 tachograph cards

S1.2 downloading equipment

S1.3 calibration device

S1.4 motion sensor

S1.5 management device

S2 users:

S2.1 drivers and co-drivers

S2.2 workshop staff, fitters and staff of vehicle manufacturers

S2.3 control officers from national control authorities

S2.4 staff of the respective haulage company

S2.5 unknown

4.3.2 Objects

1. VU identification
2. Currently paired motion sensor ID
3. Driver card insertion and withdrawal data
4. Driver activity data
5. Places where daily work periods start and/or end
6. Odometer data
7. Detailed speed data
8. Events data
9. Faults data
10. Calibration data
11. Time adjustment data
12. Control activity data
13. Company locks data
14. Download activity data
15. Specific conditions data
16. PIN from workshop card
17. European public key EUR.PK
18. Member state certificate $MS_i.C$
19. Equipment certificate $EQT_j.C$ includes equipment public key $EQT_j.PK$
20. Equipment private key $EQT_j.SK$
21. Part of the Master key Km_{vu}
22. Software upgrade keys K_{Enc_SW} and PK_{Auth_SW}
23. Session key between motion sensor and vehicle unit K_{sm}
24. Session key between tachograph cards and vehicle unit K_{st}
25. Secure boot keys K_{Enc_DSP} and $K_{Enc\_STORAGE}$
26. Part of the master key read out from the workshop card Km_{wc}
27. K_m : temporarily reconstructed from part of the master key Km_{VU}
28. K_{ID} : motion sensor identification key, temporarily reconstructed from the master key K_m
29. K_P : Temporarily reconstructed from $Enc(K_m|K_P)$

4.3.3 Access Rights

Record Name(Objects)	Subjects									
	Entities					Users				
	S1.1	S1.2	S1.3	S1.4	S1.5	S2.1	S2.2	S2.3	S2.4	S2.5
VU identification					W(once)	R	R	R	R	R
Currently paired motion sensor ID				W		R	R	R	R	R
Driver card insertion and withdrawal data						R/W	R/W	R/W	R/W	
Driver activity data	R					R/W	R/W	R	R	R/W
Places where daily work periods start and/or end	R					R/W	R/W	R	R	R/W
Odometer data						R/W	R/W	R/W	R/W	R/W
Detailed speed data						R/W	R/W	R/W	R/W	W
Events data	R					R/W	R/W	R/W	R/W	R/W
Faults data	R					R/W	R/W	R/W	R/W	R/W
Calibration data	R		R/W			R	R/W	R	R	R
Time adjustment data	R		R/W			R	R/W	R	R	R

Control activity data	R					R	R	R/W	R	R
Company locks data	R					R	R	R	R/W	R
Download activity data	R	R				R	R/W	R/W	R/W	R
Specific conditions data	R					R/W	R/W	R/W	R/W	R/W
PIN from workshop card	W						W			
European public key EUR.PK					W(once)	U	U	U	U	
Member state certificate MS_i.C					W(once)	U	U	U	U	
Equipment certificate $EQT_j.C$ includes equipment public key $EQT_j.PK$					W(once)	U	U	U	U	
Equipment private key $EQT_j.SK$					W(once)	U	U	U	U	
Part of the Master key Km_{vu}					W(once)	U	U	U	U	
Software upgrade keys K_{Enc_SW} and PK_{Auth_SW}					W(once)		U			

Session key between motion sensor and vehicle unit K_{sm}				G/U		G/U	G/U	G/U	G/U	
Session key between tachograph cards and vehicle unit K_{st}	G/U					G/U	G/U	G/U	G/U	
Secure boot K_{Enc_DSP} and $K_{Enc\_STORAGE}$						U	U	U	U	U
Part of the master key read out from the workshop card Km_{wc}							U			
K_m : temporarily reconstructed from part of the master key Km_{VU}							U			
K_{ID} : motion sensor identification key, temporarily reconstructed from the master key K_m							U			
K_P : Temporarily reconstructed from Enc(K_m|K_P)							U			

R = read; W = write; G = generate, U = use

4.4 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 threats are identical to those given in [9] chapter 3.3.

Threats averted solely by the TOE:

T.Card_Data_Exchange	Users could try to modify user data while exchanged between TOE and tachograph cards (addition, modification, deletion, replay of signal).
T.Faults	Faults in hardware, software, communication procedures could place the TOE in unforeseen conditions compromising its security[6].
T.Output_Data	Users could try to modify data output (print, display or download).

Threats averted by the TOE and its operational environment:

T.Access	Users could try to access functions[6] not allowed to them (e.g. drivers gaining access to calibration function).
T.Calibration_Parameters	Users could try to use miscalibrated equipment[6] (through calibration data modification, or through organisational weaknesses).
T.Clock	Users could try to modify internal clock[6].
T.Design	Users could try to gain illicit knowledge of design[6] either from manufacturer's material (through theft, bribery, etc.) or from reverse engineering.
T.Environment	Users could compromise the TOE security[6] through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, etc.).
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 TOE 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].
T.Power_Supply	Users could try to defeat the TOE security objectives[6] by modifying (cutting, reducing, increasing) its power supply.

[6] The terms 'miscalibrated equipment', 'TOE security', 'TOE security objectives', 'data output', 'not allowed functions', 'TOE in a well defined state', 'TOE design', 'correctness of the internal clock', 'integrity of the TOE hardware', 'integrity of the TOE software', 'full activated security functionality of the TOE' 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.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 TOE software[6].
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 TOE security[6].

Application Note 7: Threat T.Faults represents a 'natural' flaw not induced by an attacker; hence, nothreat agent can be stated here.

The threat agent for T.Tests is User. It can be deduced from the semantic content of T.Tests.

Threats averted solely by the TOE's operational environment:

T.Non_Activated	Users could use non-activated equipment[6].

4.5 Organizational Security Policies

The TOE and/or its environment must 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.

4.5.1 OSPs related to the TOE:

OSP.Accountability	The TOE must collect accurate accountability data.
OSP.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
OSP.Processing	The TOE 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 TOE must be disabled or removed before the TOE activation during the manufacturing process.

4.5.2 OSPs related to the TOE and its operational environment:

OSP.Type_Approved_MS[12]	The TOE only operates together with a motion sensor being type

[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'

approved according to Annex IB [6].

OSP.Management_Device **The Management Device (MD) supports the appropriate communication interface with the VU and secures the relevant secrets inside the MD as appropriate.**

4.5.3 OSPs related to the TOE's operational environment:

OSP.PKI

1) The European Authority establishes 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 properly operates the ERCA steering other levels (the Member State and the equipment levels) of the PKI.
2) The ERCA securely generates 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 ensures that it issues MSi.C certificates only for the rightful MSCAs.
4) The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs securely generates their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
6) MSCAs ensures that they issue EQTj.C certificates only for the rightful equipment.

OSP.MS_Keys

1) The European Authority establishes 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 properly operates the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure.
2) The ERCA securely generates both parts (K_{mVU} and K_{mWC}) of the master key (K_m).
3) The ERCA ensures that it securely convey this key material only to the rightful MSCAs.
4) The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs securely calculates 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

[12] The identity data of the motion sensor (serial number N_S) will be sent to the VU on request by the MS itself (see instruction #40 in [12]). The 'certificate' $Enc(K_{ID}|N_S)$ stored in the motion sensor is merely used by it for VU authentication, but not for verifying N_S by the VU (see instruction #41 in [12]). Therefore, the VU accepts this data (serial number N_S) 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.

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.

4.6 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, etc.)[16]
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated. Inspection personal is educated about the security check points of the TOE.

[13] to the motion sensors
[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 Comission Regulation [5]). This assumption is made in the current ST only for the sake of compatibility with the GST [9] and is necessary from functional point of view.

5. Security Objectives

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

5.1 Security Objectives for the TOE

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 controls user access to functions and data.
O.Accountability	The TOE collects accurate accountability data.
O.Audit	The TOE audits attempts to undermine system security and should trace them to associated users.
O.Authentication	The TOE authenticates users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The TOE maintains stored data integrity.
O.Output	The TOE ensures that data output reflects accurately data measured or stored.
O.Processing	The TOE ensures that processing of inputs to derive user data is accurate.
O.Reliability	The TOE provides a reliable service.
O.Secured_Data_Exchange	The TOE secures data exchanges with the motion sensor and with tachograph cards.
O.Software_Analysis[17]	There is no way to analyse or debug software[18] in the field after the TOE activation.
O.Software_Upgrade	**The TOE must ensure authenticity, integrity and confidentiality of the software to be installed during software upgrade.**

5.2 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.

[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.

