Digital Tachograph
DTCO 1381 Security Target

Project:	**DTCO 1381, Release 4.0e and 4.0ed**
Author:	Norbert Köhn, VNI CVS S3 EMEA TS HM
Status:	released
Filename:	1381R4ed.HOM.4465.Security_Target.docx

Table of content

History 2
List of terms and abbreviations 4
Terms 4
Abbreviations 7
List of figures 9
List of tables 10
1 ST Introduction 11
1.1 ST reference 11
1.2 TOE overview 11
1.2.1 TOE definition and operational usage 11
1.2.2 TOE Configurations 13
1.2.3 TOE major security features for operational use 14
1.2.4 TOE Type 15
1.2.5 TOE connectivity 17
1.2.6 Configuration of the TOE as vehicle unit 18
2 Conformance claims 20
2.1 CC conformance claim 20
2.2 PP claim 20
2.3 Package claim 20
2.4 2.4 Conformance claim rationale 20
3 Security problem definition 22
3.1 Introduction 22
3.1.1 Assets 22
3.1.2 Subjects and external entities 23
3.2 Threats 24
3.3 Assumptions 25
3.4 Organisational security policies 26
4 Security objectives 27
4.1 Security objectives for the TOE 27
4.2 Security objectives for the operational environment 27
5 Extended components definition 30
5.1 Rationale for extended component 30
5.2 Extended component definition 30
5.2.1 FCS_RNG Generation of random numbers 30
6 Security requirements 31
6.1 Security functional requirements for the TOE 31
6.1.1 Security functional requirements for the VU 31
6.1.2 Security functional requirements for external communications (2nd Generation) 52
6.1.3 Security functional requirements for external communications (1st generation) 58
6.2 Security assurance requirements for the TOE 61
7 Rationale 62
7.1 Security objectives rationale 62
7.2 Security requirements rationale 65

7.2.1 Rationale for SFRs' dependencies 65
7.2.2 Security functional requirements rationale 69
7.2.3 Security Assurance Requirements Rationale 81
7.2.4 Security Requirements – Internal Consistency 82
8 TOE summary specification 83
8.1 TOE_SS.Identification_Authentication 83
8.2 TOE_SS.Access_Control 83
8.3 TOE_SS.Accountability of users 84
8.4 TOE_SS.Audit of events and faults 84
8.5 TOE_SS.Residual information protection for secret data 85
8.6 TOE_SS.Integrity and authenticity of exported data 85
8.7 TOE_SS.Stored_Data_Accuracy 85
8.8 TOE_SS.Reliability 86
8.9 TOE_SS.Data_Exchange 86
8.10 TOE_SS.Cryptographic_support 86
9 Reference documents 87
Common Criteria 87
10 Annex A – Key & Certificate Tables 89
11 Annex B – Operations for FCS_RNG.1 103
11.1 Class PTG.2 103
11.2 Class PTG.3 103
11.3 Class DRG.2 104
11.4 Class DRG.3 104
11.5 Class DRG.4 105
11.6 Class NTG.1 105
12 Annex C – List of used cryptographic methods 107
12.1 Annex C.1 - General 107
12.2 Annex C.2 – List of cryptographic mechanisms 107

List of terms and abbreviations

Terms

Term	Meaning
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 approved to do so by an EU Member State, so that the assumption A.Approved_Workshops is fulfilled.
Attacker	Threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained.
Authentication	A function intended to establish and verify a claimed identity.
Authentication data	Data used to support verification of the identity of an entity.
Authenticity	The property that information is coming from a party whose identity can be verified.
Calibration	Updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Member State) and vehicle characteristics (w, k, l, tyre size, speed limiting device setting (if applicable), current UTC time, current odometer value); during the calibration of a recording equipment, the types and identifiers of all type approval relevant seals in place shall also be stored in the data memory. Any update or confirmation of UTC time only, shall be considered as a time adjustment and not as a calibration. Calibration of recording equipment requires the use of a workshop card.
Company card	A tachograph card issued by the authorities of a Member State to a transport undertaking needing to operate vehicles fitted with a tachograph, which identifies the transport undertaking, and allows for the displaying, downloading and printing of the data, stored in the tachograph, which have been locked by that transport undertaking.
Control card	A tachograph card issued by the authorities of a Member State to a national competent control authority that identifies the control body and, optionally, the control officer. It allows access to the data stored in the data memory or in the driver cards and, optionally, in the workshop cards for reading, printing and/or downloading. It also gives access to the roadside calibration checking function, and to data on the remote early detection communication reader.
Data memory	An electronic data storage device built into the recording equipment.
Digital Signature	Data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data.
Downloading	The copying, together with the digital signature, of a part, or of a complete set, of data files recorded in the data memory of the vehicle unit or in the memory of a tachograph card, provided that this process does not alter or delete any stored data.
Driver card	A tachograph card, issued by the authorities of a Member State to a particular driver that identifies the driver and allows for the storage of driver activity data.
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)

Term	Meaning
Event	An abnormal operation detected by the smart tachograph that may result from a fraud attempt.
External GNSS Facility	A facility that contains the GNSS receiver when the vehicle unit is not a single unit as well as other components needed to protect the communication of position data to the rest of the vehicle unit.
Fault	An abnormal operation detected by the smart tachograph that may arise from an equipment malfunction or failure.
GNSS Receiver	An electronic device that receives and digitally processes the signals from one or more Global Navigation Satellite System(s) (GNSS) in order to provide position, speed and time information.
Human user	A legitimate user of the TOE being a driver, controller, workshop or company. A human user is in possession of a valid tachograph card.
Identification data	Identification data include VU identification data. Identification data are part of User data.
Installation	The mounting of a tachograph in a vehicle.
Integrity	The property of accuracy and completeness of information.
Intelligent Dedicated Equipment	The equipment used to perform data downloading to the external storage medium (e.g. personal computer).
Interface	A facility between systems that provides the media through which they can connect and interact.
Interoperability	The capacity of systems and the underlying business processes to exchange data and to share information.
Manufacturer	The generic term for a VU Manufacturer producing and completing the VU as the TOE.
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. 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)	An organisation established by a Member State Authority, responsible for implementation of the MSA policy and for signing certificates for public keys to be inserted in equipment (vehicle units or tachograph cards).
Motion data	The data exchanged with the VU, representative of speed and distance travelled.
Motion Sensor	Part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Non-valid Card	A card detected as faulty, or for which initial authentication failed, or for which the start of validity date is not yet reached, or for which the expiry date has passed.
Personal Identification Number (PIN)	Depending on context: - a secret password necessary for using a workshop card and only known to the approved workshop to which that card is issued. - a secret password generated by a VU (or by a person operating a VU) and used to authenticate ITS units connecting to the VU over the ITS interface (see Annex IC, Appendix 13).
Periodic Inspection	A set of operations performed to check that the tachograph works properly, that its settings correspond to the vehicle parameters, and that no manipulation devices are attached to the tachograph.

