DTCO 1381 Security Target

Author: Winfried Rogenz I CVAM TTS LRH

Revision: 1.8
Maturity: <initial / **final**>
Status: <draft / **released** / obsolete>
Release: DTCO 1381, Release 2.0
File: 1381R2..0276.Security_Target.doc

1 History

Rev.	Date	Maturity	Author	Reason
1.0	03.04.2009	final	Winfried Rogenz	Changing of TOE reference, adoption from document 1382._SEC.01.Security_Target.doc, version 1.11, 09.12.2008
1.1	29.04.2009	final	Winfried Rogenz	Correction table page 63
1.2	17.02.2011	Final	Winfried Rogenz	Amendment after publishing protection profile BSI-CC-PP-057
1.3	05.09.2011	Final	Winfried Rogenz	Correction after remarks from the evaluator
1.4	20.09.2011	Final	Winfried Rogenz	Correction after remarks from the evaluator
1.5	06.10.2011	Final	Winfried Rogenz	Formal Corrections
1.6	25.04.2012	Final	Winfried Rogenz	Formal corrections after TOE-Design
1.7	09.05.2012	Final	Winfried Rogenz	Correction after remarks from the certification body
1.8	09.05.2012	Final	Winfried Rogenz	Fornal Corrections

2 Table of Contents

3 Terms and Abbreviations

3.1 Terms

Term	Explanation
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 ST 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 lever 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.
Digital Tachograph System	Equipment, people or organisations, involved in any way with the recording equipment and tachograph cards.
Entity	A device connected to the VU
Equipment Level	At the equipment level, one single key pair (EQTj.SK and EQTj.PK) is generated and inserted in each equipment unit (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQTj.C). This key pair is used for (i) authentication between vehicle units and tachograph cards, (ii) enciphering services: transport of session keys between vehicle units and tachograph cards, and (iii) digital signature of data downloaded from vehicle units or tachograph cards to external media. The final master key Km and the identification key K_{ID} are used for authentication between the vehicle unit and the motion sensor as well as

Term	Explanation
	for an encrypted transfer of the motion sensor individual pairing key K_P from the motion sensor to the vehicle unit. The master key Km, 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 [16844-3] 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 [1360] and represents an important additional contribution. It was approved by the European Authority. The ERCA policy is available from the web site http://dtc.jrc.it. Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
European Authority	An organisation being responsible for the European Root Certification Authority policy. It is represented by European Commission Directorate General for Transport and Energy Unit E1 – Land Transport Policy Rue de Mot, 24 B-1040 Bruxelles 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 detailedinformation.
European Root Certification Authority (ERCA)	An organisation being responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment (TP.360) Via E. Fermi, 1 I-21020 Ispra (VA) At the European level, ERCA generates a single European key pair (EUR.SK and EUR.PK). It uses the European private key to certify the Member States` public keys and keeps the records of all certified keys. A change of the European (root) key pair is currently not intended. ERCA also generates two symmetric partial master keys for the motion sensor: Km_{wc} and Km_{vu}. The first partial key Km_{wc} is intended to be stored in each workshop tachograph card; the second partial key Km_{vu} is

Term	Explanation
	inserted into each vehicle unit. The final master key Km 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.
Management Device	A dedicated device for software upgrade of the TOE
Member State Authority (MSA)	Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA). The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself. MSA is also responsible for inserting data containing Km_{wc}, Km_{vu}, motion sensor identification and authentication data encrypted with Km and K_{id} into respective equipment (workshop card, vehicle unit and motion sensor). Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
Member State Certification Authority (MSCA)	At the Member State level, each MSCA generates a Member State key pair (MSi.SK and MSi.PK). Member States' public keys are certified by the ERCA (MSi.C). MSCAs use their Member State private key to certify public keys to be inserted in equipment (vehicle unit or tachograph card) and keep the records of all certified public keys with the identification of the equipment concerned. MSCA is allowed to change its Member State key pair. MSCA also calculates an additional identification key Kid as XOR of the master key Km with a constant control vector CV. MSCA is responsible for managing and distributing Km_{wc}, Km_{vu}, motion sensor identification and authentication data encrypted with Km and K_{id} to 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.
Personal Identification	A short secret password being only known to the approved workshops

Term	Explanation
Number (PIN)	
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.
ysically separated parts	Physical components of the vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
Reference data.	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to [ISO 7816-4]
Security data	The specific data needed to support srcurity enforcing functions (e.g. cryptographic keys). Security data are part of the 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
SW-Upgrade	Software-Upgrade installs a new version of software in the TOE.
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[1]
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
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[1] or MS serial

[1] for tachograph cards, cf. [3821_IB_11], sec. 3.1

Term	Explanation
	number encrypted with the identification key ($Enc(K_{ID}|N_S)$) together with pairing key encrypted with the master key ($Enc(Km|K_P)$).[2]
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. 3821_IB_10][9], UIA_208 representing security attributes of the role 'User'.
User data	Any data, other than security data (sec. III.12.2 of [3821_IB]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [3821_IB]. 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 [CC]). Information stored in TOE resources that can beoperated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC]).
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] for motion sensor, cf. [16844-3]

3.2 Abbreviations

Term/Abbreviation	Explanation
CA	Certification Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining (an operation mode of a block cipher; here of TDES)
CC	Common criteria
CCMB	Common Criteria Management Board
DAT	Data
DES	Data Encryption Standard (see FIPS PUB 46-3)
DL	Download
DTCO	Digital Tachograph
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EC	European Community
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES)
EQT_j.C	equipment certificate
EQT_j.SK	equipment private key
EQT_j.PK	equipment public key
EUR.PK	European public key
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
FIL	File
Fun	Function
GST	Generic security target
Km	Master key
Km_{vu}	Part of the Master key, will manage the pairing between a motion sensor and the vehicle unit
Kvu	Individual device key used to calculate MACs for the data integrity control of user data records
Kp	Pairing key of the motion sensor
K_{sm}	Session key between motion sensor and vehicle unit
K_{st}	Session key between tachograph cards and vehicle unit

Term/Abbreviation	Explanation
kt	transport key software upgrade
MAC	Message Authentication Code
MD	Management Device
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member Sate Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
MS_i.C	Member State certificate
n.a.	Not applicable
OSP	Organisational security policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection profile
REQ xxx	Requirement number in [3821_IB]
RTC	Real time clock
ST	Security Target
SAR	Security assurance requirements
SFR	Security functional requirement
SFP	Security Function Policy
ST	Security Target
TBD	To Be Defined
TC	Tachograph Card
TDES	Triple Data Encryption Standard (see FIPS PUB 46-3)
TOE	Target Of Evaluation
TSF	TOE security functionality
UDE	User Data Export
VU	Vehicle Unit

4 ST Introduction

This document contains a description of the digital Tachograph DTCO 1381 Rel. 2.0 (the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the security requirements. It states the claimed minimum resistance against attacks of security functional requirements and the required level of assurance for the development and the evaluation.

This document is based on the Vehicle Unit Generic Security Target, which is described in Appendix 10 of Annex IB 3821_IB_10] of the European Regulation (EEC) No 3821/85 [3821] amended by the Council Regulation (EEC) No 2135/98 [2135] and the Council Regulation (EC) No. 1360/2002 [1360].The document states the security objectives on the environment and describes how they are implemented in the digital Tachograph DTCO 1381 Rel. 2.0.

Requirements referred to in the document, are those of the body of Annex IB [3821_IB]. For clarity of reading, duplication sometimes arises between Annex IB body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex IB body requirement referred by this security target requirement, the Annex IB body requirement shall prevail.

Annex IB body requirements not referred by security targets are not the subject of TSF. Unique labels have been assigned to threats, objectives, and procedural means and security requirements specifications for the purpose of traceability to development and evaluation documentation.

4.1 ST reference

Title:	DTCO 1381 Security Target
Revision:	1.8
Author:	Winfried Rogenz I CVAM TTS LRH
Publication date:	09.05.2012

4.2 TOE reference

Developer name:	Continental Automotive GmbH
TOE Name:	Digital Tachograph DTCO 1381
TOE Version number:	Release 2.0

4.3 TOE overview

4.3.1 TOE definition and operational usage

The digital Tachograph DTCO 1381 Rel. 2.0 is a vehicle unit (VU) in the sense of Annex IB [3821_IB] intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. It is connected to a motion sensor with which it exchanges vehicle's motion data.

The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. . It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards.

The physical scope of the TOE is a device[3] 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, and facilities for entry of user's inputs and embedded software) and of related user manuals. It must be connected to a motion sensor (MS) and to a power supply unit. It can temporarily be connected with other devices used for calibration, data export, software upgrade, and diagnostics.