5.2.1 Design environment (cf. the life cycle diagram in Figure 2 above)

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

5.2.2 Manufacturing environment

OE.Manufacturing	The TOE manufacturer ensures that the assignment of responsibilities during manufacturing is done in a manner which main-tains IT security and that during the manufacturing process the TOE is protected from physical attacks which might compromise IT security.
OE.Sec_Data_Generation	Security data generation algorithms are accessible to authorised and trusted persons only.
OE.Sec_Data_Transport	Security data is generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.
OE.Delivery	The TOE manufacturer , vehicle manufacturers and fitters or workshops ensure that handling of the TOE is done in a manner which maintains IT security.
OE.Software_Upgrade	Software revisions are granted security certification before they can be implemented in the TOE.
OE.Sec_Data_Strong[19]	Security data inserted into the TOE is 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 TOE are disabled or removed before the TOE activation by the manufacturer during the manufacturing process.
OE.Management_Device	**The TOE is personalized by the Management Device (MD). MD signs and encrypts the Main Processor software as well as the personalization file before being loaded into the VU.**

[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].

Application Note 10: Please note that the design and the manufacturing environments are not the intended usage environments for the TOE (cf. the Application Note 2 above). The security objectives for these environments being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test_Points, OE.Delivery) are the subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing environments do not address any potential TOE user and, therefore, cannot be reflected in the documents of the assurance class AGD. The remaining security objectives for the manufacturing environment (OE.Sec_Data_Generation, OE.Sec_Data_Transport, OE.Sec_Data_Strong and OE.Software_Upgrade) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

5.2.3 Workshops environment

OE.Activation	Vehicle manufacturers and fitters or workshops 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 carry by trusted and approved fitters or workshops.
OE.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.

5.2.4 End-user environment

OE.Card_Availability	Tachograph cards are available to TOE users and delivered by Member State Authorities to authorised persons only.
OE.Card_Traceability	Card delivery is traceable (white lists, black lists), and black lists are used during security audits.
OE.Controls	Law enforcement controls is performed regularly and randomly, and includes security audits.
OE.Driver_Card_Uniqueness	Drivers possess, at one time, one valid driver card only.
OE.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, etc.).
OE.Regular_Inspections	Recording equipment is periodically inspected and calibrated.
OE.Type_Approved_MS	The Motion Sensor of the recording equipment connected to the TOE is type approved according to Annex IB [6].

5.3 Security Objectives 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].

	Threats																	OSPs								Assumptions								
		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.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Fatihful_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														

	Threats																	OSPs								Assumptions								
		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.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Fatihful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
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								X										
OE.Development					X												X																		
OE.Manufacturing				X	X																														
OE.Sec_Data_Generation																X								X	X										
OE.Sec_Data_Transport																X								X	X										

	Threats																	OSPs								Assumptions								
		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.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Fatihful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
OE.Delivery													X																					
OE.Software_Upgrade																X	X	X																
OE.Sec_Data_Strong																X								X	X									
OE.Test_Points																						X												
OE.Management_Device																										X								
OE.Activation	X												X														X								
OE.Approved_Workshops						X		X					X															X					X		
OE.Faithful_Calibration						X		X																									X		

	Threats																	OSPs								Assumptions							
		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.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Fatihful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
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_Drivers																																		X	
OE.Regular_Inspections						X		X		X	X	X	X		X		X																		X
OE.Type_Approved_MS										X		X											X												

Table 4: Security Objectives Rationale

The rationales for the mapping in the above table are given below.

5.3.1 Rationale for Threats

T.Access is addressed by O.Authentication to ensure the identification of the user, O.Access to control access of the user to functions, O.Audit to trace attempts of unauthorised accesses, OE.Activation to ensure access of the relevant users to relevant functions of the TOE.

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 activities carried (even without an identification) with the TOE. 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 well-known 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 to ensure that data output reflects accurately data measured or stored. Also the security objective O.Reliability makes it difficult for the user to gain information about the design of the TOE by reverse engineering.

T.Calibration_Parameters is addressed by O.Access to ensure that the calibration function is accessible to workshops only, O.Authentication to ensure the identification of the workshop, O.Processing to ensure that processing of inputs made by the workshop to derive calibration data is accurate, 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 TOE, which helps addressing the threat as well.

T.Card_Data_Exchange is countered by the combination of the security objectives O.Audit, O.Secured_Data_Exchange and O.Reliability. The security objective O.Secured_Data_Exchange secures the data exchange between the TOE and the tachograph card, such that modifications of the data are detected, in which case by the security objective O.Audit modifications of exchanged data are audited by the TOE. With O.Reliability data are exchanged by reliable services.

T.Clock is addressed by the security objectives; O.Access, O.Authentication, O.Processing, OE.Approved_Workshops, OE.Regular_Inspections, OE.Faithful_Calibration and OE.Controls. O.Access ensures that the full time adjustment function is accessible to workshops only, O.Authentication ensures the identification of the workshop, O.Processing ensures that processing of inputs made by the workshop to derive time adjustment data is accurate. Workshops are approved by Member State 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 TOE, which helps addressing the threat.

T.Environment is addressed by O.Processing to ensure that processing of inputs to derive user data is accurate, 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 TOE, which helps addressing the threat.

T.Fake_Devices is addressed by O.Access, O.Authentication, O.Audit, O.Processing, O.Reliability, O.Secured_Data_Exchange. OE.Type_Approved_MS ensures that only motion sensors with correct identification data have the credentials 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 addressed by O.Reliability, O.Output and O.Processing. O.Audit also 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, O.Secured_Data_Exchange, OE.Regular_Inspections and 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 also helps addressing the threat through installations, calibrations, checks, inspections and 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 and OE.Controls. It is also addressed by the O.Access, O.Processing, O.Secured_Data_Exchange to ensure appropriate protection while stored in the VU. O.Reliability is relevant here as well.

T.Software is addressed in the user environment by O.Output, O.Processing, O.Reliability and O.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 manufacturing, the threat is addressed by the OE.Development. 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 must 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.

5.3.2 Rationale for Operational Security Policies

OSP.Accountability is fulfilled by O.Accountability.

OSP.Audit is fulfilled by O.Audit.

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.

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

5.3.3 Rationale for Assumptions

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.

6. Extended Components Definition

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

7. Security Requirements

This Security Target clarifies and adapts the security requirements as given in the Digital Tachograph-Vehicle Unit Protection Profile, BSI-CC-PP-0057, Version 1.0, 13th July 2010 [13].

This part of the Security Target 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 ST author are denoted as underlined text.

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 ST author are denoted by showing as underlined text.

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.

7.1 Security Functional Requirements

The security functional requirements are as derived in the PP [13] which covers the SFRs from the generic security target from [9].

In the following the necessary assignments as foreseen by the PP for the SFRs in the protection profile and the necessary enhancements for software-update functionality are processed. For the software-update functionality, some new SFRs are included.

Each of the below SFRs includes in curly braces {…} a list of SFRs 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 SFR(s) from [9]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

The complete coverage of the SFR(s) from [9] is documented in Annex A, sec. 10 below.

7.1.1 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 ST 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, tachograph cards and management device (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_UID.2/MD: Identification of the Management Device – (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/MD, FIA_UAU.3/MD: Authentication of the Management Device – 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_COP.1/ECDSA: for signature verification of the software update data – (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1)

Security Functional Groups	Security Functional Requirements concerned
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 – 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 – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device – 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)

Security Functional Groups	Security Functional Requirements concerned
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

Security Functional Groups	Security Functional Requirements concerned

Security Functional Groups	Security Functional Requirements concerned
Accuracy of recorded and stored data (according to [9], sec. 4.6)	– 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) – FDP_ITC.2/SW-Upgrade: import of user data with security attributes – FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC) – FDP_SDI.2: Stored data integrity – FPT_TDC.1/SW-Upgrade: capability to ensure the consistency of data for the update – FCS_COP.1/AES: for decryption of the software update data and encryption / decryption of the data transferred between the security processor and the main processor – FCS_COP.1/ECDSA: for sign verification of the software update data Supported by: – FCS_CKM.1/AES: Cryptographic key generation – (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 – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device

Security Functional Groups	Security Functional Requirements concerned
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.2// HW_sabotage : 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

Security Functional Groups	Security Functional Requirements concerned
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/TDES, 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.

7.1.1.1 FAU_GEN Security audit data generation

FAU_GEN.1 Audit 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_208,** 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[21] and {UIA_206, UIA_214, AUD_202, ACR_205, RLB_203, RLB_206, RLB_210, RLB_214[22], DEX_202, DEX_204}; RLB_208.

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 ST, the information specified in {REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, 105a[23]}; none.

7.1.1.2 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.

7.1.1.3 FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage {ACT_206}[24]

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 unauthorised deletion.

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

FAU_STG.4 Prevention of audit data loss {ACT_206}[25]

Hierarchical to: FAU_STG.3

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

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

[21] all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_203}
[22] Last card session not correctly closed
[23] all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_203}
[24] REQ081 to 093 and REQ102 to 105a
[25] REQ 083, 086, 089, 092, 105b; REQ105b is completely covered by ACT_206.

Application Note 17: The data memory is able to hold 'driver card insertion and withdrawal data' (REQ082), 'driver activity data' (REQ085) and 'places where daily work periods start and/or end' (REQ088) for at least 365 days. Since these requirements are not subject to GST [9][26], they are also not included in the formal content of FAU_STG.4.
For same reason, the respective part of requirement for 'specific conditions data' (REQ105b, at least 365 days) is also out of scope of the formal content of FAU_STG.4.