Term	Meaning
Personalisation	The process by which the equipment-individual data are stored in and unambiguously, inseparably associated with the related equipment.
Physically separated parts	Physical components of the vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
Printer	Component of the recording equipment that provides printouts of stored data.
Remote Early Detection Communication	Communication between the remote early detection communication facility and the remote early detection communication reader during targeted roadside checks with the aim of remotely detecting possible manipulation or misuse of recording equipment.
Remote Early Detection Communication Facility	The equipment of the vehicle unit that is used to perform targeted roadside checks (sometimes referred to as Remote Communication Facility).
Remote Early Detection Communication Reader	A system used by control officers for targeted roadside checks of vehicle units, using a DSRC connection.
Repair	Any repair of a motion sensor or of a vehicle unit or of a cable that requires the disconnection of its power supply, or its disconnection from other tachograph components, or the opening of the motion sensor or vehicle unit.
Security Certification	Process to certify, by a Common Criteria certification body, that the recording equipment (or component) or the tachograph card fulfils the security requirements defined in the relevant Protection Profile.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys).
Self Test	Test run cyclically and automatically, or following an external request, by the recording equipment to detect faults. When used in this document "self-test" designates either a built-in test or a self-test, as defined in *[2016_799_IC]* Annex 1IC..
Smart Tachograph System	The recording equipment, tachograph cards and the set of all directly or indirectly interacting equipment during their construction, installation, use, testing and control, such as cards, remote early detection communication reader and any other equipment for data downloading, data analysis, calibration, generating, managing or introducing security elements, etc.
Software Upgrade	Software Upgrade installs a new version of software in the TOE.
Time Adjustment	An automatic adjustment of current time at regular intervals and within a maximum tolerance of one minute, or an adjustment performed during calibration.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [*CC_1]*]). In the context of this ST, the term security data is also used.
Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable.
Unknown User.	A user that has not been authenticated by the TOE.
User	A human user or connected IT entity
User data	Any data, other than security data, recorded or stored by the VU User data include identification data and activity data. CC gives the following generic definitions for user data: Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [*CC_1]*). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [*CC_2]*).

Term	Meaning
Vehicle Unit	The tachograph 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, the vehicle unit includes, among other things, a processing unit, a data memory, a time measurement function, two smart card interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user's inputs.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
Workshop Card	A tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the cardholder and allows for the testing, calibration and activation of tachographs, and/or downloading from them.

Abbreviations

Abbreviation	Meaning
AES	Advanced Encryption Standard
CA	Certification Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining (an operation mode of a block cipher
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)
EGF	External GNSS Facility
EC	European Community
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES)
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
FIL	File
Fun	Function
IDE	Intelligent dedicated equipment
MAC	Message Authentication Code
MD	Management Device
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN)
n.a.	Not applicable
OSP	Organisational security policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection profile
RTC	Real time clock
SAR	Security assurance requirements

Abbreviation	Meaning
SFP	Security functional policy
SFR	Security functional requirement
ST	Security Target
TBD	To Be Defined
TC	Tachograph Card
TDES	Triple Data Encryption Standard
TOE	Target Of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy
UDE	User Data Export
VU	Vehicle Unit

List of figures

Figure 1-1 Configuration 1: Internal GNSS receiver and internal remote early detection communication facility 13
Figure 1-2 Configuration 2: Internal GNSS receiver and external remote early detection communication facility 14
Figure 1-3 VU typical life cycle 16
Figure 1-4 VU operational environment (internal remote early detection communication facility / internal GNSS receiver)..... 17
Figure 1-5 VU operational environment (external remote early detection communication facility /internal GNSS receiver)..... 18

List of tables

Table 1-1 Mode of operations ... 13
Table 3-1: Primary assets ... 22
Table 3-2 Secondary assets ... 22
Table 3-3 Subjects and external entities ... 24
Table 3-4 Threats addressed solely by the TOE ... 24
Table 3-5 Threats averted by the TOE and its operational environment ... 25
Table 3-6 Assumptions ... 26
Table 3-7 Organisational security policies ... 26
Table 4-1 Security objectives for the TOE ... 27
Table 4-2 Security objectives for the operational environment ... 29
Table 6-1: Standardised domain parameters ... 54
Table 6-2: Cipher suites ... 55
Table 7-1 Security Objectives rationale ... 63
Table 7-2 SFR's dependencies ... 68
Table 7-3 Coverage of security objectives for the TOE by SFRs ... 72
Table 7-4 Suitability of the SFRs ... 81
Table 7-5 SAR Dependencies (additional to EAL 4 only) ... 81
Table 10-1 First-generation asymmetric keys generated, used or stored by a VU ... 90
Table 10-2 First-generation symmetric keys generated, used or stored by a VU ... 91
Table 10-3 First-generation certificates used or stored by a VU ... 92
Table 10-4 Second-generation asymmetric keys generated, used or stored by a VU ... 95
Table 10-5 Second-generation symmetric keys generated, used or stored by a VU ... 98
Table 10-6 Second-generation certificates used or stored by a VU ... 102

1 ST Introduction

This document contains a description of the digital Tachograph DTCO 1381 Rel. 4.0e and 4.0ed (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.

Annex IC of *[2016_799_IC]* requirements not included in this protection profile are not the subject of security certification.

The vehicle unit general characteristics, functions and modes of operation are described in [*[2016_799_IC]* Annex IC, Chapter 2. The VU construction and functional requirements are specified in *[2016_799_IC]* Annex IC, Chapter 3.

1.1 ST reference

Title:	Digital Tachograph DTCO 1381 Security Target
Revision:	1.2
Author:	Norbert Köhn, VNI CVS S3 EMEA TS HM
Publication date:	16.02.2021
Developer name:	Continental Automotive GmbH
TOE Name:	Digital Tachograph DTCO 1381
TOE Version number:	Release 4.0e and 4.0ed

1.2 TOE overview

1.2.1 TOE definition and operational usage

The Target of evaluation digital Tachograph DTCO 1381 Rel. 4.0e and 4.0ed is a second generation vehicle unit (VU) in the sense of Annex IC *[2016_799_IC]* 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 human user activities data in its internal data memory, it also records human user activities data in tachograph cards. The VU outputs data to display, printer and external devices.

The TOE is connected to a motion sensor with which it obtains the vehicle's motion data. Information from the motion sensor is corroborated by vehicle motion information derived from a GNSS receiver, and optionally by other sources independent of the motion sensor **(Note: not applicable for the TOE)**.