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

The TOE itself is depicted in the following figure (it shall be noted that although the printer mechanism is part of the TOE, the paper document once produced is not):

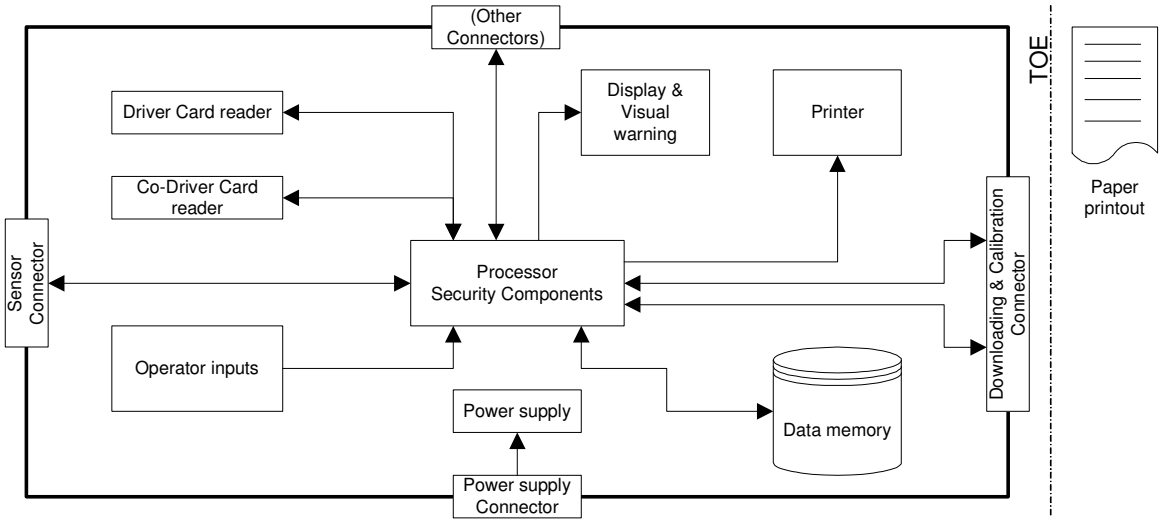


Figure 1 Digital Tachograph DTCO 1381

[3] single or physically distributed device

4.3.2 TOE major security features for operational use

The main security features of the TOE is as specified in 3821_IB_10][4]: The data to be measured[5] and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

It concretely means that security of the VU aims to protect

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

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

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

d) the integrity and authenticity of data downloaded.

The main security feature stated above is provided by the following major security services (please refer to 3821_IB_10], chap. 4):

a) TOE_SS.Identification_Authentication (of motion sensor, tachograph cards and management devices),

b) TOE_SS.Access (Access control to functions and stored data),

c) TOE_SS.Accountability (Accountability of users),

d) TOE_SS.Audit (Audit of events and faults),

e) TOE_SS.Object_Reuse (Object reuse for secret data),

f) TOE_SS.Accuracy (Accuracy of recorded and stored data),

g) TOE_SS.Reliability (Reliability of services),

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

Application Note 1 At least two services listed above – TOE_SS.Identification_Authentication as well as TOE_SS.Data_Exchange require TOE_SS.Cryptographic_support according to [3821_IB_10], sec. 4.9.

[4] O.VU_Main

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

4.3.3 TOE Type

The TOE type -digital Tachograph DTCO 1381 Rel. 2.0- is a vehicle unit (VU) in the sense of Annex IB [3821_IB].

The typical life cycle of the VU is described in the following figure:

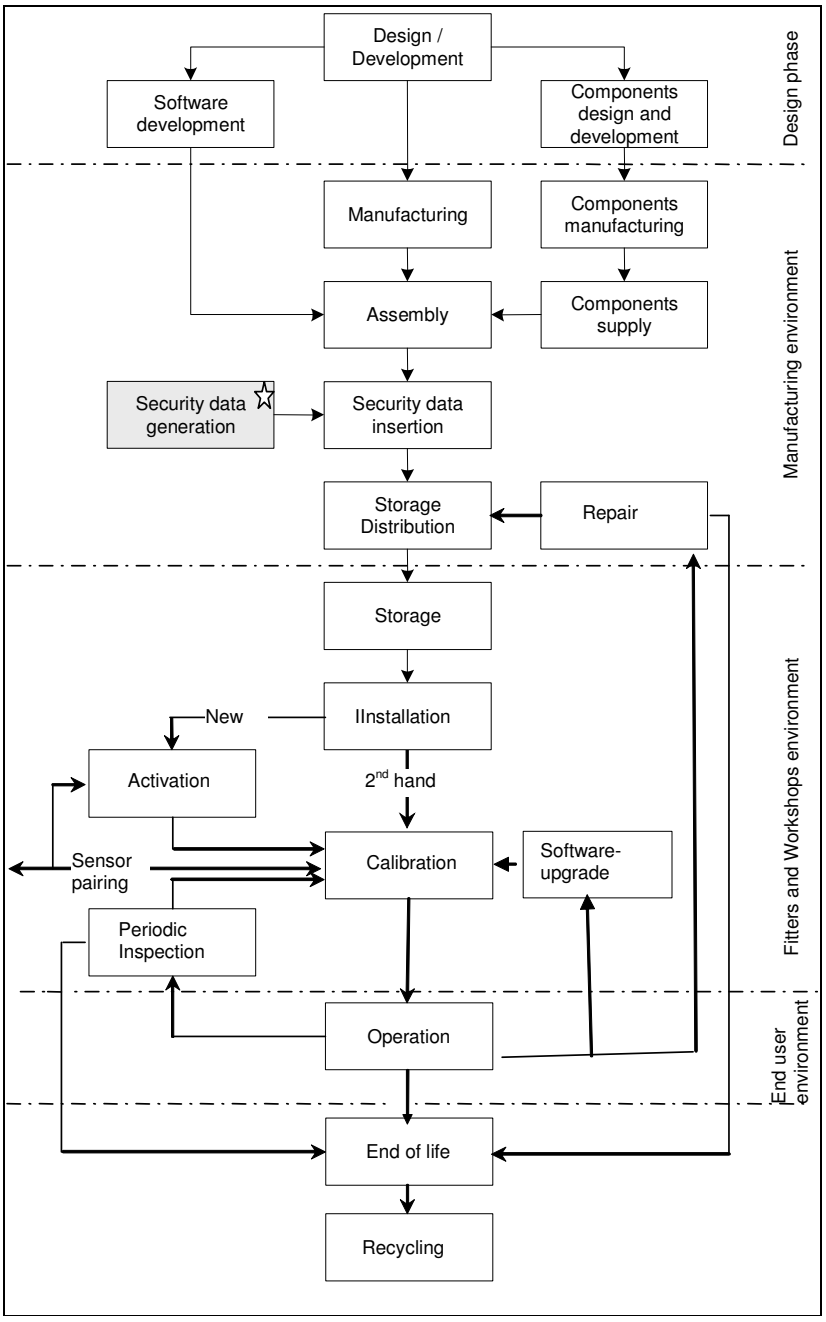


Figure 2 Life Cycle of the DTCO 1381

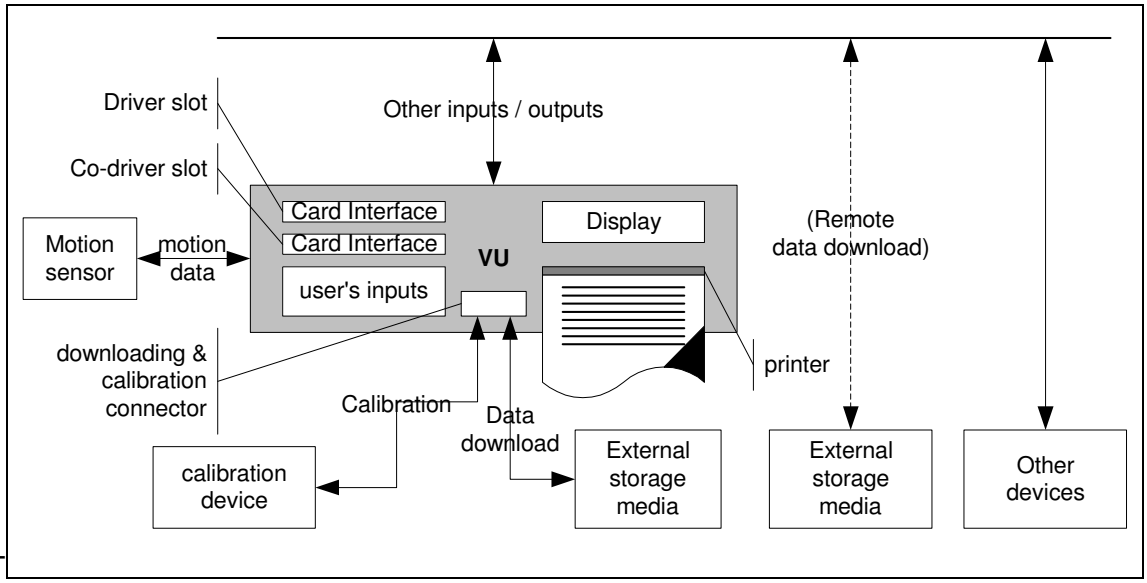
Application Note 2 For the TOE a repair in the fitters and workshop environments is not planned. Fitters or workshops can only change elements of the TOE as e.g. front covers, printer.... An approved software upgrade can also be performed in the workshop environment.

Application Note 3 The security requirements in sec. 4 of 3821_IB_10] 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 security target also focuses on the *operational phase* of the VU in the end user environment. Some single properties of the *calibration phase*[6] being significant for the security of the TOE in its operational phase are also considered by the current ST as required by 3821_IB_10]. The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [3821_IB], 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. 5.3 below). Usually, the TOE delivery from its manufacturer to the first customer (approved workshops) exactly happens at the transition from the *manufacturing* to the *calibration* phase.