7.1.2 Class FCO Communication

7.1.2.1 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 ST 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.

Application Note 17a: The dependency is justified as the vehicle unit identification data can be downloaded if the technical data from the VU is requested by the Intelligent Dedicated Equipment (IDE) according to DDP_011 [14]. Moreover, according to DDP_054 [14] it is mandatory for the IDE to request the overview data transfer during a download session as this only will ensure that the VU certificates are recorded within the downloaded file (and allow for verification of digital signature). Certificate Holder Reference (CHR) field of the VU certificate includes the serial number of the VU according to CSM_017 [10]. This serial number is part of the permanent identification data as referred to in (ACT_202) and it can be used to trace between technical data and overview data. Hence the dependency of the SFR is interpreted as the fact that the VU always knows its own identity which can be downloaded in the technical data if requested by the download equipment (IDE).

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}.

7.1.3 Class FCS Cryptographic Support

7.1.3.1 FCS_CKM Cryptographic key management

FCS_CKM.1/TDES 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;

[26] ACT_206 does not require keeping data for at least 365 days

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

FCS_CKM.1.1/TDES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm cryptographic key derivation algorithms (for the session keys K_{SM} and K_{ST} 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].

Note: FCS_CKM.1/TDES corresponds to FCS_CKM.1 in the protection profile [13] .

FCS_CKM.1/AES Cryptographic key generation {CSP_202}

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: is fulfilled by FCS_COP.1/AES;

FCS_CKM.4 Cryptographic key destruction: is fulfilled **for $K_{Enc\_STORAGE}$** by FCS_CKM.4 **and not fulfilled, but justified for $K_{Enc\_DSP:}$ The key K_{Enc_DSP} is used for encrypted communication between security processor and main processor. Since the security data shall be destroyed in case of a physical tampering attack, not destructing K_{Enc_DSP} will not cause any vulnerability.**

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Using the Output of a Random Bit Generator (for cryptographic secure boot keys K_{Enc_DSP} and $K_{Enc\_STORAGE}$) and specified cryptographic key sizes 256 bits that meet the following: list of standards:

a) K_{Enc_DSP} , $K_{Enc\_STORAGE}$ key generation algorithms are not made according to any standard.

FCS_CKM.2 Cryptographic key distribution {CSP_203}

Hierarchical to: -

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

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/TDES or FCS_CKM.1/AES]:

a) fulfilled by FCS_CKM.1/TDES for the session keys K_{SM} and K_{ST} as well as for the temporarily stored keys K_m, K_P and K_{ID};
b) fulfilled by FCS_CKM.1/AES for secure boot keys K_{Enc_DSP} ,

$K_{Enc\_STORAGE}$;

c) fulfilled by FDP_ITC.2//IS for the temporarily stored key Km_{wc} (entry DEX_203);

d) not fulfilled, but **justified** for EUR.PK, EQT.SK, Km_{vu}, **K_{Enc_SW}, PK_{Auth_SW}**: The persistently stored keys (EUR.PK, EQTj.SK, Km_{vu}, **K_{Enc_SW}, PK_{Auth_SW}**) 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) Secure boot keys – K_{Enc_DSP} and $K_{Enc\_STORAGE}$: internally generated and permanently stored during during personalization;

k) Software upgrade keys – K_{Enc_SW} and PK_{Auth_SW}: stored during manufacturing of the TOE.

K_{Enc_SW} shall be cryptographic key size of 256 bits that meet the following: [AES], [OFB].

PK_{Auth_SW} shall be cryptographic key size of 192 bits (Curve P-192) that meet the following: [ECDSA], [SHA-256].

FCS_CKM.4 Cryptographic key destruction {CSP_205}

Hierarchical to: -

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

FCS_CKM.4.1 The TSF shall destroy cryptographic key 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) Software upgrade keys – K_{Enc_SW} and PK_{Auth_SW}: 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;
k) Secure boot key – $K_{Enc\_STORAGE}$: will be internally generated and stored during personalization at the end of the manufacturing of 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. $K_{Enc\_STORAGE}$ shall be destroyed in case of a physical tampering attack.

Application Note 18: The component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of temporary or permanent nature. In contrast, the component FDP_RIP.1 concerns in this ST only the temporarily stored instantiations of objects in question. The permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} must not be destroyed as long as the TOE is operational. Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} unavailable at decommissioning the TOE is a matter of the related organisational policy.

7.1.3.2 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/TDES]: is fulfilled by FCS_CKM.1/TDES FCS_CKM.4: is fulfilled by FCS_CKM.4.
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 and [10] for the Tachograph Cards.

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, respectively.

FCS_COP.1/AES Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/AES]: **not fulfilled, but justified for K_{Enc_SW}, K_{Enc_DSP} and $K_{Enc\_STORAGE}$: The persistently stored key K_{Enc_SW} will be loaded into the TOE while K_{Enc_DSP} and $K_{Enc\_STORAGE}$ will be internally generated and stored during personalization at the end of the manufacturing of the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.** FCS_CKM.4: is fulfilled by FCS_CKM.4.
FCS_COP.1.1/AES	The TSF shall perform the cryptographic operations (encryption and decryption) in accordance with a specified cryptographic algorithm AES in OFB mode and cryptographic key size 256 bits that meet the following: [AES], [OFB].

FCS_COP.1/ECDSA Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: **not fulfilled, but justified for PK_{Auth_SW}: The persistently stored key PK_{Auth_SW} 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_COP.1.1/ECDSA	The TSF shall perform the cryptographic operations (signature verification) in accordance with a specified cryptographic algorithm ECDSA using SHA-256 and cryptographic key size 192 bits (Curve P-192) that meet the following: [ECDSA], [SHA-256].

7.1.4 Class FDP User Data Protection

7.1.4.1 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 - subjects: - User. - Motion Sensor. - objects: - application and data files structure as required by ACC_211 - operations: - as defined in FDP_ACF.1.2/FIL

Application Note 19: The current assignment shall cover 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: - User. - Unknown User. - Motion Sensor. - objects: - Vehicle unit identification data (REQ075, REQ076) - currently paired motion sensor identification data (REQ079, REQ 155) - Driver card insertion and withdrawal data (REQ081) - Driver activity data (REQ084) - Places where daily work periods start / end (REQ087) - Odometer data(REQ090) - Detailed speed data (REQ093) - Events data (REQ094, REQ095) - Faults data (REQ096) - calibration data (REQ097, REQ098) - time adjustment data (REQ100, REQ101) - Control activity data (REQ102, REQ103) - Company locks data (REQ104) - Download activity data (REQ105) - Specific conditions data (REQ105a)

-operations:

- as defined in FDP_ACF.1.2/FUN

Application Note 20: The current assignment shall cover 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:
  - User.
  - Motion Sensor.
- objects:
  - VU identification data (REQ075, REQ076)
  - MS identification data (REQ079, REQ 155)
  - calibration data (REQ097, REQ098)
  - time adjustment data (REQ100, REQ101)
  - security data (REQ080)
  - MS Audit Records {AUD_204}
- operations:
  - as defined in FDP_ACF.1.2/DAT

Application Note 21: The current assignment shall cover 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}[27]

as required by ACC_201.

[27] 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_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:
  - User.
- objects:
  - Vehicles used data (REQ197, REQ217)
  - Driver activity data (REQ199, REQ219)
  - Places where daily work periods start / end (REQ202, REQ221)
  - Events data (REQ204, REQ205, REQ223)
  - Faults data (REQ207, REQ208, REQ223)
  - Control activity data (REQ210, REQ225)
  - Card session data (REQ212)
  - Specific conditions data (REQ212a, REQ230a)
  - Calibration and time adjustment data (REQ226, REQ227)
  - Control activity data (REQ233)
- -operations:
  - as defined in FDP_ACF.1.2/UDE

Application Note 22: The current assignment shall cover 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:
  - User.
  - Motion Sensor.
- objects:
  - Data stored on VU memory:
    - Driver card insertion and withdrawal data (REQ081)
    - Driver activity data (REQ084)
    - Places where daily work periods start / end (REQ087)
    - Odometer data(REQ090)

- Detailed speed data (REQ093)
- Control activity data (REQ102, REQ103)
- Company locks data (REQ104)
- Download activity data (REQ105)
- Specific conditions data (REQ105a)

- Data stored on Tachograph cards (REQ109, REQ109a)
- Vehicles used data (REQ197, REQ217)
- Driver activity data (REQ199, REQ219)
- Places daily work periods start/end(REQ202, REQ221)
- Events data (REQ204, REQ205, REQ223)
- Faults data (REQ207, REQ208, REQ223)
- Control activity data (REQ210, REQ225)
- Card session data (REQ212)
- Specific conditions data (REQ212a, REQ230a)
- Calibration and time adjustment data (REQ226, REQ227)
- Control activity data (REQ233)

- SW Upgrade patch

-operations:

- as defined in FDP_ACF.1.2/IS

Application Note 23: The current assignment shall cover 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 updateable software components (Main Processor Software) and User with identity WORKSHOP for upgrades in the Workshop.

7.1.4.2 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: - subjects: - User.

- Motion Sensor.