The TOE may be connected to

a. an external remote early detection facility (a DSRC communication module) , to allow remote early detection equipment to detect possible manipulation or misuse of the VU, and to

b. ~~*an external GNSS facility), to allow for recording of the position of the vehicle at certain points during the daily working period, and providing a second source of vehicle motion information*~~.

Both of these devices may alternatively be embedded in the VU, which may in these cases be connected to suitable external antennas or contain embedded antennas. The ~~*VU may also communicate with external devices involved in Intelligent Transport Systems through an optional wireless interface*~~.

With regard to security requirements of GNSS and remote early detection functionalities:

a. When the GNSS receiver is within the same physical boundary as the VU, its protection is addressed by this ST. When the VU is used with an external GNSS facility, the external GNSS facility has to be considered to be a part of the VU. However, the external GNSS facility has then a separate physical boundary, its protection is explicitly addressed through the External GNSS Facility PP, and it is outside the boundary of the TOE for this ST.

b. When the VU is used with an external remote early detection communication facility, the latter is considered to be a part of the VU. However, no security requirement from this ST applies directly to it, and it is outside the boundary of the TOE defined in this ST. When the remote early detection communication facility is within the same physical boundary as the VU no security requirement is directly applicable to it. However, it may benefit from the protections against physical attacks provided by the VU housing, and it is shown inside the boundary of the TOE in Figure 1-1.

Human users identify themselves to the TOE using tachograph cards.

The physical scope of the TOE is a device to be installed in a vehicle. The TOE consists of

a. a hardware box including
   i. a processing unit,
   ii. a data memory,
   iii. a real time clock,
   iv. two smart card interface devices for driver and co-driver,
   v. a printer,
   vi. a display,
   vii. a visual warning system,
   viii. facilities for entry of human user's inputs
   ix. embedded software
b. related user manuals.

The TOE must also support external connections or interfaces to the following:

a. a motion sensor (MS);
b. two smart cards;
c. a power supply unit;
d. a global navigation system (GNSS);
e. a remote early detection communication reader;
f. ~~*optionally, external device(s) for ITS applications*~~ ;
g. other devices used for calibration, data export, software upgrade and diagnostics,
h. Intelligent dedicated equipment for data download.

The TOE supports connection to GNSS either through equipment contained within the TOE enclosure, ~~*or through connection to an external device supporting the connection*~~.

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 has four modes of operation:

− operational mode,

− control mode,

− calibration mode,

− company mode.

The TOE switches to the appropriate mode of operation according to the valid tachograph cards inserted into the card interface devices, as shown in the table below. The modes of operation are significant in that certain operations can be carried out only whilst in certain modes of operation (see *[2016_799_IC]* Annex IC, section 2.3]). Note that the shaded boxes below denote a card conflict, and will trigger an audit event.

Mode of operation		**Driver slot**				
		No card	Driver card	Control card	Workshop card	Company card
Co-driver slot	No card	Operational	Operational	Control	Calibration	Company
	Driver card	Operational	Operational	Control	Calibration	Company
	Control card	Control	Control	Control	Operational	Operational

Mode of operation		Driver slot				
		No card	Driver card	Control card	Workshop card	Company card
	Workshop card	Calibration	Calibration	Operational	Calibration	Operational
	Company card	Company	Company	Operational	Operational	Company

Table 1-1 Mode of operations

1.2.2 TOE Configurations

The following figures depict the possible TOE configurations. It should be noted that although the printer mechanism is part of the TOE, the paper documents that it produces are not). Also Bluetooth pairing and Bluetooth connection of the ITS interface are outside the scope of the TOE.

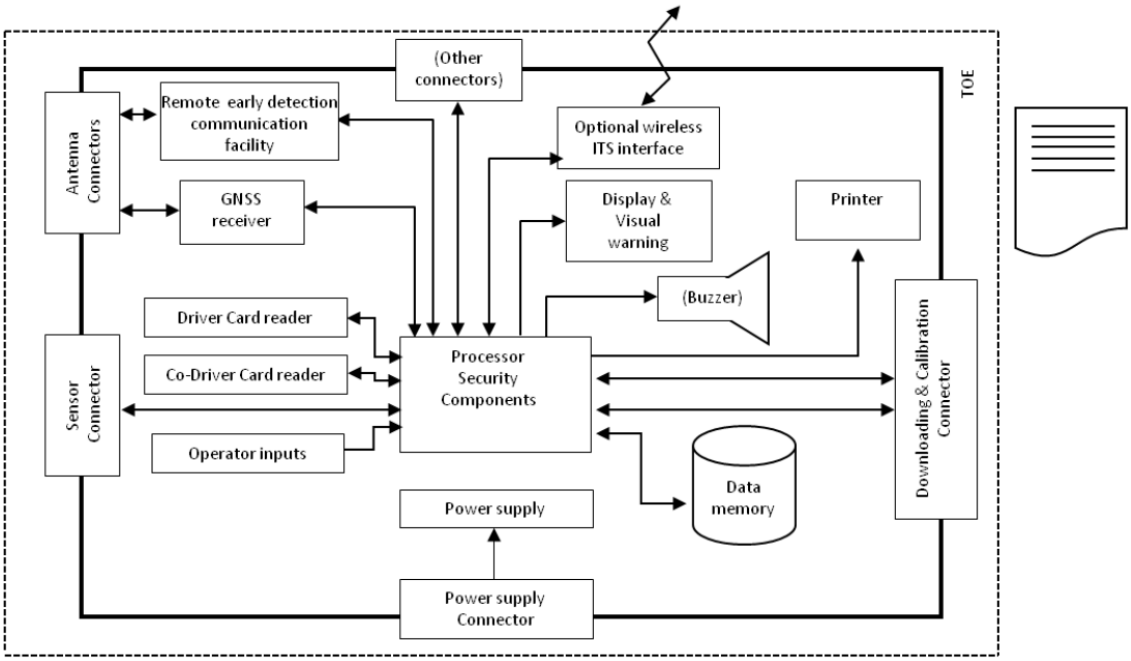


Figure 1-1 Configuration 1: Internal GNSS receiver and internal remote early detection communication facility