4.3.4 Non-TOE hardware/software/firmware

The TOE operational environment while installed is depicted in the following figure:



T

Figure 3 VU operational environment

The following TOE external components are

a) *mandatory* for a proper TOE operation
   - power supply e.g. from the vehicle where the TOE is installed
   - motion sensor

[6] calibration phase compromises all operations within the fitters and workshop environment

b) *functionally necessary* for an Annex I B compliant operation
- calibration device (fitters and workshops environment only)
- tachograph cards (four different types of them)
- printer paper
- external storage media for data download

c) *helpful* for a convenient TOE operation
- connection to the vehicle network e.g. CAN-connection

Application Note 4 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 3821_IB_10] is a prerequisite for the type approval of a motion sensor and tachograph cards.

5 Conformance claims

5.1 CC conformance claim

This security target claims conformance to:

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [CC_1]

Common Criteria for Information Technology Security Evaluation, Part 2: Aecurity Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [CC_2]

Common Criteria for Information Technology Security Evaluation, Part3: Aecurity Assurance Requirements CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [CC3]

.

as follows

• Part 2 conformant.

• Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1, Recision 3, July 2009 [CEM] has to be taken into account.

5.2 PP conformance claim

This ST is conformant to the following documents:

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

Application Note 5 This vehicle unit ST covers all requirements of the vehicle unit generic ITSEC ST as contained in 3821_IB_10]. The coverage of the requirements of3821_IB_10] by the security functional requirements of the current ST is stated in Annex A, chap. 12 of this security target.

5.3 Package claim

This ST is conformant to the following security requirements package:

Assurance package E3hCC31_AP , as defined in section 9.2 below.

This assurance package is commensurate with [[JIL] 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. 9.2 below).

6 Security problem definition

6.1 Introduction

Assets

The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap.3 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 [3821_IB]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [3821_IB].	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 management device to transmit the upgrade file - 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 [7] Integrity Authenticity [8]

Table 1: Primary assets

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

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

[7] 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 en external medium shall not be protected.

[8] 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 [16844-3], sec. 7.5 (instruction #80); (ii) between the TOE and a tachograph card – in [3821_IB_2], chap. 4 (access condition = AUT). Integrity and authenticity of data to be downloaded to en external medium shall always be protected.

Object No.	Asset	Definition	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 [3821_IB], sec. III.12.2, - vehicle unit part of the symmetric master key for communication with MS (Km_{VU}), see [3821_IB_11], sec. 3.1.3, - session key between motion sensor and vehicle unit K_{Sm} (see [16844-3], sec. 7.4.5 (instruction 42)), - session key between tachograph cards and vehicle unit K_{St} (see [3821_IB_11], sec. 3.2) transport key software upgrade kt	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 [3821_IB], sec. III.12.2.	Integrity Authenticity

Table 2 Secondary assets

Application Note 6 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. [3821_IB_11], chap. 4.

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

Subjects and external entities

28 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. 3821_IB_10], 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 3821_IB_10], 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 ($Enc(Km\|K_P)$)
4	-	Tachograph Card	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: driver card,

External Entity No.	Subject No.	Role	Definition
			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 ($Enc(Km\|K_P)$).
-		- Attacker	see item User above.

Table 3: Subjects and external entities

Application Note 7 This table defines the subjects in the sense of [CC] 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 [CC]). 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.

6.2 Threats

This section of the security problem definition 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 3821_IB_10] chapter 3.3.

6.2.1 Threats averted solely by the TOE

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

T.Faults Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.[9]

T.Output_Data Users could try to modify data output (print, display or download).[9]

6.2.2 Threats averted by the TOE and its operational environment

T.Access	Users could try to access functions[9] not allowed to them (e.g. drivers gaining access to calibration function).
T.Calibration_Parameters	Users could try to use miscalibrated equipment[9] (through calibration data modification, or through organisational weaknesses).
T.Clock	Users could try to modify internal clock.[9]
T.Design	Users could try to gain illicit knowledge of design[9] either from manufacturer's material (through theft, bribery …) or from reverse engineering.
T.Environment	Users could compromise the VU security[9] through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).
T.Fake_Devices	Users could try to connect fake devices (motion sensor, smart cards) to the VU.[10]
T.Hardware	Users could try to modify VU hardware.[9]
T.Identification	Users could try to use several identifications or no identification.[11]
T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).[12]
T.Power_Supply	Users could try to defeat the VU security objectives[9] by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data[13] during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify VU software.[9]
T.Stored_Data	Users could try to modify stored data (security[14] or user data).

[9] The terms 'miscalibrated equipment', 'VU security', 'VU security objectives', 'data output', 'not allowed functions', 'VU in a well defined state', 'VU design', 'correctness of the internal clock', 'integrity of VU hardware', 'integrity of the VU software', 'full activated security functionality of the VU' correspond with 3821_IB_10] and are covered by the assets 'Accessibility to the TOE functions and data only for authorised subjects' and 'Genuineness of the TOE'

[10] 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'.

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

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

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

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

T.Tests The use of non invalidated test modes or of existing back doors could compromise the VU security.

Application Note 8 Threat T.Faults represents a 'natural' flaw not induced by an attacker; hence, no threat agent can be stated here.
The threat agent for T.Tests is User. It can be deduced from the semantic content of T.Tests.

6.2.3 Threats averted solely by the TOE's operational environment

T.Non_Activated Users could use non activated equipment.[9]

6.3 Organisational security policies

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

They are defined here to reflect those security objectives from 3821_IB_10] for which there is no threat directly and fully associated.

6.3.1 OSPs related to the TOE

OSP.Accountability The VU must collect accurate accountability data.

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

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

OSP.Test_Points All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU must disabled or removed before the VU activation during the manufacturing process

6.3.2 OSPs related to the TOE and its operational environment

OSP.Type_Approved_MS[15] The VU shall only be operated together with a motion sensor being type approved according to Annex I (B).

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

[15] The identity data of the motion sensor (serial number Ns) will be sent to the VU on request by the MS itself (see instruction #40 in [16844-3]). The 'certificate' Enc(K_{ID}|Ns) stored in the motion sensor is merely used by it for VU authentication, but not for verifying Ns by the VU (see instruction #41 in [16844-3]). Therefore, the VU accepts this data (serial number Ns) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved.

6.3.3 OSPs related to the TOE's operational environment

OSP.PKI

1) The European Authority shall establish a PKI according to [3821_IB_11], sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of the PKI.
2) The ERCA shall securely generate its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs.
3) The ERCA shall ensure that it issues MSi.C certificates only for the rightful MSCAs.
4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs shall securely generate their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
6) MSCAs shall ensure that they issue EQTj.C certificates only for the rightful equipment.

OSP.MS_Keys

1) The European Authority shall establish a special key infrastructure for management of the motion sensor keys according to [16844-3] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority shall properly operate the ERCA steering other levels (the Member State and theequipment levels) of this key infrastructure.
2) The ERCA shall securely generate both parts (Km_{VU} and Km_{WC}) of the master key (Km).
3) The ERCA shall ensure that it securely convey this key material only to the rightful MSCAs.
4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
5) MSCAs shall securely calculate the motion sensor identification key (K_{ID}) and the motion sensor's credentials: MS individual serial number encrypted with the identification key ($Enc(K_{ID}|N_S)$) and MS individual pairing key encrypted with the master key ($Enc(Km|K_P)$).
6) MSCAs shall ensure that they issue these MS credentials[16], Km_{VU}[17] and Km_{WC}[18] only to the rightful equipment.

[16] to the motion sensors
[17] to the vehicle units
[18] 1to the workshop cards

6.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.
The GST in 3821_IB_10] 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 3821_IB_10]).

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 and (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 …).[19]
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated.

[19] The assumption A.Faithful_Drivers taken from the Generic Security Target 3821_IB_10] seems not to be realistic and enforceable, because the driver is the person, who has to be controlled and surveyed (see the Council Regulation [1360] This assumption is made in the current ST only for the sake of compatibility with the GST 3821_IB_10]. and is necessary from *functional* point of view.

7 Security objectives

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

7.1 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 of as defined in in 3821_IB_10] chapter 3.5.

O.Access	The TOE must control user access to functions and data.
O.Accountability	The TOE must collect accurate accountability data.
O.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
O.Authentication	The TOE should authenticate users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The TOE must maintain stored data integrity.
O.Output	The TOE must ensure that data output reflects accurately data measured or stored.
O.Processing	The TOE must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The TOE must provide a reliable service.
O.Secured_Data_Exchange	The TOE must secure data exchanges with the motion sensor and with tachograph cards.
O.Software_Analysis[20]	There shall be no way to analyse or debug software[21] in the field after the TOE activation.
O.Software_Upgrade	The TOE must ensure authenticity and integrity of software to be installed during a software upgrade.

[20] This objective is added for the sake of a more clear description of the security policy: In the GST [3821_IB_10]], this aspect is part of O.Reliability, what might be not self-evident. The special concern here is RLB_204 in 3821_IB_10]

[21] 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

7.2 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 3821_IB_10] chapter 3.6, Where they are represented as security measures.

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

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

7.2.2 Manufacturing environment

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

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

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

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

OE.Software_Upgrade Software revisions shall be granted security certification before they can be implemented in the TOE.