- security attributes for subject:

- User:

-USER_GROUP

— DRIVER (driver card)

— CONTROLLER (control card)

— WORKSHOP (workshop card)

— COMPANY (company card)

— UNKNOWN (no card inserted)

-USER_ID, composed of:

—card issuing Member State code and of the card number

— UNKNOWN if user group is UNKNOWN

- Motion Sensor:

- serial number

- approval number

- objects:

- application and data files structure as required by ACC_211

- security attributes for objects:

- VU identification data (REQ075)
- Security elements (REQ080)

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.
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}.

Application Note 24: The current assignment in FDP_ACF.1.1 shall cover the entire files structure of the TOE-application 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: - User.

- Unknown User.
- Motion Sensor.

- security attributes for subject:
  - User:
    - USER_GROUP
      - — DRIVER (driver card)
      - — CONTROLLER (control card)
      - — WORKSHOP (workshop card)
      - — COMPANY (company card)
      - — UNKNOWN (no card inserted)
    - USER_ID, composed of:
      - —card issuing Member State code and of the card number
      - — UNKNOWN if user group is UNKNOWN
  - Motion Sensor:
    - serial number
    - approval number
- objects:
  - Vehicle unit identification data (REQ075, REQ076)
  - MS identification data (REQ079, REQ 155)
  - Driver card insertion and withdrawal data (REQ081)
  - Driver activity data (REQ084)
  - Places where daily work periods start / end (REQ087)
  - Odometer data(REQ090)
  - Detailed speed data (REQ093)
  - Events data (REQ094, REQ095)
  - Faults data (REQ096)
  - calibration data (REQ097, REQ098)
  - time adjustment data (REQ100, REQ101)
  - Control activity data (REQ102, REQ103)
  - Company locks data (REQ104)
  - Download activity data (REQ105)
  - Specific conditions data (REQ105a)
- security attributes for objects: mode of operation (REQ006, REQ007, REQ008) and the VU activation status.

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.

Application Note 25: The current assignment in FDP_ACF.1.1 shall cover 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/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:
  - User.
  - Motion Sensor.
- security attributes for subject:
  - User:
    - USER_GROUP
      - — DRIVER (driver card)
      - — CONTROLLER (control card)
      - — WORKSHOP (workshop card)
      - — COMPANY (company card)
      - — UNKNOWN (no card inserted)
    - USER_ID, composed of:
      - —card issuing Member State code and of the card number
      - — UNKNOWN if user group is UNKNOWN
  - Motion Sensor:
    - serial number
    - approval number
- objects:
  - VU identification data (REQ075, REQ076)
  - MS identification data (REQ079, REQ 155)
  - Calibration data (REQ097, REQ098)

- Time adjustment data (REQ100, REQ101)
- Security data (REQ080)
- MS Audit Records {AUD_204}

- security attributes for objects:
  - VU identification data (REQ076)
  - MS identification data:
    - serial number
    - approval number
    - first pairing date
  - Calibration data: CALIBRATION mode of operation
  - Time adjustment data: CALIBRATION mode of operation
  - Security data(REQ080): Software upgrade keys K_{Enc_SW} and PK_{Auth_SW} are used to decrypt and verify the security data (REQ080) which is signed and encrypted before insertion into the VU during the manufacturing phase.
  - MS Audit Records: Audit records from MS is sent to the VU in an encrypted form with session key K_{SM} [12]

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.

Application Note 26: The current assignment shall cover 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}[28].

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

[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.

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:
  - User.
- security attributes for subject:
  - USER_GROUP
    - DRIVER
    - CONTROLLER
    - WORKSHOP
  - USER_ID, composed of:
    - Member State code
    - Card number.
- objects:
  - Vehicles used data (REQ197, REQ217)
  - Driver activity data (REQ199, REQ219)
  - Places daily work periods start / end (REQ202, REQ221)
  - Events data (REQ204, REQ205, REQ223)
  - Faults data (REQ207, REQ208, REQ223)
  - Control activity data (REQ210, REQ225)
  - Card session data (REQ212)
  - Specific conditions data (REQ212a, REQ230a)
  - Calibration and time adjustment data (REQ226, REQ227)
  - Control activity data (REQ233)
- security attributes for objects: Mutual authentication between the VU and the Tachograph card must have been performed (PRO SM / AUT) in order to satisfy the access condition required for the VU to update on the tachograph cards as described in TCS_400, TCS_405 and TCS_410.

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.

Application Note 27: The current assignment shall cover subjects, objects, and as their attributes required by REQ 109 and 109a.

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 the SFP_Input_Sources to objects based on the following: - subjects: - User. - Motion Sensor. - security attributes for subject: - User: -USER_GROUP — DRIVER (driver card) — CONTROLLER (control card) — WORKSHOP (workshop card) — COMPANY (company card) — UNKNOWN (no card inserted) -USER_ID, composed of: —card issuing Member State code and of the card number — UNKNOWN if user group is UNKNOWN - Motion Sensor: - serial number - approval number - objects: - Data stored on VU memory: - Driver card insertion and withdrawal data (REQ081) - Driver activity data (REQ084) - Places where daily work periods start / end (REQ087) - Odometer data(REQ090) - Detailed speed data (REQ093) - Control activity data (REQ102, REQ103) - Company locks data (REQ104) - Download activity data (REQ105) - Specific conditions data (REQ105a) - Data stored on Tachograph cards (REQ109, REQ109a) - Vehicles used data (REQ197, REQ217) - Driver activity data (REQ199, REQ219) - Places daily work periods start/end(REQ202, REQ221)

- Events data (REQ204, REQ205, REQ223)
- Faults data (REQ207, REQ208, REQ223)
- Control activity data (REQ210, REQ225)
- Card session data (REQ212)
- Specific conditions data (REQ212a, REQ230a)
- Calibration and time adjustment data (REQ226, REQ227)
- Control activity data (REQ233)

- SW Upgrade patch

- security attributes for objects:
  - Data stored on VU memory: mode of operation
  - vehicle motion data : pulse counter value.
  - recording equipment calibration parameters:
    CALIBRATION mode of operation
  - user's inputs : time of events entered manually
  - Data stored on Tachograph cards:
    Mutual authentication between the VU and the Tachograph card must have been performed (PRO SM / AUT) in order to satisfy the access condition required for the VU to update on the tachograph cards as described in TCS_400, TCS_405 and TCS_410.
  - SW Upgrade patch:
    - CALIBRATION mode of operation
    - Software upgrade keys K_{Enc_SW} and PK_{Auth_SW}

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 (Especially for MS and TC)}.
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}.

Application Note 28: The current assignment shall cover subjects, objects, and their attributes as required by ACR_201 (right input sources) and RLB_205 (no external executable code).

FDP_ACF.1/SW-Upgrade Security attribute based access control {RLB_205}

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/SW-Upgrade FMT_MSA.3: is fulfilled by FMT_MSA.3/SW-Upgrade
FDP_ACF.1.1/SW-Upgrade	The TSF shall enforce SFP SW-Upgrade to objects based on the following: updateable software components (Main Processor software) may be exchanged if the confidentiality, integrity and the authenticity of the patch

	data is confirmed with help of the update 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 at the workshop is only possible after workshop card authentication, - software upgrade is only possible if the confidentiality, integrity and the authenticity of the patch data is confirmed with help of the update credentials.
FDP_ACF.1.3/SW-Upgrade	The TSF shall explicitly authorise 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 rule: none.

7.1.4.3 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 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.

7.1.4.4 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 {RLB_205}

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**: **The new TOE software to replace the current TOE software, the new TOE software is accepted by the TOE only together with the corresponding credentials, which contain all information needed for verification. That is, the TOE needs first to decrypt and then verify the signature on the new TOE software before allowing it to replace the current TOE software. So, it is not necessary to establish 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 protocol used 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-	The TSF shall enforce the following rules when importing user data

Upgrade	controlled under the SFP from outside the TOE: update of the TOE software is allowed only if the integrity and the authenticity of the new TOE software patch is confirmed with the help of the update credentials.

7.1.4.5 FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {REU_201}

Hierarchical to: -

Dependencies: -

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a **temporarily stored** resource is made unavailable upon the *deallocation of the resource from* 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) Software upgrade keys – K_{Enc_SW} and PK_{Auth_SW} (at most by the end of the software update).
k) Secure boot key – $K_{Enc\_STORAGE}$ (at most by the end of secure boot)

Application Note 29: The component FDP_RIP.1 concerns in this ST only the temporarily stored (e.g. in RAM) instantiations of objects in question. In contrast, the component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of temporary or permanent nature. Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} unavailable at decommissioning the TOE is a matter of the related organisational policy.

Application Note 30: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMSEC. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

7.1.4.6 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.

Application Note 31: The context for the current SFR is built by the related requirements ACR_204, ACR_205 (sec. 4.6.3 of [9] 'Stored data integrity'). This context gives a clue for interpretation that it is not a matter of temporarily, but of permanently stored user data (

see definition in glossary).

7.1.5 Class FIA Identification and Authentication

7.1.5.1 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 2 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.

*Application Note 32:*The positive integer number expected above shall be ≤ 20, cf. UIA_206 in [9].