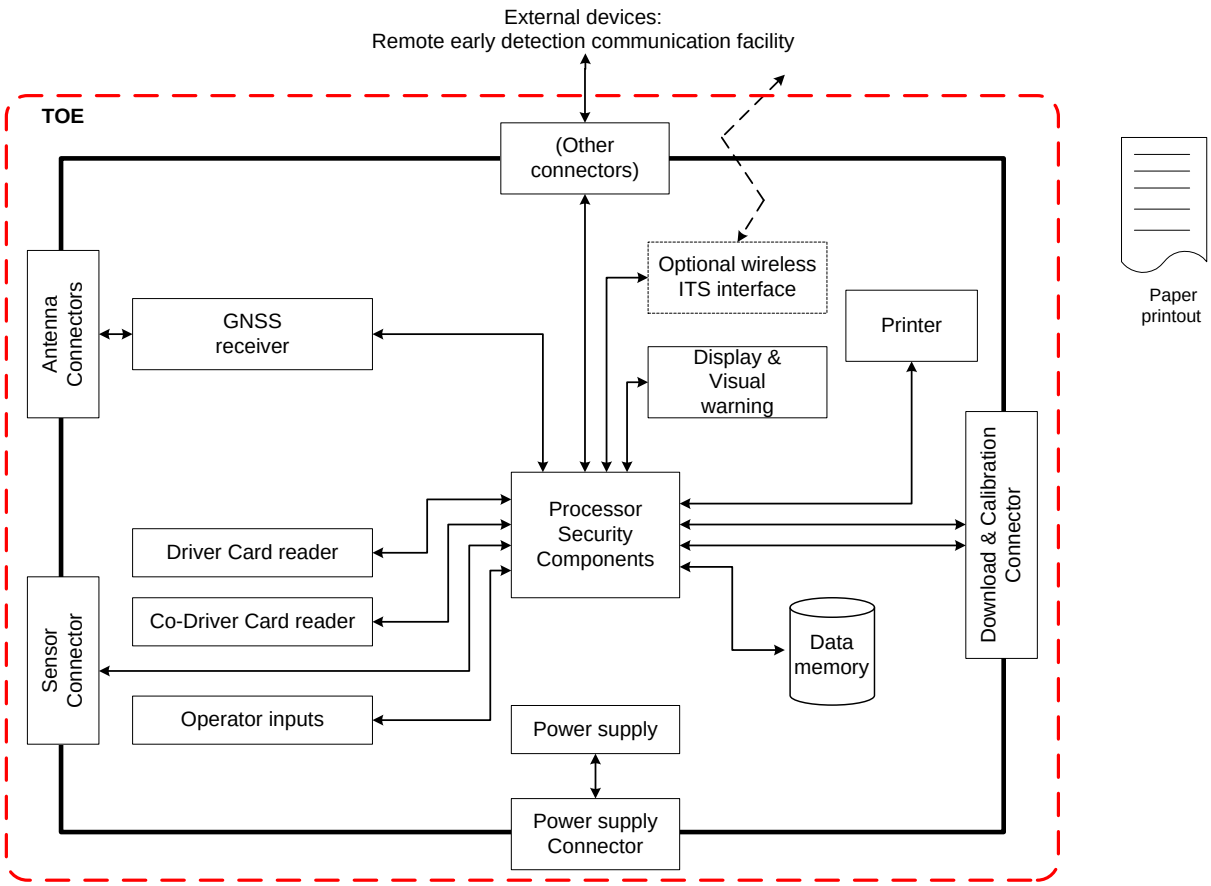


Figure 1-2 Configuration 2: Internal GNSS receiver and external remote early detection communication facility

The TOE addressed by the protection profile *[PP]* will have one of four different configurations (external/internal regarding of the TOE physical boundary):

- Configuration 1: Internal GNSS receiver and internal remote early detection communication facility (Figure 1-1),
- Configuration 2: Internal GNSS receiver and external remote early detection communication facility Figure 1-2,
- Configuration 3: External GNSS receiver and external remote early detection,
- Configuration 4: External GNSS receiver and internal remote early detection communication facility.

The applicable configurations for the TOE are configuration 1 and 2.

1.2.3 TOE major security features for operational use

The TOE security features aim to:

- protect the data memory in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,
- protect the confidentiality, integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
- protect the integrity, authenticity and where applicable, confidentiality of data exchanged between the vehicle unit and the tachograph cards
- protect the integrity and authenticity of data exchanged between the vehicle unit ~~*and the external GNSS facility, if and only if the TOE is connected to an EGF*~~,
- protect the confidentiality, integrity and authenticity of data output through the remote early detection communication for control purposes, and
- protect the integrity, authenticity and non-repudiation of data downloaded.

The main security features are provided by the following major security services described below:

1.2.3.1 Identification and Authentication

The TOE identifies and authenticates tachograph cards and motion sensors and management devices.

1.2.3.2 Access control to functions and stored data

The TOE controls access to stored data and functions based on the mode of operation.

The TOE regularly sends its current remote early detection data to the internal or external remote early detection communication facility (REDCF). This data is encrypted and authenticated. The data can be accessed by any remote early detection communication reader that interrogates the REDCF, without any authentication being necessary. Access to remote early detection communication data is controlled on the basis of possession of the correct key from which the TOE-specific decryption key can be derived.

1.2.3.3 Accountability of users

User activity is recorded such that users can be held accountable for their actions.

1.2.3.4 Audit of events and faults

The TOE detects and records a range of events and faults.

1.2.3.5 Residual information protection for secret data

Encryption keys and certificates are deleted from the TOE when no longer needed, such that the information can no longer be retrieved.

1.2.3.6 Integrity and authenticity of exported data

The integrity and authenticity of user data exported (downloaded) to an external storage medium, in accordance with *[2016_799_IC]* Annex IC, Appendix 7, is assured through the use of digital signatures.

1.2.3.7 Stored Data Accuracy

Data stored in the TOE fully and accurately reflects the input values from all sources ((motion sensor, VU real time clock, calibration connector, Tachograph cards, VU keyboard, ~~*external GNSS facility (if applicable*~~)).

1.2.3.8 Reliability of services

The TOE provides features that aim to assure the reliability of its services. These features include, but are not limited to self-testing, physical protection, control of executable code, resource management and secure handling of events. If the TOE allows applications other than the tachograph application, then separation of application execution and security data must be implemented.

1.2.3.9 Data exchange

The confidentiality and integrity of data exchange with the remote early detection communication reader and the workshop card is maintained as required by *[2016_799_IC]* Annex 1C, Appendix 11.

1.2.4 TOE Type

The TOE type –digital Tachograph DTCO 1381 Rel. 4.0e and 4.0ed- is a second-generation tachograph vehicle unit[1]. Second generation digital tachographs, called smart tachographs, include a connection to the global navigation satellite system (GNSS) facility, a remote early detection communication facility, and an interface with intelligent transport systems.
The typical life cycle of the VU is depicted in Figure 1-3 below.

The security policy defined by this security target focuses on the operational phase in the end user environment. However, some single properties of the calibration phase, being significant for the security of the TOE in its operational phase, are also considered by the current ST. The TOE distinguishes between its calibration and operational phases by modes of operation as

[1] Note that if the VU is designed to operate with an external GNSS facility, the TOE is only a part of the VU. The terms VU or vehicle unit is often used within the ST interchangeably with the term TOE, but it is important to recognize the distinction when an external GNSS facility is present.

defined in *[2016_799_IC]*: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU.