OE.Sec_Data_Strong[22] Security data inserted into the TOE shall be cryptographically strong as required by [3821_IB_11]..

OE.Test_Points[23] All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation by the VU manufacturer during the manufacturing process.

Application Note 9 Please note that the design and the manufacturing environments are not the intended usage environments for the TOE (cf. the *Application Note 3* above).

[22] The security objective OE.Sec_Data_Strong is defined in addition to 3821_IB_10] in order to reflect an aim of establishing the PKI and the symmetric key infrastructure (OSP.PKI and OSP.MS_Keys)

[23] this objective is added for the sake of a more clear description of the security policy: In the GST 3821_IB_10], 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 3821_IB_10].

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.

7.2.3 Fitter and workshops environment

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

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

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

OE.Management_Device The Management Device (MD) is installed in the approved workshops according to A.Approved_Workshops. The software upgrade data and necessary key data (for the software upgrade) are imported into the MD by the approved workshops according to A.Approved_Workshops.

7.2.4 End user environment

OE.Card_Availability Tachograph cards shall be available to TOE users and delivered by Member State Authorities to authorised persons only.

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

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

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

OE.Faithful_Drivers[24] Drivers shall play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …).

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

[24] The objective OE.Faithful_Drivers taken from the Generic Security Target 3821_IB_10] seems not to be realistic and enforceable, because the driver is the person, who has to be controlled and surveyed (see the Council Regulation [1360]). This objective is claimed in the current ST only for the sake of compatibility with the GST 3821_IB_10] and is necessary from a f*unctional* point of view, see also A.Faithful_Drivers.

OE.Type_Approved_MS[25] The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to Annex I (B).

[25] 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 [16844-3]). The 'certificate' $Enc(K_{ID}|N_S)$ stored in the motion sensor is merely used by it for VU authentication, but not for verifying NS by the VU (see instruction #41 in [16844-3]]). 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 (-> UIA_202).

7.3 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 3821_IB_10] chapter 8.

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

	Threats																	OSPs								Assumptions								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
OE.Manufacturing				X	x																													
OE.Sec_Data_Strong																x								X	x									
OE.Sec_Data_Generation																x								X	X									
OE.Sec_Data_Transport																x								x	X									
OE.Test. Points																						x												
OE.Activation	X												x														x								
OE.Approved_Workshops						X		X					x															x					x		
OE.Card_Availability		x																											x						
OE.Card_Traceability		x																												x					
OE.Controls						X		X	x	X	x		x		x	x	x	x													x				
OE.Driver_Card_Uniqueness		x																														x			
OE.Faithful_Calibration						X		x																									x		
OE.Management device																										x									
OE.Faithful_Drivers																																		x	
OE.Regular_Inspections						X		x		X	x	x	x		x		x																		x

	Threats																	OSPs							Assumptions								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
OE.Type_Approved_MS										X		x											x											

1 **Table 4 Security Objective rationale**

2

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

- **T.Access** is addressed by O.Authentication to ensure the identification of the user, O.Access to control access of the user to functions and O.Audit to trace attempts of unauthorised accesses. OE.Activation The activation of the TOE after its installation ensures access of the user to functions.
- **T.Identification** is addressed by O.Authentication to ensure the identification of the user, O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address this threat by storing all activity carried (even without an identification) with the VU. The OE.Driver_Card_Uniqueness, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.
- **T.Faults** is addressed by O.Reliability for fault tolerance. Indeed, if the TOE provides a reliable service as required by O.Reliability, the TOE cannot experience uncontrollable internal states. Hence, also each possible fault of the TOE will be controllable, i.e. the TOE will be in a wellknown state at any time. Therefore, threats grounding in faults of the TOE will be eliminated.
- **T.Tests** is addressed by O.Reliability and OE.Manufacturing. Indeed, if the TOE provides a reliable service as required by O.Reliability and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the TOE can neither enter any invalidated test mode nor have any back door. Hence, the related threat will be eliminated.
- **T.Design** is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Software_Analysis to prevent reverse engineering and by O.Output (RLB_206) to ensure that data output reflects accurately data measured or store. and O.Reliability (RLB_201, 204, 206).
- **T.Calibration_Parameters** is addressed by O.Access to ensure that the calibration function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive calibration data is accurate, by O.Integrity to maintain the integrity of calibration parameters stored. Workshops are approved by Member States authorities and are therefore trusted to calibrate properly the equipment (OE.Approved_Workshops, OE.Faithful_Calibration). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the VU, which helps addressing the threat.
- **T.Card_Data_Exchange** is addressed by O.Secured_Data_Exchange. O.Audit contributes to address the threat by recording events related to card data exchange integrity or authenticity errors. O.Reliability (ACR_201, 201a), O.Processing (ACR_201a).
- **T.Clock** is addressed by O.Access to ensure that the full time adjustment function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive time

adjustment data is accurate. Workshops are approved by Member States authorities and are therefore trusted to properly set the clock (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Faithful_Calibration), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.

- **T.Environment**: is addressed by O.Processing to ensure that processing of inputs to derive user data is accurate.and by O.Reliability to ensure that physical attacks are countered. OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.
- **T.Fake_Devices** is addressed by O.Access (ACC_205) O.Authentication (UIA_201 – 205, 207 – 211, 213, UIA_221 – 223), O.Audit (UIA_206, 214, 220), O.Processing (ACR_201a), O.Reliability (ACR_201, 201a), O.Secured_Data_Exchange (CSP_201 - 205). OE.Type_Approved_MS ensures that only motion sensors with correct identification data have the credentials that are required to successfully authenticate themselves. OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the whole installation.
- **T.Hardware** is mostly addressed in the user environment by O.Reliability, O.Output, O.Processing and by O.Audit contributes to address the threat by recording events related to hardware manipulation. The OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the installation.
- **T.Motion_Data** is addressed by O.Authentication, O.Reliability (UIA_206, ACR_201, 201a), O.Secured_Data_Exchange and OE.Regular_Inspections , OE.Type_Approved_MS. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.
- **T.Non_Activated** is addressed by the OE.Activation and OE.Delivery. Workshops are approved by Member States authorities and are therefore trusted to activate properly the equipment (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Controls), also contribute to address the threat.
- **T.Output_Data** is addressed by O.Output. O.Audit contributes to address the threat by recording events related to data display, print and download.
- **T.Power_Supply** is mainly addressed by O.Reliability to ensure appropriate behaviour of the VU against the attack. O.Audit contributes to address the threat by keeping records of attempts to tamper with power supply. OE.Controls includes controls by law enforcement officers of power supply interruption records held in the VU, which helps addressing the threat. OE.Regular_Inspections helps addressing the threat through installations, calibrations, checks, inspections , repairs tcarried out by trusted fitters and workshops.
- **T.Security_Data** is addressed by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport, OE.Software_Upgrade, OE.Controls. It is addressed by the O.Access, O.Processing, O..Secured_Data_Exchange to ensure appropriate protection while stored in the VU. O.Reliability (REU_201, RLB_206).

- **T.Software** is addressed in the user environment by the O.Output, O.Processing, and O.Reliability to ensure the integrity of the code. O.Audit contributes to address the threat by recording events related to integrity errors. During design and manufacture, the threat is addressed by the OE.Development objectives. O.Software_Upgrade (integrity of the new SW). OE.Controls, OE.Regular_Inspections (checking for the audit records related).
- **T.Stored_Data** is addressed mainly by O.Integrity, O.Access, O.Output and O.Reliability to ensure that no illicit access to data is possible. The O.Audit contributes to address the threat by recording data integrity errors. OE.Sofware_Upgrade ,included that Software revisions shall be security certified before they can be implemented in the TOE to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU, which helps addressing the threat.
- **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
- **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.

8 Extended components definition

8.1 Extended components definition

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

9 Security requirements

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

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 8.1 of Part 1 [CC_1]] of the CC. Each of these operations is used in this ST.

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

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

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this text is underlined and italicised like *this*. Assignment having been made by the ST author are *double underlined and italicised*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a 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.

9.1 Security functional requirements

The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in section 4 of the ITSEC vehicle unit GST in 3821_IB_10]. Each of the below SFRs includes in bold-face curly braces **{…}** a list of SEFs related. This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from 3821_IB_10]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

The complete coverage of the SEF(s) from 3821_IB_10] is documented in Annex A, chap.12 below.