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 (is commensurate with 'Unknown equipment' in the current ST) (definition (z) and REQ007).

7.1.5.2 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}.

7.1.5.3 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 of the user to be performed before the user is authenticated.

(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.)

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

(The PIN-based authentication is applicable for the workshop cards, whose identification is ruled by FIA_UID.2/TC.)

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.

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

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.1/MD Timing of authentication {UIA_222}

Hierarchical to: -

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

FIA_UAU.1.1/MD The TSF shall allow MD identification as required by FIA_UID.2.1/MD on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/MD 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}.

(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.)

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 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.3/MD Unforgeable authentication {UIA_223}

Hierarchical to:	-
Dependencies:	-
FIA_UAU.3.1/MD	The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2/MD	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 every 10 seconds.

Application Note 37: The condition under which re-authentication is required expected above shall be 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:

- after power supply recovery,
- periodically with a period changing randomly between 10 and 14 hours,
- when session counter is expired (the maximum number is 240),
- when the inserted tachograph card returns "0x6A88",
- A time frame, t2, after tachograph card data update which is performed a time frame, t1, after midnight. That is, cummulated time frame t1+t2 after midnight where t1 and t2 are selected randomly between 10 and 60 minutes.
- If re-authentication is not performed in any cases listed above, a flag is set indicating a pending re-authentication. The pending re-authentication is performed a random time frame, between 10 and 60 minutes, after the flag is set. In case tachograph card data needs to be updated while the flag is set, re-authentication is performed immediately before the update.

Application Note 38: The condition under which re-authentication is required expected above shall be more frequently than once per day, cf. UIA_210 in [9].

7.1.5.4 FIA_UID User identification

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

Hierarchical to: FIA_UID.1

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.

FIA_UID.2/MD User identification before any action {UIA_221}

Hierarchical to: FIA_UID.1

Dependencies: -

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

7.1.6 Class FPR Privacy

7.1.6.1 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/ECDSA, FCS_COP.1/AES**, 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]~~.

Application Note 40: 'To observe the cryptographic operations' means here 'using any TOE external interface in order to gain the values of cryptographic keys being to keep secret'.

7.1.7 Class FPT Protection of the TSF

7.1.7.1 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}.

7.1.7.2 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.2//HW_sabotage	Notification of physical attack {RLB_207, RLB_208}
Hierarchical to:	FPT_PHP.1
Dependencies:	FMT_MOF.1: not fulfilled, but **justified:**

	It is a matter of RLB_207 and RLB_208: this function (detection of removal of the smart card placed in any slot outside the control of the TOE) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a not applicable way for RLB_207 and RLB_208.
FPT_PHP.2.1//HW_sabotage	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2//HW_sabotage	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// HW_sabotage	For the smart card interfaces of the TOE, the TSF shall monitor the devices and elements and notify any user except WORKSHOP and audit record generation when physical tampering, **by removal of the smart card placed in any slot outside the control of the TOE,** with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance 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.

7.1.7.3 FPT_STM Time stamps

FPT_STM.1 Reliable time stamps {ACR_201}

Hierarchical to: -

Dependencies: -

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

Application Note 41: This requirement is the matter of the VU's real time clock. According to ACC_208 and REQ157 small time adjustments are allowed and therefore, are out of the scope of this requirement

7.1.7.4 FPT_TDC Inter-TSF TSF Data Consistency

FPT_TDC.1//IS Inter-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 {RLB_205}

Hierarchical to: -

Dependencies:	-
FPT_TDC.1.1//SW-Upgrade	The TSF shall provide the capability to consistently interpret SW upgrade patch data and update 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 component and particular VU when interpreting the TSF data from another trusted IT product.

7.1.7.5 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~~ verifies the integrity of security data.
FPT_TST.1.3	The TSF shall ~~provide authorised users with the capability to~~ verifies the integrity of stored TSF executable code.

7.1.8 Class FRU Resource Utilisation

7.1.8.1 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.

Application Note 42: The current assignment is to consider in the context of RLB_212 (sec. 4.7.6 of [9] 'Data availability'). Controlled resources in this context may be 'functions and data covered by the current set of SFRs'.

7.1.9 Class FMT Security Management

7.1.9.1 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[29] 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 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.

[29] see the definition of the role “User” in Table 3 above

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.

FMT_MSA.3/SW-Upgrade 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/SW-Upgrade	The TSF shall enforce the SFP_SW-Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/SW-Upgrade	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

7.1.9.2 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.

7.1.9.3 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.

7.1.9.4 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 User Groups: - 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.

7.2 Security Assurance Requirements

The security assurance requirements for the TOE are as derived in the PP [13], which are the requirements for the Evaluation Assurance Level 4 augmented with ATE_DPT.2 and AVA_VAN.5. The security assurance requirements are listed in the table below.

Assurance Classes	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV.IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic Modular Design
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_TAT.1 Well-defined development tools
	ALC_DEL.1 Delivery procedures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules

	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 6: Security Assurance Requirements

7.3 Security Requirements Rationale

7.3.1 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/TDES	Cryptographic key generation									X		
FCS_CKM.1/AES	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		
FCS_COP.1/RSA	Cryptographic operation									X		
FCS_COP.1/AES	Cryptographic operation											X
FCS_COP.1/ECDSA	Cryptographic operation											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
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

		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_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
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.1/MD	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.3/MD	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		
FIA_UID.2/MD	User identification before any action	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_MSA.3/SW-Upgrade	Static attribute initialisation											X
FMT_MOF.1	Management of security functions	X							X			
FMT_SMF.1	Specification of Management Functions	X								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.2//HW_sabotage	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			

		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
FPT_TDC.1//SW-Upgrade	Inter-TSF basic TSF data consistency											X
FPT_TST.1	TSF testing			X					X			
FRU_PRS.1	Limited priority of service								X			

Table 7: Coverage of Security Objectives for the TOE by SFR

Note: FCS_CKM.1/TDES corresponds to FCS_CKM.1 in the protection profile [13].

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

Security Objectives	Security Functional Requirements
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-Upgrade SFP SW-Upgrade for the upgrade of the software in the TOE 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 Defines security attributes for SFP SW-Upgrade FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation 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

Security Objectives	Security Functional Requirements
	allowing any other action FIA_UID.2/MD A management device 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. 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_MSA.3/SW-Upgrade Provides the SFP SW-Upgrade 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 attrib-utes 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

Security Objectives	Security Functional Requirements
	allowing any other action FIA_UID.2/MD A management device 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.) 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 FIA_UID.2/MD A management device 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.1/MD Allows MD 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.3/MD Provides unforgeable authentication for the management device FIA_UAU.5//TC Multiple authentication mechanisms according to

Security Objectives	Security Functional Requirements
	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 FIA_UID.2/MD A management device is successfully identified before allowing any other action
O.Integrity	FAU_STG.1 Protect the stored audit records from unauthorised deletion 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 FPT_TDC.1/SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer
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_ACC.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade 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 Defines security attributes for SFP SW-Upgrade 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 user data, from outside of the TOE using the SFP SW-Upgrade. Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.

Security Objectives	Security Functional Requirements
	FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation 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. 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/SW-Upgrade Provides the SFP SW-Upgrade 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 FPT_TDC.1/SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer
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 Defines security attributes for SFP SW-Upgrade 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 Defines security attributes for SFP SW-Upgrade 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 user data, from outside of the TOE using the SFP SW-Upgrade. Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected. FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation of resource

Security Objectives	Security Functional Requirements
	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 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. FMT_MSA.3/SW-Upgrade Provides the SFP SW-Upgrade 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_Deviation Detection of physical tampering (Power_Deviation) and generation of an audit record FPT_PHP.2/HW_sabotage Detection of physical tampering (Removal of the smart card placed in any slot outside the control of the TOE) 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 secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer. 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 Generates an evidence of origin for the data to be downloaded to external media. FCS_CKM.1/TDES Generates of session keys for the motion sensor and the tachograph cards FCS_CKM.2 Controls distribution of cryptographic keys in accordance

Security Objectives	Security Functional Requirements
	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 authentica-tion. 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 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

Security Objectives	Security Functional Requirements
	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	FCS_COP.1/AES Provides the cryptographic operation AES. FCS_COP.1/ECDSA Provides the cryptographic operation ECDSA FCS_CKM.1/AES Generates secure boot keys FCS_CKM.3 Controls cryptographic key access and storage in the TOE FCS_CKM.4 Destroys cryptographic keys in the TOE FDP_ACC.1/ SW-Upgrade SFP SW-Upgrade for the upgrade of the software in the TOE FDP_ACF.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade FDP_ITC.2/SW-Upgrade Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. : Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected FMT_MSA.3/SW-Upgrade Provides the SFP SW_Upgrade 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. FPT_TDC.1/SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer

Table 8: Suitability of the SFRs

7.3.2 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. 7.1 above. All dependencies being expected by CC part 2 are either fulfilled or their non-fulfilment is justified.

7.3.3 Security Assurance Requirements Rationale

The current Security Target is claimed to be conformant with the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

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. This decision represents a part of the conscious security policy for the recording equipment required by the legislative [6] and reflected by the current ST.