A security evaluation/certification conformant to the PP *[PP]* will have to consider all life phases to the extent required by the assurance package chosen here for the TOE (see section 6.2 below). Usually, the TOE delivery from its manufacturer to the first customer (an approved workshop[2]) happens exactly at the transition from the manufacturing to the calibration phase.

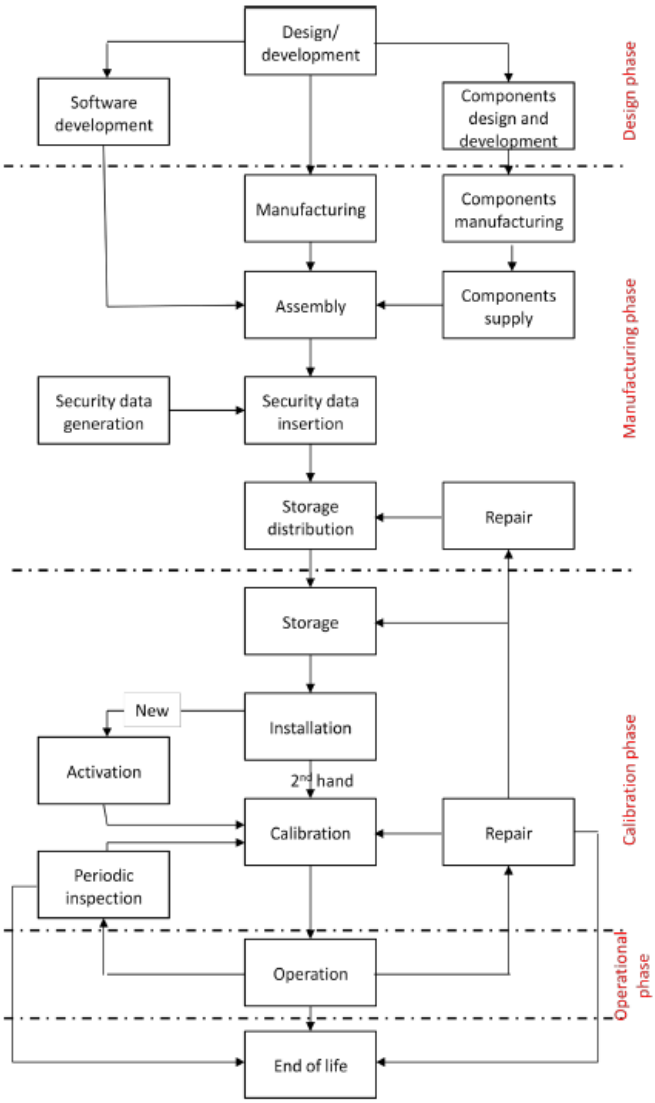


Figure 1-3 VU typical life cycle

Note that Repair in the above diagram may include refurbishment, in which case depersonalisation may be required.

Application note 1-1 For the TOE a repair in the fitters and workshop environments is not planned. An approved software upgrade can also be performed in the workshop environment.

[2] A vehicle manufacturer may also be an approved workshop.

1.2.5 TOE connectivity

The vehicle units operational environment is depicted in Figure 1-4 and Figure 1-5 below.

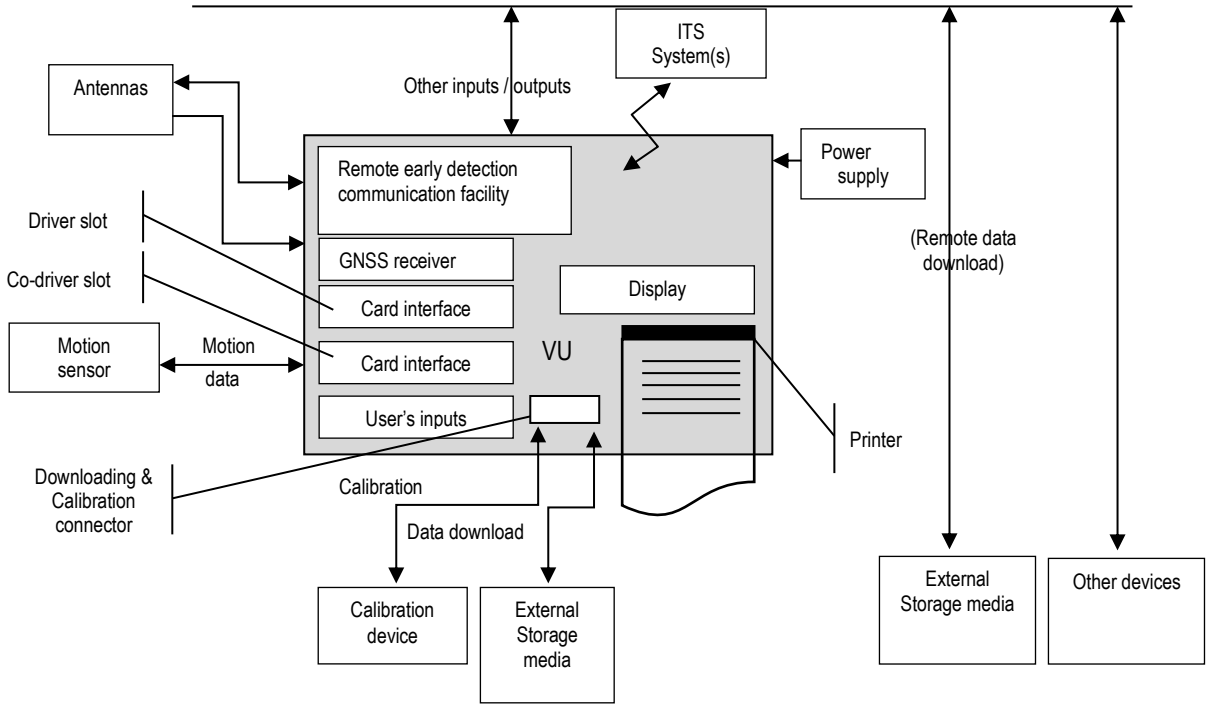


Figure 1-4 VU operational environment (internal remote early detection communication facility / internal GNSS receiver)

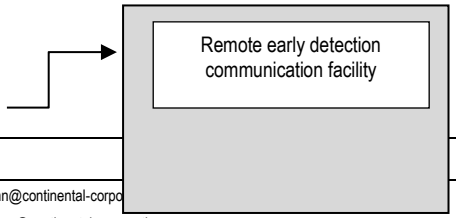
The following TOE external components are

a) *mandatory* for a proper TOE operation
- power supply (e.g. from the vehicle where the TOE is installed)
- motion sensor
-access to GNSS signals(either provided within the TOE or ~~*through an external GNSS facility*~~ see *[2016_799_IC]* Annex IC, Appendix 12)
- DSRC connection to a remote early detection communication reader (either provided within the TOE or through an external remote early detection communication facility see *[2016_799_IC]*, Annex IC, Appendix 14);

b) *functionally necessary* for an Annex I C compliant operation
- calibration device (calibration phase only)
- tachograph cards (four different types)
- printer paper
- external storage media for data download

c) *helpful* for a convenient TOE operation, but not required
- connection to the vehicle network e.g. CAN-connection ,see *[16844-4]*
- connection to ITS systems (see *[2016_799_IC]*, Annex IC, Appendix 13)

Application note 1-2 The TOE will verify, whether the motion sensor, tachograph cards and external GNSS facility (if applicable) connected possess appropriate credentials showing their belonging to the digital tachograph system. A security certification according to [2016_799_IC], Annex IC, Appendix 10 is a prerequisite for the type approval of a motion sensor, tachograph cards and an external GNSS facility.