9.1.1 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 und tachograph cards (according to3821_IB_10], sec. 4.1)	– FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_AFL.1/MS: Authentication failure: motion sensor – FIA_AFL.1/TC: Authentication failure: tachograph cards – (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE Supported by: – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards – (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1)

Security Functional Groups	Security Functional Requirements concerned
Access control to functions and stored data (according to 3821_IB_10], 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 Supported by: – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT – FMT_MSA.3/UDE – FMT_MSA.3/IS – (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)
Accountability of users (according to 3821_IB_10], 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

Security Functional Groups	Security Functional Requirements concerned
	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 3821_IB_10], 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 3821_IB_10], sec. 4.5)	– FDP_RIP.1 Subset residual information protection Supported by: – FCS_CKM.4: Cryptographic key destruction
Accuracy of recorded and stored data (according to 3821_IB_10], 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 Supported by: – (FDP_ACC.1/IS, FDP_ACF.1/IS): right input sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): limited manual entry – FAU_GEN.1: Audit records: Generation

Security Functional Groups	Security Functional Requirements concerned
	– 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
Reliability of services (according to 3821_IB_10], sec. 4.7)	– FDP_ITC.2//IS: no executable code from external sources – FPR_UNO.1: Unobservability of leaked data – FPT_FLS.1: Failure with preservation of secure state – FPT_PHP.2//Power_Deviation: Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services Supported by: – FAU_GEN.1: Audit records: Generation – (FDP_ACC.1/IS, FDP_ACF.1/IS): no executable code from external sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): Tachograph Card withdrawal – FMT_MOF.1: No test entry points
Data exchange with motion sensor, tachograph cards and external media (download function) (according to 3821_IB_10], 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

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

Table 5 Security functional groups vs. SFRs

9.1.2 Class FAU Security Audit

9.1.2.1 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_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[26][27] and {UIA_206, UIA_214, ACR_205, ACT_201, ACT_203,

[26]

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

ACT_204, ACT_205, AUD_201, AUD_202, AUD_203, RLB_203, RLB_206, RLB_210, RLB_214[28], DEX_202, DEX_204}; *no other specifically defined audit events.*

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 29}; *no other audit relevant information.*

9.1.2.2 FAU_SAR - Security audit review

FAU_SAR.1 Audit review **{AUD_205}**

Hierarchical to: -

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

FAU_SAR.1.1 The TSF shall provide everybody with the capability to read the recorded information according to REQ 011 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.

9.1.2.3 FAU_STG - Security audit event storage

FAU_STG.1 Protected audit trail storage **{ACT_206[30]}**.

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_201, ACT_206}**[31]

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 behave according to REQ 083, 086, 089, 092 and 105b if the audit trail is full.

[28] Last card session not correctly closed
[29] all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_203}
[30] REQ081 to 093 and REQ102 to 105a
[31] REQ105b

Application Note 10: The data memory shall be 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 3821_IB_10][32], 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.

9.1.3 Class FCO Communication

9.1.3.1 FCO_NRO Non-repudation 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.

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 information, and the data to be downloaded to external media 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 [3821_IB_11], sec. 6.1,

no further limitation on the evidence of origin.

9.1.4 Class FCS Cryptographic Support

9.1.4.1 FCS_CKM - Cryptographic key management

FCS_CKM.1 Cryptographic key generation **{CSP_202}**

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: is fulfilled by FCS_CKM.2; FCS_CKM.4 Cryptographic key destruction: is fulfilled by FCS_CKM.4

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

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

Key description	Algorithm and size	Standard, specification
Motion sensor Master key Km is temporarily stored key derived from the static key material within the workshop environment (OE.Approved_Worshops) outside of the VU's operational phase	Two keys TDES key	[16844-3]
Pairing key of the motion sensor K_p is temporarily stored key derived from the static key material within the workshop environment (OE.Approved_Worshops) outside of the VU's operational phase	Two keys TDES key	[16844-3]
motion sensor identification key K_{ID} is temporarily stored key derived from the static key material within the workshop environment (OE.Approved_Worshops) outside of the VU's operational phase	Two keys TDES key	[16844-3]
Session key between motion sensor and vehicle unit K_{sm}	Two keys TDES key	[16844-3]
session key between tachograph cards and vehicle unit K_{st}	Two keys TDES key	[3821_IB_11], CSM_020
Kt is temporarily stored key derived from the static key material within the workshop environment (OE.Approved_Worshops) outside of the VU's operational phase	*Two keys TDES key*	*As defined by the proprietary specification for the SW-Upgrade by the TOE developer*

FCS_CKM.2 Cryptographic key distribution **{CSP_203}**

Hierarchical to: -

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

FCS_CKM.4: is fulfilled by FCS_CKM.4

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

Distributed key	Standard, specification
session key between motion sensor and vehicle unit K_{sm}	[16844-3], 7.4.5
session key between tachograph cards and vehicle unit K_{st}	[3821_IB_11], CSM_020

FCS_CKM.3 Cryptographic key access **{CSP_204}**

Hierarchical to: -

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

a) fulfilled by FCS_CKM.1 for the session keys K_{SM} and K_{ST} as well as for the temporarily stored keys K_m, K_P and K_{ID};
b) fulfilled by FDP_ITC.2//IS for the temporarily stored key Km_{wc} (entry DEX_203);
c) not fulfilled, but **justified** for EUR.PK, EQT.SK, Km_{vu}: The persistently stored keys (EUR.PK, EQT_j.SK, Km_{vu}) will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

FCS_CKM.4: is fulfilled by FCS_CKM.4

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

Key	key access method and specification
Part of the Master key Km_{wc}	read out from the workshop card and temporarily stored in the TOE (calibration phase);
Motion sensor Master key Km	temporarily reconstructed from part of the Master key Km_{vu} and part of the Master key Km_{wc} , [3821_IB_11]], CSM_036, CSM_037 (calibration phase);
motion sensor identification key K_{ID}	temporarily reconstructed from the Master key Km a motion sensor identification key K_{ID} as specified in [16844-3], sec. 7.2, 7.4.3 (calibration phase)
Pairing key of the motion sensor K_p	temporarily reconstructed from Enc (Km_i K_p) a motion sensor identification key K_{ID} as specified in [16844-3], sec. 7.2, 7.4.3

Key	key access method and specification
	(calibration phase)
session key between motion sensor and vehicle unit K_{sm}	Internally generated and temporary stored during session between the TOE and the motion sensor connected (calibration and operational phases)
session key between tachograph cards and vehicle unit K_{st}	Internally generated and temporary stored during session between the TOE and the tachograph card connected (calibration and operational phases)
European public key EUR.PK	Stored during manufacturing of the TOE calibration and operational phases)
equipment private key EQT_i.SK	Stored during manufacturing of the TOE (calibration and operational phases)
part of the Master key Km_{vu}	Stored during manufacturing of the TOE (calibration and operational phases)
security device public key SECDEV.PK	*Stored during manufacturing of the TOE*
transport key software upgrade Kt	*temporarily decoded from the transmitted data from the management device (at most by the end of the software upgrade)*
Individual device key K_{vu}	*Stored during manufacturing of the TOE*

1

2 **FCS_CKM.4** Cryptographic key destruction **{CSP_205}**

Hierarchical to: -

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

3 ***FCS_CKM.4.1*** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic
4 key destruction method as specified below that meets the following list of standards*:*

Key	key destruction method
Part of the Master key Km_{wc}	delete after use (at most by the end of the calibration phase)
Motion sensor Master key Km	Delete after use use (at most by the end of the calibration phase)
motion sensor identification key K_{ID}	delete after use (at most by the end of the calibration phase)

Key	key destruction method
Pairing key of the motion sensor K_p	delete after use (at most by the end of the calibration phase)
session key between motion sensor and vehicle unit K_{sm}	Delete for replacement (by closing a motion sensor communication session during the pairing process)
session key between tachograph cards and vehicle unit K_{st}	Delete for replacement (by closing a card communication session)
European public key EUR.PK	These public keys does not represent any secret and, hence, needn't to be deleted.
equipment private key 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
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
Individual device key K_{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*
security device public key SECDEV.PK	*These public keys does not represent any secret and, hence, needn't to be deleted.*
transport key software upgrade Kt	*Delete after use use (at most by the end of the calibration phase)*

***Application Note 11*:** 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

9.1.4.2 FCS_COP Cryptographic operation

FCS_COP.1/TDES Cryptographic operation **{CSP_201}**

Hierarchical to: -

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

FCS_CKM.4: is fulfilled by FCS_CKM.4

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: [16844-3] for the Motion Sensor and [3821_IB_11] 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: [3821_IB_11] for the Tachograph Cards authentication and [3821_IB_11], CSM_034 for downloading to external media, respectively..

Application Note 12: It is a matter of RSA decrypting and verifying in the context of CSM_020 ([3821_IB_11] – VU <-> TC authentication) using static keys imported outside the VU's operational phase (OE.Sec_Data_xx). Due to this fact the dependency FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 is not applicable to these keys.

9.1.5 Class FDP User Data Protection

9.1.5.1 FDP_ACC Access control policy

FDP_ACC.1/FIL Subset access control **{ACC_211}**

Hierarchical to: -

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

FDP_ACC.1.1/FIL The TSF shall enforce the File_Structure SFP on *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 *the subjects, objects, and operations as referred 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},***
- *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 access control SFP DATA on *the subjects, objects, and operations as required in:*

- *VU identification data: **{ACT_202}** (REQ075: structure) and **{ACC_204}** (REQ076: once recorded),*
- *MS identification data: **{ACC_205}** (REQ079: Manufacturing-ID and REQ155: pairing),*
- *Calibration Mode Data: **{ACC_207}** (REQ097) and **{ACC_209}** (REQ100),*
- *Security Data: **{ACC_210}** (REQ080),*
- *MS Audit Records: **{AUD_204}** [33]*

*as required by **ACC_201**.*

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

Hierarchical to: -

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

FDP_ACC.1.1/UDE The TSF shall enforce the SFP User_Data_Export on *the subjects, objects, and operations as required in 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 *the subjects, objects, and operations as required in {ACR_201, RLB_205}.*

FDP_ACC.1/SW-Upgrade Subset access control **{RLB_205}**

[33] 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.