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

The augmentation of EAL4 chosen comprises the following assurance components:

– ATE_DPT.2 and
– AVA_VAN.5.

For these additional assurance 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 9: SAR Dependencies

8. TOE Summary Specification

Security Service	Security Functional Requirements concerned
Identification and authentication of motion sensor, tachograph cards and management device: It describes the identification and authentication of motion sensor, user (by using tachograph cards), and management device. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (UIA_201 to UIA_206 for motion sensor, UIA_207 to UIA_214 for user, UIA_221 to UIA_223 for management device). 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 before allowing any other TSF-mediated actions in accordance with FIA_UAU.2//MS. TSF detects and prevents use of authentication data that has been copied and replayed (FIA_UAU.3/MS) and supports enforcing the SFP FUNCTION and SFP Input Sources to avoid value changes of security attributes (FMT_MSA.1, FMT_MSA.3/FUN and FMT_MSA.3/IS). The TOE identifies and authenticates its users at card insertion before allowing any further TSF-mediated actions in accordance with FIA_UID.2/TC, FIA_UAU.1/TC and FIA_UAU.5//TC as well as FIA_UAU.1/PIN. The authentication is mutual and triggered by the TOE. TSF detects and prevents use of authentication data that has been copied and replayed (FIA_UAU.3/TC), maintains the list of security attributes belonging to individual users as required by FIA_ATD.1//TC and prevents value changes of security attributes (FMT_MSA.1). 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. The TOE identifies and authenticates the management device (MD) by decryption and the signature verification of the file received from MD. The files received from MD are personalization file and TOE software which are signed and encrypted by the cryptographic keys of MD. The corresponding keys for decryption and signature verification on the TOE are securely loaded to the TOE during the manufacturing process.	– FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – FIA_UID.2/MD: Identification of the Management Device – (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/MD, FIA_UAU.3/MD: Authentication of the Management Device – 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 FMT_MSA.3/FUN FDP_ACC.1/FUN functions FIA_UID.1/MD, FIA_UID.2/MD, FIA_UID.3/MD: user identity management device Supported by: – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards – FCS_COP.1/ECDSA: for signature verification of the software update data – (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1)

Security Service	Security Functional Requirements concerned
Access control to functions and stored data: It ensures that the access to read, create or modify any information into the TOE is granted to only by those authorised. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (ACC_201 for general access control, ACC_202-ACC_203 for functions, ACC_204 to ACC_210 for data, ACC_211 for file structure). TSF controls the access to the data and functions and enforces the File Structure SFP, SFP FUNCTION, SFP DATA, SFP User Data Export, SFP Input Sources, SFP SW-Upgrade as required by FDP_ACC.1/*, FDP_ACF.1/* and FMT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE, FMT_MSA.3/SW-Upgrade. TSF implements the File Structure SFP for tachograph application and data files structure as required by ACC_211 (FDP_ACC.1/FIL, FDP_ACF.1/FIL) and enforces the SFP FUNCTION, SFP DATA, SFP User Data Export on subjects, objects, and operations as required in [6] and described in 7.1.4 (FDP_ACC.1/DAT, FDP_ACF.1/DAT, FDP_ACC.1/UDE, FDP_ACF.1/UDE). TSF ensures that user data (entered manually) related to requirement 109a [6] may only be entered for the period last card withdrawal — current insertion (requirement 050a) in accordance with the requirements FDP_ACC.1/UDE, FDP_ACF.1/UDE. Software update of the security and non-security relevant software components is only possible after the corresponding authentication and verification with help of credentials as required in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade. Nobody may change the public/private keys and the Km_{VU} after their insertion during the personalization. Nobody may read the private keys and the Km_{VU} after their insertion during the personalization process in full compliance with FMT_MSA.1, MT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE.	– (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 – 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 – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT – FMT_MSA.3/UDE – FMT_MSA.3/IS – FMT_MSA.3/SW-Upgrade. – (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)

Security Service	Security Functional Requirements concerned
Accountability of users: It defines the accountability for each user. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (ACT_201 to ACT_207). The audit function will be started up as soon as the TOE has external power supply after activation and shut down, when the external power supply is interrupted. In this case TSF records within each audit record at least the information date and time of begin and end of the event and the type of event. TSF, for events impairing the security of the TOE, records those events with associated data ([6] (requirements 094, 096 and 109) as required in FAU_GEN.1. TSF enforces audit records storage rules [6] (requirement 094) and (requirement 096) in a way as required in FDP_ETC.2, furthermore, it preserves the audit trail as required by FAU_STG.1 TSF stores audit records generated by the motion sensor in its data memory as required by FAU_GEN.1 and the transfer of the record from the motion sensor to the TOE is encrypted according to FCS_COP.1/TDES. 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 for security. TSF is also able to provide reliable time stamps based on the RTC time information (as required in FPT_STM.1) for its own use. TSF writes the relevant audit records on tachograph cards in a way as required by FDP_ACC.1/DAT and FDP_ACF.1/DAT and update binary with secure messaging is used [10] (FCS_COP.1/TDES). TSF overwrites the oldest stored audit records and behaves according to [6] requirements 083, 086, 089, 092 and 105b, if the audit trail is full as required in FAU_STG.4.	– 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

Security Service	Security Functional Requirements concerned
Audit of events and faults: It defines the audit capabilities. It is required only for events that may indicate a manipulation or a security breach attempt. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (AUD_201 to AUD_205). TSF, for events impairing the security of the TOE, records those events with associated data as required in FAU_GEN.1 and makes it possible to print, display and download audit records except for the events listed in REQ 011 as required by FAU_SAR.1.	– 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.

Security Service	Security Functional Requirements concerned
Object reuse for secret data: It provides residual information protection by deallocating the resource. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (REU_201) TSF ensures that any previous information content of a resource used for operations in which security relevant material is involved in volatile memory in the TOE, is erased upon the allocation of a new resource as required in FDP_RIP.1. Furthermore temporarily active keys are destroyed in accordance with FCS_CKM.4. Other temporary storage objects can be re-used without implying inadmissible information flow.	– FDP_RIP.1 Subset residual information protection Supported by: – FCS_CKM.4: Cryptographic key destruction

Security Service	Security Functional Requirements concerned
Accuracy of recorded and stored data: It provides accuracy services by controlling the information flow, checking the internal data transfers, and checking the stored data integrity. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (ACR_201-ACR_201a for information flow, ACR_202-ACR_203 for internal data transfers, ACR_204-ACR_205 for stored data integrity). TSF ensures that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 [6] may only be processed from the right input sources: • vehicle motion data, as required by FPT_TDC.1//IS • VU's real time clock, as required in FPT_STM.1 • recording equipment calibration parameters, as required in FDP_ITC.1 • tachograph cards, as required by FPT_TDC.1//IS, supported by users' inputs in accordance with the requirements FDP_ACC.1/IS, FDP_ACF.1/IS, FPT_STM.1, FDP_ITC.1, FDP_ITC.2//IS, FPT_TDC.1//IS. TSF ensures that user data related to requirement 109a [6], may only be entered for the period last card withdrawal — current insertion (requirement 050a) in accordance with the requirements FDP_ACC.1/UDE and FDP_ACF.1/UDE. TSF protects the user data stored in the TOE by	– 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) – FDP_ITC.2/SW-Upgrade: import of user data with security attributes – FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC) – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media – FDP_SDI.2: Stored data integrity – FPT_TDC.1/SW-Upgrade: capability to ensure the consistency of data for the update – FCS_COP.1/AES: for decryption of the software update data and encryption / decryption of the data transferred between the security processor and the main processor – FCS_COP.1/ECDSA: for signature verification of the software update data Supported by: – FCS_CKM.1/AES: Cryptographic key generation – (FDP_ACC.1/IS, FDP_ACF.1/IS): right

Security Service	Security Functional Requirements concerned
SHA-1 hash values which are calculated about the data and stored in the TOE together with the data. The integrity of the user data is checked regularly fulfilling the requirement FDP_SDI.2. Upon detection of a stored user data integrity error, TSF generates an audit record in accordance with FAU_GEN.1 Software update is only possible after the corresponding authentication as required in FIA_UAU.1/MD, FIA_UAU.3/MD. SW-Upgrade is performed only if the integrity and the authenticity of the patch data is confirmed by means of update credentials (FPT_TDC.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade) which are used by FCS_COP.1/AES and FCS_COP.1/ECDSA.	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 – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device