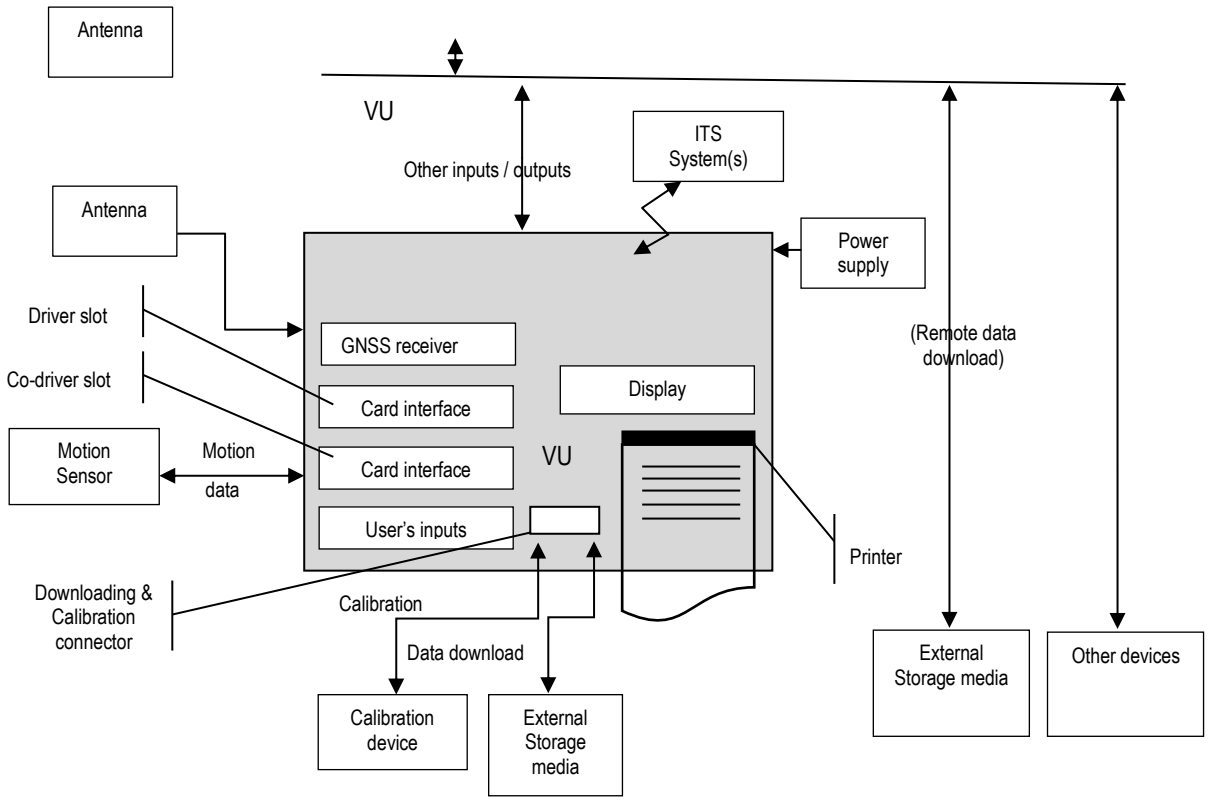


Figure 1-5 VU operational environment (external remote early detection communication facility /internal GNSS receiver)

Application note 1-3 Due to the necessity of ensuring a smooth transition between the 1st generation digital tachograph system and the 2nd generation specified in[2016_799_IC] [5], Annex IC, the TOE is operated and used not only with 2nd generation tachograph cards, but also with 1st generation tachograph cards (i.e. using the security mechanisms and card interface protocol specified in[2016_799_IC] Annex IC for the 1st generation).

This applies to 1st generation driver, company and control cards, but not to workshop cards, mainly because 1st generation workshop cards do not contain the security elements necessary to pair the TOE with 2nd generation motion sensors.

The capability of the TOE to be used with 1st generation tachograph cards may be suppressed once and forever by workshops, so that 1st generation tachograph cards can no longer be accepted by the TOE.

This may only be done after the European Commission has launched a procedure aiming to request workshops to do so, for example during the periodic inspection of recording equipment. Such procedure may be needed according to the results of a digital tachograph system threat assessment.

The TOE therefore contains both 1st generation and 2nd generation security elements, and is able to execute both 1st generation and 2nd generation security mechanisms, according to the generation of the cards that are inserted in the TOE.

Full details of inter-generational operability requirements are in [2016_799_IC], Annex IC, Appendix 15.

1.2.6 Configuration of the TOE as vehicle unit

The TOE DTCO 1381 must be configured for the use as vehicle unit in a real vehicle. This configuration includes the setting of operating parameters of the TOE (e.g. Illumination, colour of the display, front cover, functionality of the CAN Bus diagnostic parameters), activation and calibration.

The setting of the operating parameters has no influence of the security functional requirements of the TOE and is done by trusted fitters and workshops and other users. The activation and calibration is only done by trusted fitters and workshops. This setting is done with a separate set of access rules. These rules are independent from the legal access rules for the activation and calibration of the TOE.

The DTCO 1381 Rel. 4.0e and 4.0ed also supports the passing of weight data provided by a vehicle-internal on-board weighing system and the transmission of these data by the remote early detection communication facility in accordance to Article 1 and Appendix 14 of [2016_799_IC], Annex IC and *[2019_1213_EU]*

Since the weight data are not in scope of [2016_799_IC], Annex IC or the Protection Profile [PP], the passing of these weight data has no influence to the security functional requirements of the TOE.

For the TOE DTCO 1381 there exists only **one accurate** configuration variant related to security functional requirements. This is delivered as TOE DTCO 1381 to the trusted fitters and workshops for installation as vehicle unit in a real vehicle. This delivered configuration variant and the further necessary steps for the setting of operation parameters, activation and calibration of the TOE DTCO 1381 in a real vehicle are described in the guidance documentation.