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 *the subjects, objects, and operations as required in {RLB_205}.*

9.1.5.2 FDP_ACF - Access control functions

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

Hierarchical to: -

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

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

FDP_ACF.1.1/FIL The TSF shall enforce the File Structure SFP to objects based on the following*: the entire files structure of the TOE-application as required by ACC_211.*

FDP_ACF.1.2/FIL The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: none.

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

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

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

Hierarchical to: -

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

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

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

- *operational modes {ACC_202} and the related restrictions on access rights {ACC_203},*
- *calibration functions { ACC_206} and time adjustment {ACC_208}*
- *limited manual entry, {ACR_201a} and*
- *Tachograph Card withdrawal {RLB_213}.*

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

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

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

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

Hierarchical to: -

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

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

FDP_ACF.1.1/DAT The TSF shall enforce the SFP_DATA to objects based on the following: *the subjects, objects, and their attributes listed in FDP_ACC.1/DAT above.*

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

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

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

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

Hierarchical to: -

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

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

FDP_ACF.1.1/UDE The TSF shall enforce SFP_User_Data_Export to objects based on the following: *the subjects, objects, and their attributes as referred in REQ109 and 109a*.

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

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

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

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

Hierarchical to: -

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

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

FDP_ACF.1.1/IS The TSF shall enforce SFP_Input_Sources to objects based on the following: *the subjects, objects, and their attributes as referred in **{ACR_201, RLB_205}**.*

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[34]}.

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

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

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

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/Software-Upgrade

FMT_MSA.3: is fulfilled by FMT_MSA.3/Software-Ipgrade

FDP_ACF.1.1/SW-Upgrade The TSF shall enforce *SFP_SW-Upgrade* to objects based on the following: *the subjects*, objects, and their attributes as referred in {RLB_205}.

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: *rules as defined by FDP_ITC.2/SW-Upgrade*.

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: all data not recognized as an authentic SW-Upgrade*.

9.1.5.3 FDP_ETC Export from the TOE

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

Hierarchical to: -

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

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

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported 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.

9.1.5.4 FDP_ITC Import from outside of the TOE

[34] Especially for the MS and the TC

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, DEX_201, DEX_202, DEX_203, DEX_204, RLB_205}**

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 ST.

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:
- [16844-3] for the Motion Sensor {ACR_201, DEX_201}
- DEX_202 (audit record and continue to use imported data)
- [3821_IB_11] 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/Software-Upgrade

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

Indeed, trusted channel VU<->MD 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//Software-Upgrade + FDP_ETC.2 + FIA_UAU.1/MDMS)}, it can be dispensed with this dependency in the current context of the ST.

FPT_TDC.1: is fulfilled by FPT_TDC.1//Software-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-Upgrade The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *only data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they must be rejected.*

9.1.5.5 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:

Object Reuse for
Part of the Master key Km_{wc} (at most by the end of the calibration phase)
Motion sensor Master key Km (at most by the end of the calibration phase)
motion sensor identification key K_{ID} (at most by the end of the calibration phase)
Pairing key of the motion sensor K_p (at most by the end of the calibration phase)

Object Reuse for
session key between motion sensor and vehicle unit K_{sm} (when its temporarily stored value is not in use anymore)
session key between tachograph cards and vehicle unit K_{st} (by closing a card communication session)
equipment private key EQT_j.SK (when its temporarily stored value is not in use anymore)
part of the Master key Km_{vu} (when its temporarily stored value is not in use anymore)
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)
transport key software upgrade Kt (at most by the end of the calibration phase)

***Application Note 13*:** 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 14*:** 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.

9.1.5.6 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity **{ACR_204, ACR_205}**

Hierarchical to: -

Dependencies: -

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

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

Application Note 15: The context for the current SFR is built by the related requirements ACR_204, ACR_205 (sec. 4.6.3 of 3821_IB_10] 'Stored data integrity'). This context gives a clue for interpretation that it is not a matter of temporarily, but of permanently stored user data.[35]

9.1.6 Class FIA Identification and Authentication

9.1.6.1 FIA_AFL Authentication failures

FIA_AFL.1/**MS** Authentication failure handling **{UIA_206}**

[35] see definition in glossary

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 16*:** The positive integer number expected above shall be ≤ 20, cf. UIA_206 in 3821_IB_10].

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 and the card as non valid[36] (definition z and REQ007).

FIA_AFL.1/Remote Authentication failure handling **{UIA_220}**

Hierarchical to: -

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

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

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

- *warn the remotely connected company*.

9.1.6.2 FIA_ATD User attribute definition

FIA_ATD.1//TC User attribute definition **{UIA_208, UIA_216}**

[36] is commensurate with 'Unknown equipment' in the current PP

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, UIA_216}.

9.1.7 FIA_UAU User authentication

FIA_UAU.1/TC Timing of authentication **{UIA_209, UIA_217}**

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[37].

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[38]

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[39].

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/TC[40]

FIA_UAU.1.1/MD The TSF shall allow *MD identification* on behalf of the user to be performed before the user is authenticated[41].

[37] According to CSM_20 in [3821_IB_11] the TC identification (certificate exchange) is to perform strictly before the mutual authentication between the VU and the TC.

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

[39] According to CSM_20 in [3821_IB_11] the TC identification (certificate exchange) is to perform strictly before the PIN authentication of the Workshop Card.

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

[41] According to the respective communication protocol the MD identification (certificate exchange) is to perform strictly before the authentication of the MD.

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}**[42].

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, UIA_219}**

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, UIA_218}.**

Hierarchical to: -

Dependencies: -

[42] 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.

FIA_UAU.5.1/TC The TSF shall provide multiple authentication mechanisms according to CSM_20 in [3821_IB_11] to support user authentication.

FIA_UAU.5.2/TC The TSF shall authenticate any user's claimed identity according to the CSM_20 in [3821_IB_11].

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 30 seconds, in power save mode up to 45 minutes*.

***Application Note 17*:** The condition under which re-authentication is required expected above shall be more frequently than once per hour, cf. UIA_204 in 3821_IB_10].

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 *twice a day*.

***Application Note 18*:** The condition under which re-authentication is required expected above shall be more frequently than once per day, cf. UIA_210 in 3821_IB_10].

9.1.7.3 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, UIA_215}**

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.

9.1.8 Class FMT Security Management

9.1.8.1 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[43] 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.

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

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

FMT_MSA.3/UDE Static attribute initialisation

Hierarchical to: -

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

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

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

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

FMT_MSA.3/IS Static attribute initialisation

Hierarchical to: -

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

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

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

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

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.

9.1.8.2 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.

9.1.8.3 Specification of Management Functions (FMT_SMF)

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 mode as specified in REQ 010.

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.

9.1.9 Class FPR Privacy (FPR)

9.1.9.1 FPR_UNO - Unobservability

FPR_UNO.1 Unobservability **{RLB_204 for leaked data}**

Hierarchical to: -

Dependencies: -

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

***Application Note 19*:** 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'.

9.1.10 Protection of the TSF (FPT)

9.1.10.2 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}.

9.1.10.3 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.

***Application Note 20*:** Is a matter of RLB_209: this function (detection of power deviation) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a wrong way for RLB_209. Due to this fact the dependency FMT_MOF.1 is not applicable.

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.

9.1.10.4 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 21: This requirement is the matter of the VU's real time clock.

9.1.10.5 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 [16844-3] for the Motion Sensor and by [3821_IB_11] 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 [16844-3] for the Motion Sensor and by [3821_IB_11] 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 *secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2//SW-Upgrade The TSF shall use *the interpretation rules (communication protocols) as defined by the proprietary specification for the SW-Upgrade by the TOE developer* when interpreting the TSF data from another trusted IT product.

***Application Note 22*:** Trusted IT product in this case is a special device of the SW-Upgrade issuer preparing the new software for distribution.

9.1.10.6 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)**.

FPT_TST.1.2 The TSF shall verify the integrity of security data .

FPT_TST.1.3 The TSF shall verify the integrity of stored executable code.

9.1.11 Resource Utilisation (FRU)

9.1.11.7 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 *controlled resources* shall be mediated on the basis of the subjects assigned priority.

Application Note 23: The current assignment is to consider in the context of RLB_212 (sec. 4.7.6 of 3821_IB_10] 'Data availability'). Controlled resources in this context may be 'functions and data covered by the current set of SFRs'.

9.2 Security assurance requirements

The European Regulation [3821_IB] requires for a vehicle unit the assurance level ITSEC E3, high 3821_IB_10] as specified in 3821_IB_10], chap. 6 and 7.

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

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

The CC community acts on the presumption that the assurance components of CCv3.1 and CCv2.x are equivalent to each other. Due to this fact, the author of the PP compiled and defined an appropriate assurance package **E3hCC31_AP** as shown below (validity of this proposal is confined to the Digital Tachograph System).

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

Assurance Classes	Assurance Family	E3hCC31_AP (based on EAL4)
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	STE_FUN	1
	ATE_IND	2
AVA Vulnerability Assessment	AVA_VAN	5

***Application Note 24*:** The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

***Application Note 25*:** The requirement RLB_215 is covered by ADV_ARC (security domain separation); the requirement RLB_204 is partially covered by ADV_ARC (self-protection).