Security Service	Security Functional Requirements concerned
Reliability of services: It provides reliability services related to test, software, physical protection, power supply interruptions, reset conditions, data availability and multiple applications. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (RLB_201 to RLB_203 for tests, RLB_204-RLB_205 for software, RLB_206 to RLB_208 for physical protection, RLB_209-RLB_210 for power supply interruptions, RLB_211 for reset conditions, RLB_212 to RLB_214 for data availability, RLB_215 for multiple applications). Inputs from external sources are not accepted as executable code (as required in FDP_ITC.2//IS, FDP_ACC.1/IS, FDP_ACF.1/IS). SW-Upgrade of the TOE is accepted only if the update patch can be decrypted and the digital signature on it can be verified (FDP_ITC.2/SW-Upgrade) with the help of credentials as required in FDP_ACC.1/SW-Upgrade, FDP_ACF.1/SW-Upgrade and FPT_TDC.1/SW-Upgrade. The cryptographic keys necessary for decryption and digital signature verification are securely loaded to the TOE during the manufacturing before the personalization (FMT_MSA.3/SW-Upgrade). TSF controls the access to the data and functions of the TOE and prevents analysis or debug of TOE's software (including the cryptographic material) in the field after the TOE activation (FPR_UNO.1). This includes that TSF allows the calibration functions only in calibration mode (REQ 010) in accordance with FMT_SMF.1. TSF ensures that cards cannot be released before relevant data have been stored to them (FDP_ACC.1/FUN, FDP_ACF.1/FUN).	– 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.2/HW_sabotage : Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services – FDP_ACC.1/SW-Upgrade – FDP_ACF.1/SW-Upgrade – FPT_TDC.1/SW-Upgrade

Security Service	Security Functional Requirements concerned
TSF preserves a secure state when deviation from specified values of the power supply, including cut-off is detected. In that case TSF, in compliance with FPT_FLS.1, • generates an audit record (except when in calibration mode) compliant with FAU_GEN.1, • preserves the secure state of the TOE, • maintains the security functions, related to components or processes still operational, • preserves the stored data integrity In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, TSF resets the TOE clearly as required by FPT_FLS.1 and an audit record is generated and stored after power supply reconnection as required by FAU_GEN.1. TSF deletes security sensitive information in the flash memory of the security processor when electrical or environmental attack on the TOE security module is detected (FPT_PHP.3). In that scope TSF detects high/low temperature on the security module, a disconnection on the mesh wiring, resistance value change of the mesh wiring, hence a drilling on the mesh structure and mesh battery removal. All other physical tampering attempts can be detected by visual inspection. After its activation, the TOE detects removal of the smart card placed in any slot outside the control of the TOE as required by FPT_PHP.2/HW_sabotage and generates an audit record as required by FAU_GEN.1. TSF executes self tests during initial start-up, and during normal operation to verify its correct operation (FPT_TST.1). The TOE self tests include the verification of the integrity of security data and the verification of stored executable code. TSF ensures that access to resources is obtained when required and that resources are neither requested nor retained unnecessarily as required by FRU_PRS.1. All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE are disabled during the personalization in accordance with FMT_MOF.1. It is not possible to restore them for later use.	– FMT_MSA.3/SW-Upgrade 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

Security Service	Security Functional Requirements concerned
Cryptographic support: It provides support for security mechanism when needed. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (CSP_201 to CSP_205)	– 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) and for encryption/decryption during the mutual authentication mechanism.

Security Service	Security Functional Requirements concerned
	– FCS_COP.1/AES : for decrypting the personalization file and the deployment software loaded to the TOE during the personalization. For decrypting the deployment software loaded to the TOE during the software upgrade. For Encryption/decryption operations during the secure boot. – FCS_COP.1/ECDSA: for verifying the digital signature on the personalization file and deployment software when loaded on the TOE – (FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management

Security Service	Security Functional Requirements concerned
Data exchange with motion sensor, tachograph cards and external media (download function): It provides the data exchange service between the TOE and motion sensor, tachograph cards and external media. It is defined in Appendix 10 of Annex IB [6] and summarized in Annex A: Coverage of the requirements of Appendix 10 (DEX_201-DEX202 for motion sensor, DEX_203 to DEX_205 for tachograph cards, DEX_206 to DEX_208 for external media). TSF protects the authenticity and integrity of data being exchanged between the TOE and the external subjects (tachograph card, motion sensor, downloading equipment). The data transfer between the TOE and • tachograph cards is secured according to ISO/IEC 7816-4 to the extent as defined in [9] CSM_021 – Retail-MAC as required in FCS_COP.1/TDES. TSF verifies the integrity and authenticity of data imported from tachograph cards. Upon detection of card data integrity or authenticity error, TSF generates an audit record compliant with FAU_GEN.1 and does not use the data as required in FDP_ITC.2//IS. TSF exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity as required in FDP_ETC.2. • the motion sensor is secured according to ISO 16844-3:2004 [12] and as required in FCS_COP.1/TDES and after proper authentication as required in FIA_UAU.2//MS, FIA_UAU.6/MS, FIA_UID.2/MS. TSF verifies the integrity and authenticity of motion data imported from the motion sensor. Upon detection of a motion data integrity or authenticity error, TSF generates an audit record and continues to use imported data as required in FDP_ITC.2//IS. • downloading equipment are secured according to PKCS#1 V2.0 and with hash algorithm SHA-1 as required in	– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media. Appendix 7 of the regulation [6] describes the data structures 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/TDES, 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

Security Service	Security Functional Requirements concerned
FCS_COP.1/RSA. The TOE identification, its equipment key certificate and the member state certificate are also downloaded (FCO_NRO.1). The verifier of the data must possess European public key to verify the certificate chain.	– FAU_GEN.1: Audit records: Generation

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 IB of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002 amended by

- Commission Regulation (EC) No 432/2004 of 5 March 2004
- Council Regulation (EC) No 1791/2006 of 20 November 2006
- Commission Regulation (EC) No 68/2009 of 23 January 2009
- Commission Regulation (EU) No 1266/2009 of 16 December 2009

[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 IB of Commission Regulation (EEC) No. 1360/2002 – Tachograph Cards Specification

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

[10] Appendix 11 of Annex IB 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, First Edition, 2004-11-01 with Technical Corrigendum 1:2006, 2006-03-01, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface

[13] Digital Tachograph-Vehicle Unit Common Criteria Protection Profile, BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik

[14] Appendix 7 of Annex IB of Commission Regulation (EEC) No. 1360/2002 – DATA DOWNLOADING PROTOCOLS

Other Reference Documents

[ECDSA] FIPS 186-2 Digital Signature Standard (ECDSA).

[SHA-256] FIPS 180-2 Secure Hash Standard (SHA-256).

[AES] Advanced Encryption Standard (AES) (FIPS PUB 197).

[OFB] NIST Special Publication 800-38A 2001 Edition.

[NIST] Special Publication 800-133 Recommendation for Cryptographic Key Generation, Dec. 2012

10. Annex A: Coverage of the requirements of Appendix 10

The following table demonstrates the coverage of the requirements of [9], chapter 4 by the security functional requirements chosen from [1], [2], [3] and specified in section 7.1 "Security Functional Requirements" above.

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	IDENTIFICATION & AUTHENTICATION	
UIA_201	The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.	FIA_UID.2/MS
UIA_202	The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.	OSP.Type_Approved_MS
UIA_203	The VU shall authenticate the motion sensor it is connected to: - at motion sensor connection, - at each calibration of the recording equipment, - at power supply recovery. Authentication shall be mutual and triggered by the VU.	FIA_UAU.2//MS
UIA_204	The VU shall periodically *(every 10 seconds)* re-identify and re-authenticates the motion sensor it is connected to, and ensures that the motion sensor identified during the last calibration of the recording equipment has not been changed.	FIA_UAU.6/MS
UIA_205	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MS
UIA_206	After 3 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 SFR 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/MS, FAU_GEN.1
UIA_207	The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.	FIA_UID.2/TC

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	IDENTIFICATION & AUTHENTICATION (cont'd)	
UIA_208	The user identity shall consist 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.	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_MSA.3/FUN FMT_SMF.1 FMT_SMR.1//TC for five different User Groups
UIA_209	The VU shall authenticate its users at card insertion.	FIA_UAU.1/TC
UIA_210	The VU shall re-authenticate its users: - at power supply recovery, - periodically or after occurrence of specific events (TBD by manufacturers and more frequently than once per day).	FIA_UAU.6/TC
UIA_211	Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.	FIA_UAU.5//TC
UIA_212	In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long. Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.	FIA_UAU.1/PIN
UIA_213	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_214	After 5 consecutive unsuccessful authentication attempts have been detected, the SFR shall: - generate an audit record of the event, - warn the user, - assume the user as UNKNOWN, and the card as non valid (definition (z) and requirement 007).	FIA_AFL.1/TC, FAU_GEN.1
UIA_221	For every interaction with a management device, the VU shall be able to establish the device identity.	FIA_UID.2/MD

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	IDENTIFICATION & AUTHENTICATION (cont'd)	
UIA_222	Before allowing any further interaction, the Vusuccessfully authenticates the management device.	FIA_UAU.1/MD
UIA_223	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MD FMT_MSA.3/IS
	ACCESS CONTROL	
ACC_201	The VU shall manage and check access control rights to functions and to data.	FDP_ACC.1/FUN for functions FMT_MSA.3/FUN FDP_ACC.1/DAT for data FMT_MSA.3/DAT
ACC_202	The VU shall enforce the mode of operation selection rules (requirements 006 to 009).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for choosing an operation mode according to REQ006 to 009.
ACC_203	The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for accessible functions in each mode of operation (REQ010)
ACC_204	The VU shall enforce the VU identification data write access rules (requirement 076)	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ076 FMT_MSA.3/DAT
ACC_205	The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ079 and 155 FMT_MSA.3/DAT
ACC_206	After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for REQ154 and 156.