Also the aspect that the TOE is generated in the production of the manufacturer or through an evaluated update procedure in a trusted workshop has no influence.

2 Conformance claims

2.1 CC conformance claim

This security target claims conformance to:

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April2017 [CC_1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [[CC_2]

Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [CC_3].

As follows

• Part 2 extended.

• Part 3 conformant (EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5).

2.2 PP claim

This ST is conformant to the following documents:

Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU PP), Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex IC), Version 1.0, 9th September 2016, DG JRC – Directorate E – Space, Security and Migration Cyber and Digital Citizens' Security Unit E3, BSI-CC-PP-0094, 9 May 2017

2.3 Package claim

This ST claims conformance to the assurance package defined in *[2016_799_IC]*, Annex IC, Appendix 10 as follows:

"SEC_006 The assurance level for each Protection Profile shall be EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5"

2.4 2.4 Conformance claim rationale

The type of TOE defined in this ST is a Vehicle Unit in the sense of Annex IC B *[2016_799_IC]* and strictly compliant with the TOE type defined in the PP [*[PP]* which is claimed in the section 2.2. The following threats, security objectives, assumptions and SFRs outlined in the Protection Profile *[PP]* are not used because according to chapter 1.2.2 only configuration 1 and 2 are implemented in the TOE. In these configuration is no external GNSS facility included.

T.Location_Data

OE.Type_Approval_EGF

OE.Bluetooth

A.Bluetooth

FDP_ACF.1.2 (3:DAT), third dash

FDP_ACF.1.3(4:UDE)

FDP_ITC.2.5 (first and sixth dash

FCS_COP.1.11:AES (point f)

FCS_COP.1.1(3:ECC) (point f,g)

FIA_UAU.2 (2:EGF)

FTP_ITC.1(3:EGF)

FIA_AFL.1 (4:EGF)

The following SFRs outlined in the Protection Profile *[PP]* are not used because the TOE has **no** physically separated parts according to the definition in the list of terms on page 4.

FDP_ITT.1

3 Security problem definition

3.1 Introduction

3.1.1 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 list of terms and abbreviations above for the term definitions).

No.	Asset	Definition
1	user data (recorded or stored in the TOE)	Any data, other than security data (sec. Annex A) are recorded or stored by the VU, as required of *[2016_799_IC]*, Annex IC Section 3.12.
2	user data transferred between the TOE and an external connected device[3]	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 software upgrade file - a tachograph card, - ~~*an external GNSS facility (if present*~~) - a remote early detection communication facility or - an external medium for data download. Motion data are part of this asset. User data can be received and sent.

Table 3-1: 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:

No.	Asset	Definition
3	TOE design and software code	Design information and source code (uncompiled or reversed engineered) for the TOE could facilitate an attack
4	TOE hardware	Hardware used to implement and support TOE functions
5	TOE immanent secret security data	Secret security elements (i.e. symmetric and private keys) used by the TOE in order to enforce its security functionality (see Annex A).
6	TOE immanent non-secret security data	Non-secret security elements (i.e. certificates and public keys) used by the TOE in order to enforce its security functionality (see Annex A).
7	TOE internal clock	Time source within a vehicle unit.
8	Location data	The location data is based on the National Marine Electronics Association (NMEA) sentence Recommended Minimum Specific (RMC) GNSS Data, which contains the Position information (Latitude, Longitude), Time in UTC format (hhmmss.ss), and Speed Over Ground in Knots plus additional values.

Table 3-2 Secondary assets

Application note 3-1 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 human 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

[3] No security functions are prescribed for the protection of data transferred through an ITS interface. Therefore for the purposes of this ST it is not an asset to be protected, and it is not listed here

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.

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

3.1.2 Subjects and external entities

The subjects and external entities considered by this security target are listed in the following table:

No.	Role	Definition
1	Human user	Human users are to be understood as legal human user of the TOE. The legitimate human users of the VU comprise drivers, controllers, workshops and companies. User is in possession of a valid tachograph card.
2	Unknown User	Unauthenticated user.
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 together with pairing key encrypted with the master key
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 is one 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 for 1st generation cards are a certified key pair for authentication being verifiable up to EUR.PK. Valid credentials for 2nd generation cards are a certified key pair for authentication, being verifiable up to a EUR certificate known by the VU (possibly via a link certificate)[4].
5	~~*External GNSS facility*~~	~~*An external GNSS facility possesses credentials for its authentication and their validity is verifiable. Only applicable if an external GNSS facility is used.*~~ ~~*Valid credentials are a certified key pair for authentication, being verifiable up to a EUR certificate known by the VU (possibly via a link certificate).*~~
6	Remote early detection communication reader	The equipment used to perform targeted roadside checks.
7	~~*External ITS device*~~	~~*Intelligent Transport Systems (ITS) connected using a standardised interface*~~
8	Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable.
9	Attacker	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 PP, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess an at most *high* attack potential.

[4] See Annex A For definitions of European Level (EUR) keys and certificates

No.	Role	Definition
		Please note that the attacker might assume any subject role recognised by the TOE.

Table 3-3 Subjects and external entities

The table defines the subjects in the sense of CC which can be recognised by the TOE independent of their nature (human or technical user). Where a successful appropriate identification and authentication process takes place, 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.

3.2 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 defined in the following tables:

Label	Threat
T.Card_Data_Exchange	Attackers could try to modify user data while being exchanged between VU and tachograph cards (addition, modification, deletion, replay of data).
T.Remote_Detect_Data	Attackers could try to modify user data, concerning possible manipulation or misuse, targeted to remote early detection equipment roadside checks (addition, modification, deletion, replay of data).
T.Output_Data	Attackers could try to modify, and thus misrepresent, user data output (print, display or download)

Table 3-4 Threats addressed solely by the TOE

Label	Threat
T.Access	Attackers (e.g. human users) could try to access functions not allowed to them (e.g. drivers gaining access to calibration function, to modify or delete user data.
T.Calibration_Parameters	Human Users could try to use miscalibrated equipment (through calibration data[5] modification, or through organisational weaknesses) to misrepresent driver activities (user data).
T.Clock	Attackers could try to modify internal clock of the TOE, and interference with the correct operation of the TOE.
T.Design	Attackers could try to gain illicit knowledge of the TOE design and software code either from manufacturer's material (through theft, bribery) or from reverse engineering, interfere with the correct operation of the TOE.
T.Environment	Attackers could use environmental attacks (thermal, electromagnetic, optical, chemical or mechanical) to interfere with processing of user data.
T.Fake_Devices	Attackers could try to connect unknown equipment (fake motion sensor, tachograph cards or external GNSS facility) to the TOE to misrepresent driver activities (user data at rest or being transferred between the TOE and an external connected device).