9.3 Security requirements rationale

9.3.1 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.

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FAU_GEN.1	Audit data generation		**x**	**x**								
FAU_SAR.1	Audit review		**x**	**x**								
FAU_STG.1	Protected audit trail storage		**x**	**x**		**X**						
FAU_STG.4	Prevention of audit data loss		**x**	**x**								
FCO_NRO.1	Selective proof of origin						**x**			**x**		
FCS_CKM.1	Cryptographic key generation									**x**		**x**
FCS_CKM.2	Cryptographic key distribution									**x**		
FCS_CKM.3	Cryptographic key access									**x**		**x**
FCS_CKM.4	Cryptographic key destruction									**x**		**x**
FCS_COP.1/TDES	Cryptographic operation									**x**		**x**
FCS_COP.1/RSA	Cryptographic operation									**x**		**x**
FDP_ACC.1/FIL	Subset access control	**x**										
FDP_ACC.1/FUN	Subset access control	**x**						**x**	**x**	**x**	**x**	
FDP_ACC.1/DAT	Subset access control	**x**										

		Security objectives										
		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_ACC.1/UDE	Subset access control	x										
FDP_ACC.1/IS	Subset access control	x						x	x			
FDP_ACC.1/ SW-Upgrade	Subset access control	x						x	x		x	x
FDP_ACF.1/FIL	Security attribute based access control	x										
FDP_ACF.1/FUN	Security attribute based access control	x						x	x	x	x	
FDP_ACF.1/DAT	Security attribute based access control	x										
FDP_ACF.1/UDE	Security attribute based access control	x										
FDP_ACF.1/IS	Security attribute based access control	x						x	x			
FDP_ACF.1/ SW-Upgrade	Security attribute based access control	x						x	x		x	x
FDP_ETC.2	Export of user data with security attributes		x			x	x			X		
FDP_ITC.1	Import of user data without security attributes							x	x			
FDP_ITC.2/IS	Import of user data with security attributes							x	x	X		
FDP_ITC.2/SW-Upgrade	Import of user data with security attributes							x	x		x	x
FDP_RIP.1	Subset residual information protection	x						x	x			

		Security objectives										
		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_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							
FIA_AFL.1/Remote	Authentication failure handling			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		

		Security objectives										
		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
FIA_UID.2/MD	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						x	x		x	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.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			

		Security objectives										
		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**	**x**	**x**		**x**	**x**
FPT_TST.1	TSF testing			**x**					**x**			
FRU_PRS.1	Limited priority of service								**x**			

1

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

security objectives	Security functional requirement	
O.Access	***FDP_ACC.1/FIL***	File structure SFP on application and data files structure
	FDP_ACC.1/FUN	SFP FUNCTION on the functions of the TOE
	FDP_ACC.1/DAT	SFP DATA on user data of the TOE
	FDP_ACC.1/UDE	SFP User_Data_Export for the export of user data
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACC.1/SW-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 the deallocation of the resource
	FIA_UAU.5/TC	Multiple authentication mechanisms according to CSM_20 in [3821_IB_11] to support user authentication.
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	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**.**

security objectives	Security functional requirement	
	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 *n*obody 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 *r*estrictive 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 *r*estrictive 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	Restrict the ability to enable the test functions 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

security objectives	Security functional requirement	
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	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	Provides authentication failure events for the motion sensor
	FIA_AFL.1/TC	Provides authentication failure events for the tachograph cards
	FIA_AFL.1/Remote	Provides authentication failure events for the remotely connected company
	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,

security objectives	Security functional requirement	
		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_AFL.1/Remote	Detects and records authentication failure events for the remotely connected company
	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 CSM_20 in [3821_IB_11] 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 access control SFP User_Data_Export

security objectives	Security functional requirement	
	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 access control 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 DTCO 1381 Rel. 2.0 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.
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon the deallocation of the resource

security objectives	Security functional requirement	
	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. 2.0 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 [16844-3] for the Motion Sensor and by[3821_IB_11] 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 DTCO 1381 Rel. 2.0 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

security objectives	Security functional requirement	
	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 the deallocation of the resource
	FDP_SDI.2	monitors user data stored for integrity error
	FIA_AFL.1/MS	Provides authentication failure events for the motion sensor
	FIA_AFL.1/TC	Provides authentication failure events for the tachograph cards
	FMT_MOF.1	Restrict the ability to enable the functions specified in **{RLB_201}** 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/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,**

security objectives	Security functional requirement	
		RLB_210, RLB_211}
	FPT_PHP.2/Power_Deviation	Detection of physical tampering (Power_Deviation) and generation of an audit record
	FPT_PHP.3	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1/IS	Provides the capability to consistently interpret secure messaging attributes as defined by [16844-3] for the Motion Sensor and by[3821_IB_11] 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 DTCO 1381 Rel. 2.0 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	Generates of session keys for the motion sensor and the tachograph cards
	FCS_CKM.2	Controls distribution of cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the table below that meets the following list of standards.
	FCS_CKM.3	Controls cryptographic key access and storage in the TOE
	FCS_CKM.4	Destroys cryptographic keys in the TOE
	FCS_COP.1/TDES	Provides the cryptographic operation TDES
	FCS_COP.1/RSA	Provides the cryptographic operation RSA
	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_ITC.2/IS	Provides import of user data from outside of the

security objectives	Security functional requirement	
		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 [3821_IB_11] 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
	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_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/SW-	Defines security attributes for SFP SW-Upgrade

security objectives	Security functional requirement	
	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/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/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 DTCO 1381 Rel. 2.0 developer
O.Software_Upgrade	***FCS_COP.1/TDES***	Provides the cryptographic operation TDES.
	FCS_COP.1/RSA	Provides the cryptographic operation RSA
	FCS_CKM.1	Generates of session keys for the motion sensor and the tachograph cards
	FCS_CKM.3	Controls cryptographic key access and storage in the TOE
	FCS_CKM.4	Destroys cryptographic keys in the TOE
	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_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
	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

security objectives	Security functional requirement	
		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 DTCO 1381 Rel. 2.0 developer

9.3.2 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.9.1 above. All dependencies being expected by CC part 2 are either fulfilled or their non-fulfilment is justified..

9.3.3 Security Assurance Requirements Rationale

The current security target is claimed to be conformant with the assurance package E3hCC31_AP (cf. sec. 5.3 above). As already noticed there in sec. 9.2, the assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

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

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects and external

entities, entry 'Attacker'). This decision represents a part of the conscious security policy for the recording equipment required by the legislative [3821_IB] 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 6 SAR Dependencies

9.3.4 Security Requirements – Internal Consistency

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

a) SFRs

The dependency analysis in section 9.3.2 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 9.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current PP accurately and completely reflects the Generic Security Target 3821_IB_10]]. Since the GST 3821_IB_10] is part of the related legislation, it is assumed to be internally consistent. Therefore, due to conformity between the

current ST and 3821_IB_10], also subjects and objects being used in the current ST are used in a consistent way.

b) SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 9.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 9.3.2Rationale for SFR's Dependencies and 9.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 9.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

1 10 TOE summary specification

2 The TOE provides the following security services:

TOE_SS.Identification_Authentication

The TOE provides this security service of identification and authentication of the motion sensor, of users by monitoring the tachograph cards.

Detailed properties of this security service are described in Annex A (Requirements UIA_201 to UIA_223 as defined in 3821_IB_10]

Security functional requirements concerned:

- FIA_UID.2/MS: Identification of the motion sensor
- FIA_UID.2/TC: Identification of the tachograph cards
- (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor
- (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards
- FIA_UAU.1/PIN: additional PIN authentication for the workshop card
- FIA_AFL.1/MS: Authentication failure: motion sensor
- FIA_AFL.1/TC: Authentication failure: tachograph cards
- (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE

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_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management
- FAU_GEN.1: Audit records: Generation
- (FMT_MSA.1, FMT_SMF.1)

TOE_SS.Access

The TOE provides this security service of access control for access to functions and data of the TOE according to the

mode of operation selection rules.

Detailed properties of this security service are described in Annex A (Requirements ACC_201 to ACC_211 as defined in 3821_IB_10]

Security functional requirements concerned:

- (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

Supported by:

- (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor
- (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards
- FIA_UAU.1/PIN: additional PIN authentication for the workshop card
- FMT_MSA.3/FIL
- FMT_MSA.3/FUN
- FMT_MSA.3/DAT
- FMT_MSA.3/UDE
- FMT_MSA.3/IS
- (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)

TOE_SS.Accountability

The TOE provides this security service of accountability for collection of accurate data in the TOE.