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	ACCESS CONTROL (cont'd)	
ACC_207	After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ097 FMT_MSA.3/DAT
ACC_208	After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for ACC_208
ACC_209	After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for ACC_209 FMT_MSA.3/DAT
ACC_210	The VU shall enforce appropriate read and write access rights to security data (requirement 080).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ080 FMT_MSA.3/DAT
ACC_211	Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.	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
	ACCOUNTABILITY	
ACT_201	The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).	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
ACT_202	The VU shall hold permanent identification data (requirement 075).	FDP_ACC.1/DAT, FDP_ACF.1/DAT FMT_MSA.3/DAT

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST

	ACCOUNTABILITY (cont'd)	
ACT_203	The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).	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
ACT_204	The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).	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
ACT_205	The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).	FAU_GEN.1 with an entry for REQ 090, 093
ACT_206	The VU shall ensure 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.	FAU_STG.1 with *detection* for 081 to 093 and 102 to 105a FAU_STG.4 for REQ083, 086, 089, 092, 105b (replacing oldest data)
ACT_207	The VU shall ensure 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.	FDP_ETC.2 for REQ109, 109a and 110

Requirement Appendix 10	**Requirement Description**	**Related SFR used in the current ST**
	AUDIT	

AUD_201	The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).	FAU_GEN.1 for REQ094, 096 FDP_ETC.2
AUD_202	The events affecting the security of the VU 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, – VU internal fault.	FAU_GEN.1 for AUD_202
AUD_203	The VU shall enforce audit records storage rules (requirement 094 and 096).	FAU_GEN.1
AUD_204	The VU shall store audit records generated by the motion sensor in its data memory.	FDP_ACC.1/DAT FDP_ACF.1/DAT FMT_MSA.3/DAT
AUD_205	It shall be possible to print, display and download audit records.	FAU_SAR.1
	OBJECT REUSE	
REU_201	The VU shall ensure that temporary storage objects can be reused without this invoking inadmissable information flow.	FDP_RIP.1

Requirement Appendix 10	**Requirement Description**	**Related SFR used in the current ST**
	ACCURACY	
ACR_201	The VU shall ensure that user data related to	FDP_ACC.1/IS

	requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a, 109 may only be processed from the right input sources: - Vehicle motion data, - VU's real time clock, - Recording equipment calibration parameters, - Tachograph cards, - User's inputs.	FDP_ACF.1/IS FPT_STM.1 for - VU'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. FPT_TDC.1/IS
ACR_201a	The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).	FDP_ACC.1/FUN FDP_ACF.1/FUN
ACR_202	If data are transferred between physically seperated parts of the VU, the data shall be protected from modification.	Not applicable, the TOE does not have physically seperated parts.
ACR_203	Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SFR shall generate an audit record of the event.	Not applicable, the TOE does not have physically seperated parts.
ACR_204	The VU shall check user data stored in the data memory for integrity errors.	FDP_SDI.2
ACR_205	Upon detection of a stored user data integrity error, the SFR shall generate an audit record.	FDP_SDI.2, FAU_GEN.1
	RELIABILITY	
RLB_201	c) Organisational part by manufacturer 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. d) VU cares: It is not possible to restore them for later use.	The property a) is formulated as OSP.Test_Points FMT_MOF.1 for the property b)
RLB_202	The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).	FPT_TST.1
RLB_203	Upon detection of an internal fault during self test, the SFR shall: - generates an audit record (except in calibration mode), - preserves the stored data integrity.	FAU_GEN.1 for an audit record FPT_FLS.1 for preserving the stored data integrity
Requirement Appendix 10	**Requirement Description**	**Related SFR used in the current ST**
	RELIABILITY (cont'd)	

RLB_204	There shall be no way to analyse or debug software in the field after the VU activation.	FPT_PHP.3 and ADV_ARC (self protection for stored data) FPR_UNO.1 (no successful analysis of leaked data)
RLB_205	Inputs from external sources shall not be accepted as executable code.	FDP_ITC.2//IS with FDP_ACC.1/IS, FDP_ACF.1/IS FDP_ITC.2/SW-Upgrade FPT_TDC.1/SW-Upgrade FDP_ACC.1/SW-Upgrade FDP_ACF.1/SW-Upgrade FMT_MSA.3/SW-Upgrade
RLB_206	If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 months. In such a case, the SFR shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection). If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).	FAU_GEN.1 for auditing
RLB_207	After its activation, the VU shall detect specified (Removal of the smart card placed in any slot outside the control of the TOE) hardware sabotage:	see Application Note 15 (an additional FPT_PHP.2/HW_sabotage may be suitable)
RLB_208	In the case described above, the SFR shall generate an audit record and the VU: (shall warn the user).	This requirement depends on RLB_207; see Application Note 15 (an additional FPT_PHP.2/HW_sabotage and RLB_208 in FAU_GEN.1 may be suitable)
RLB_209	The VU shall detect deviations from the specified values of the power supply, including cut-off.	FPT_PHP.2//Power_Deviation for detection
Requirement Appendix 10	**Requirement Description**	**Related SFR used in the current ST**
	RELIABILITY (cont'd)	
RLB_210	In the case described above, the SFR shall:	FAU_GEN.1 for Auditing

	- generate an audit record (except in calibration mode), - preserve the secure state of the VU, - maintain the security functions, related to components or processes still operational, - preserve the stored data integrity.	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)
RLB_211	In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall reset cleanly.	FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset
RLB_212	The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.	FRU_PRS.1
RLB_213	The VU shall ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a rule for REQ015 and 016
RLB_214	In the case described above, the SFR shall generate an audit record of the event.	FAU_GEN.1 (Last card session not correctly closed)
RLB_215	If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.	ADV_ARC (domain separation)

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	DATA EXCHANGE	
DEX_201	The VU shall verify the integrity and authenticity of motion data imported from the motion sensor.	FDP_ITC.2//IS for – vehicle motion data
DEX_202	Upon detection of a motion data integrity or authenticity error, the SFR shall: - generate an audit record, - continue to use imported data.	FAU_GEN.1. FDP_ITC.2//IS for – vehicle motion data
DEX_203	The VU shall verify the integrity and authenticity of data imported from tachograph cards.	FDP_ITC.2//IS for – tachograph cards.
DEX_204	Upon detection of a card data integrity or authenticity error, the SFR shall: - generate an audit record, - not use the data.	FAU_GEN.1 FDP_ITC.2//IS for – tachograph cards
DEX_205	The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.	FDP_ETC.2
DEX_206	The VU shall generate an evidence of origin for data downloaded to external media.	FCO_NRO.1
DEX_207	The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.	FCO_NRO.1
DEX_208	The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.	FDP_ETC.2

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	CRYPTOGRAPHIC SUPPORT	
CSP_201	Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.	FCS_COP.1/TDES FCS_COP.1/RSA FCS_COP.1/AES FCS_COP.1/ECDSA
CSP_202	If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes	FCS_CKM.1/TDES FCS_CKM.1/AES
CSP_203	If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.	FCS_CKM.2
CSP_204	If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.	FCS_CKM.3
CSP_205	If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.	FCS_CKM.4

Revision History

Revision No	Revision Reason	Date of Revision
0.1	First Publication	18.10.2012
0.2	Updated according to the lab comments (dated 31st October 2012) on version 0.1.	03.12.2012
0.3	Updated according to the observation reports dated 21st of December 2012.	22.02.2013
0.4	Updated according to the developer review.	26.02.2013
0.5	Updated according to the developer review.	27.02.2013
0.7	Updated according to the Observation Reports of the lab.	18.09.2013
0.8	Updated according to the Observation Reports of the lab.	12.11.2013
1.0	Updated according to the hardware modifications.	13.03.2015
1.1	Updated according to the Observation Reports of the lab.	19.08.2015
1.2	Updated according to the Observation Reports of the lab.	
1.3	Updated according to the Observation Reports of the lab.	16.02.2016
1.4	Updated according to the Observation Reports of the lab.	22.04.2016
1.5	Details added to TOE Summary Specification and re-authentication periods corrected.	04.07.2016
1.6	Updated according to observation reports	08.08.2016
1.7	ST Lite version	17.08.2016
1.8	Update with assurance continuity	22.09.2016
1.9	Access control policy SFR definition update	27.01.2017
2.0	Application note added to FCO_NRO.1 dependency part Assignment is changed to “every 10 seconds” in FIA_UAU.6.1/MS Assignment is changed from “3” to “2” in FIA_AFL.1.1/MS	26.04.2017
2.1	TOE Identification and version information revised. Latest feedback from lab fixed.	17.05.2017
2.2	FCS_CKM.1 references are updated	23.05.2017
2.3	Some enhancements on SFR descriptions	09.06.2017
2.4	AVU SW version is incremented to 0.8.3	06.10.2017
2.5	FCS_CKM.1/AES and FCS_CKM.4 references are updated.	19.10.2017
2.6	ST Lite version	26.04.2018