Detailed properties of this security service are described in Annex A (Requirement ACT_201 to ACT_207 as defined in 3821_IB_10]

Security functional requirements concerned:

- 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
TOE_SS.Audit	The TOE provides this security service of audit related to attempts to undermine the security of the TOE and provides the traceability to associated users. Detailed properties of this security service are described in Annex A (Requirements AUD_201 to AUD_205 as defined in 3821_IB_10] **Security functional requirements concerned:** ▪ 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.
TOE_SS.Object_Reuse	The TOE provides this security service of object reuse to ensure that temporarily stored sensitive objects are destroyed. Detailed properties of this security service are described in Annex A (Requirement REU_201 as defined in). 3821_IB_10] **Security functional requirements concerned:** ▪ FDP_RIP.1 Subset residual information protection ▪Supported by: ▪ FCS_CKM.4: Cryptographic key destruction
TOE_SS.Reliability	The TOE provides this security service of reliability of service: self-tests, no way to analyse or debug software in the field, detection of specified hardware sabotage and deviations from the specified voltage values including cut-off of the power supply. Detailed properties of this security service are described in Annex A (Requirements RLB_201 to RLB_215 as defined in). 3821_IB_10]

Security functional requirements concerned:

- FDP_ITC.2//IS: no executable code from external sources
- FPR_UNO.1: Unobservability of leaked data
- FPT_FLS.1: Failure with preservation of secure state
- FPT_PHP.2//Power_Deviation: Notification of physical attack
- FPT_PHP.3: Resistance to physical attack: stored data
- FPT_TST.1: TSF testing
- FRU_PRS.1: Availability of services
- FDP_ACC.1/SW-Upgrade
- FDP_ACF.1/SW-Upgrade
- FDP_ITC.2/SW-Upgrade
- FPT_TDC.1/SW-Upgrade
- FMT_MSA.3SW-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

TOE_SS.Accuracy

The TOE provides this security service of accuracy of stored data in the TOE.

Detailed properties of this security service are described in Annex A (Requirements ACR_201 to ACR_205 as defined in 3821_IB_10]

Security functional requirements concerned:

- FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC)
- FDP_ITC.2//IS: right input sources with sec. attributes (MS and TC)
- FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC)
- FDP_SDI.2: Stored data integrity

	Supported by: ▪ (FDP_ACC.1/IS, FDP_ACF.1/IS): right input sources ▪ (FDP_ACC.1/FUN, FDP_ACF.1/FUN): limited manual entry ▪ FAU_GEN.1: Audit records: Generation ▪ FPT_STM.1: Reliable time stamps ▪ (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor ▪ (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards
TOE_SS.Data_Exchange	The TOE provides this security service of data exchange with the motion senor and tachograph cards and connected entities for downloading. Detailed properties of this security service are described in Annex A (Requirement DEX_201 to DEX_208 as defined in 3821_IB_10]). **Security functional requirements concerned:** ▪FCO_NRO.1: Selective proof of origin for data to be downloaded to external media ▪ FDP_ETC.2 Export of user data with security attributes: to the TC and to external media ▪ FDP_ITC.2//IS Import of user data with security attributes: from the MS and the TC ▪Supported by: ▪ FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) ▪ FCS_COP.1/RSA: for data downloading to external media (signing) ▪ (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management ▪ (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media ▪ (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC ▪ FAU_GEN.1: Audit records: Generation
TOE_SS.Cryptographic_support	The TOE provides this security service of cryptographic support using standard cryptographic algorithms and procedures.

Detailed properties of this security service are described in Annex A (Requirement CSP_201 to CSP_205 as defined in 3821_IB_10]).

Security functional requirements concerned:

- FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging)
- FCS_COP.1/RSA: for data downloading to external media (signing)
- (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management

Application Note 26: The following requirements of the generic security target 3821_IB_10] are not fulfilled by the TOE security services:

- UIA_202: is covered by OSP.Type_Approved_MS
- ACR_202. ACR_203 are not applicable because the TOE is a single protected entity.
- RLB_207, RLB_208: the optional list of the hardware sabotage events in the sense of this requirement represents an empty set for the current TOE.

11 Reference documents

[16844-3].....**ISO 16844-3**, Road vehicles, Tachograph systems, Part 3: Motion sensor interface, First edition, 2004-11-01, Corrigendum 1, 2006-03-01

[2135].....**Council Regulation (EC) No. 2135/98** of 24. September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85

[3821].....**Council Regulation (EEC) No. 3821/85** of the 20. December 1985 on recording equipment in road transport.

[3821_IB].....**Annex IB** of Council Regulation (EEC) No. 3821/85 amended by CR (EC) No. 1360/2002 and last amended by CR (EU) No. 1266/2009

[3821_IB_1].....**Appendix 1** of Annex I B of Council Regulation (EEC) No. 3821/85 - Data Dictionary

[3821_IB_2].....**Appendix 2** of Annex I B of Council Regulation (EEC) No. 3821/85 - Tachograph Cards Specification

[3821_IB_10].....**Appendix 10** of Annex I B of Council Regulation (EEC) No. 3821/85 - Generic Security Targets

[3821_IB_11].....**Appendix 11** of Annex I B of Council Regulation (EEC) No. 3821/85 - Common security mechanisms

[CC].....**Common Criteria** for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009, CCMB-2009-07-(01 to 03)

[CC_1].....**Common Criteria** for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Recision 3, July 2009

[CC_2].....**Common Criteria** for Information Technology Security Evaluation, Part 2: Aecurity Functional Components; CCMB-2009-07-002, Version 3.1, Recision 3, July 2009

[CC3].....**Common Criteria** for Information Technology Security Evaluation, Part3: Security Assurance Requirements CCMB-2009-07-003, Version 3.1, Recision 3, July 2009

[CEM].....**Common Methodology** for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1, Recision 3, July 2009

[DES] .....**Data, Encryption Standard**. National Institute of Standards and Technology (NIST). FIPS Publication 46-3:.Draft 1999

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

[1360].....**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

[ISO 7816-4].....ISO/IEC 7816-4 Information technology . Identification cards. Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.

[ISO 7816-8].....ISO/IEC 7816-8 Information technology . Identification cards . Integrated circuit(s) cards with contacts. Part 8: Security related interindustry commands. First Edition: 1999.

[SHA-1] .....SHA-1 National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. April 1995

[PKCS1]] ..... RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October 1998Annex A

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

12 Annex A

The following table demonstrates the coverage of the requirements of 3821_IB_10] chapter 4 by the security functional requirements from [CC], part2 specified in section 9.1.

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	TOE_SS.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 (*period TBD by manufacturer: every 30 seconds, in power save mode up to 45 minutes and more frequently than once per hour*) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.	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 (*TBD by manufacturer: 2 and not more than 20)* 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 SEF 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
UIA_208	The user identity shall consist of: - a user group: - DRIVER (driver card), - CONTROLLER (control card), - WORKSHOP (workshop card),	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)

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	- 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	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: every 12 hours 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 SEF 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_215	For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.	FIA_UID.2/TC
UIA_216	The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.	FIA_ATD.1/TC

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
UIA_217	The VU shall successfully authenticate the remotely connected company before allowing any data export to it.	FIA_UAU.1/TC
UIA_218	Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.	FIA_UAU.5/TC
UIA_219	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_220	After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall: warn the remotely connected company.	FIA_AFL.1/Remote
UIA_221	For every interaction with a management device, the VU shall be able to establish the device identity.	FIA_UID.2/MD
UIA_222	Before allowing any further interaction, the VU shall successfully authenticate 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
	TOE_SS.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	FDP_ACC.1/DAT

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	write access rules (requirements 079 and 155)	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.
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
	TOE_SS.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 FAU_STG.4 for REQ105b FDP_ACC.1/UDE FDP_ACF.1/UDE

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
		FDP_ETC.2 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
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 REQ105b
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
	TOE_SS.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,	FAU_GEN.1 for AUD_202

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	- 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.	
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
	F.Object Reuse	
REU_201	The VU shall ensure that temporary storage objects can be reused without this involving inadmissible information flow.	FDP_RIP.1
	TOE_SS.Accuracy	
ACR_201	The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources: – vehicle motion data, – VU's real time clock, – recording equipment calibration parameters, – tachograph cards, – user's inputs.	FDP_ACC.1/IS 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 separated parts of the	*Since the TOE is a single protected entity, this requirement*

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	VU, the data shall be protected from modification.	*does not apply*
ACR_203	Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.	*Since the TOE is a single protected entity, this requirement does not apply*
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 SEF shall generate an audit record.	FDP_SDI.2, FAU_GEN.1
	TOE_SS.Reliability	
RLB_201	a) 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. b) VU shall care: It shall not be possible to restore them for later use.	FMT_MOF.1 for the property b) The property a) is formulated as OSP.Test_Points.
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 SEF shall: – generate an audit record (except in calibration mode), – preserve the stored data integrity.	FAU_GEN.1 for an audit record FPT_FLS.1 for preserving the stored data integrity
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_ACC.1/SW-Upgrade FDP_ACF.1/SW-Upgrade FDP_ITC.2/SW-Upgrade FPT_TDC.1/SW-Upgrade FMT_MSA.3SW-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	FAU_GEN.1 for auditing,

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	case, the SEF 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).	
RLB_207	After its activation, the VU shall detect specified (*TBD by manufacturer*) hardware sabotage:	The list of the specified HW sabotage is an empty set for the current TOE. Hence, no SFR is required in order to cover this item.
RLB_208	In the case described above, the SEF shall generate an audit record and the VU shall: (*TBD by manufacturer*).	This requirement depends on RLB_207: If the latter is not implemented, the current requirement cannot be implemented.
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
RLB_210	In the case described above, the SEF shall: • 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.	FAU_GEN.1 for auditing FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset (cf. also RLB_203 and RLB_211)
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 be 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 must 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 SEF 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)
	TOE_SS.Data Exchange	

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
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 SEF 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 SEF 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
	TOE_SS.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
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
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