[5] Part of user data. For definition of calibration data see *[2016_799_IC]*, Annex IC, Chapter 3.12.10.

Label	Threat
T.Hardware	Attackers could try to modify TOE hardware, and interfere with the correct operation of the TOE.
T.Identification	Human Users could try to use several identifications or no identity to misrepresent driver activities (user data).
T.Motion_Sensor	Attackers could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal), part of user data to misrepresent driver activities (user data).
~~***T.Location_Data***~~	~~*Attackers could try to modify location data when transmitted by an external GNSS facility (addition, modification, deletion, replay of signal)*[6] *to misrepresent driver activities (user data*~~).
T.Power_Supply	Attackers could try to interfere with the recording or transmission of user data by modifying (cutting, reducing, increasing) the TOE's power supply to interfere with its correct operation.
T.Security_Data	Attackers could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment and attempt to misrepresent driver activities (user data).
T.Software	Attackers could try to modify TOE software in order to interfere with the correct operation of the TOE.
T.Stored_Data	Attackers could try to modify stored data (security or user data) in order to misrepresent driver activities (user data).
T.Tests	The use of non-invalidated test modes or of existing back doors by an attacker could interfere with the correct recording or transmission of user data.

Table 3-5 Threats averted by the TOE and its operational environment

3.3 Assumptions

This section described the assumptions that are made about the operational environment in order to be able to provide the security functionality. If the TOE is placed in an operational environment does not uphold these assumptions it may be unable to operate in a secure manner.

The assumptions are provided in the following table.

Short Name	Assumption
A.Activation	Vehicle manufacturers and fitters or workshops activate the TOE after its installation at latest before the vehicle is used in Scope of Regulation EU No. 561/2006.
A.Approv_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 human 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.Cert_Infrastructure	Within the European Smart Tachograph system required key pairs and corresponding certificates are generated, managed and communicated using standardised and secure methods (see *[2016_799_IC]*, Annex IC, chapter 3).
A.Controls	Law enforcement controls of the TOE will be performed regularly and randomly, and must include security audits and (as well as visual inspection of the TOE).
A.Driver_Card_Uniquene	Drivers possess, at one time, one valid driver card only.

[6] T.Location_Data may be regarded as not applicable when an internal GNSS receiver is used.

A.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.
A.Inspections	Recording equipment will be periodically inspected and calibrated.
A.Compliant_Drivers	Drivers use their cards in accordance with provided guidance with provided guidance, and properly select their activity for those that are manually entered.
A.Type_Approved_Dev	The TOE will only be operated together with a motion sensor and an external GNSS facility (if applicable) that are type approved according to*[2016_799_IC]* Annex IC[7].
~~***A.Bluetooth***~~	~~*Bluetooth pairing and Bluetooth connection of the ITS interface are sufficiently secure not to compromise the objectives of this ST.*~~

Table 3-6 Assumptions

3.4 Organisational security policies

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

The organisational policies are providing in the following table.

Short Name	Organisational security policy
P. Crypto	The cryptographic algorithms described in *[2016_799_IC]* Annex I C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected
P.Management_Device	The Management Device supports the appropriate communication interface with the VU and secures the relevant secrets inside the MD as appropriate.

Table 3-7 Organisational security policies

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

4 Security objectives

This section identifies the security objectives for the TOE and for its operational environment. The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- provide a high-level, natural-language solution of the problem;
- divide this solution into two part-wise solutions, that reflect that different entities each have to address a part of the problem;
- demonstrate that these part-wise solutions form a complete solution to the problem.

4.1 Security objectives for the TOE

The following TOE security objectives address the protections provided by the TOE independent of the TOE environment, and are listed in the table below.

Short name	Security objective of the TOE
O.Access	The TOE must control user access to functions and data on the basis of user type and identity.
O.Accountability	The TOE must collect accurate accountability data.
O.Authentication	The TOE must authenticate users and connected entities (when a trusted path or a trusted channel[8] needs to be established towards these users).
O.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
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 and with the remote early detection communication reader.
O.Software_Update	Where updates to TOE software are possible, the TOE must check their authenticity and integrity before installing them.[9]

Table 4-1 Security objectives for the TOE

4.2 Security objectives for the operational environment

The following security objectives for the TOE's operational environment address the protection that must be provided by the TOE environment *independent* of the TOE itself, and are listed in the table below.

[8] Trusted channel is referred to in*[2016_799_IC]*], Annex IC, Appendix 11 as a secure messaging session.

[9] Where software update is implemented in the TOE the ST author must add iterations of FCS components to describe the approach employed to protect the authenticity and integrity of the update.

Specific phase	Short name	Security objective for the environment
Design phase	**OE.Development**	VU developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
Manufacturing phase	**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	Security data inserted into the TOE for compatibility with 2nd generation tachograph cards, motion sensors, ~~*EGFs (if present)*~~ and remote early detection communication readers must be cryptographically strong as required by *[2016_799_IC]* Annex IC, Appendix 11 Part B. Security data inserted into the TOE for compatibility with 1st generation tachograph cards and motion sensors must be as cryptographically strong as required by [*[2016_799_IC]*Annex IC, Appendix 11 Part A.
	OE.Test_Points	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.
Calibration phase	**OE.Activation**	Vehicle manufacturers and fitters or workshops shall activate the TOE after its installation before the vehicle is used in scope of Regulation EU No. 561/2006.
	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

Specific phase	Short name	Security objective for the environment
Operational phase	**OE.Card_Availability**	Tachograph cards shall be available to TOE human 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_Unique	Drivers shall possess, at one time, one valid driver card only.
	OE.Compliant_Drivers	Drivers must use their cards in accordance with provided guidance with provided guidance, and properly select their activity for those that are manually entered.
	OE.Regular_Inspections	Recording equipment shall be periodically inspected and calibrated.
	OE.Type_Approval_MS[10]	The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to *[2016_799_IC]* Annex IC.
	~~***OE.Type_Approval_EGF***~~	~~*The external GNSS facility connected to the TOE (if applicable) must be type approved according to [[2016_799_IC]Annex IC*[11]~~.
	~~***OE.Bluetooth***~~	~~*Bluetooth pairing and Bluetooth connection of the ITS interface must be established such that they are sufficiently secure not to allow compromise of the assets.:*~~
	OE.EOL	When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, the confidentiality of symmetric and private cryptographic key has to be safeguarded.

Table 4-2 Security objectives for the operational environment

Please note that the design and the manufacturing environments are not the intended usage environments for the TOE (see section 1.2.4). 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 and OE.Sec_Data_Strong) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

[10] Identification and authentication of the motion sensor depends on the motion sensor having implemented the required mechanisms to support it.

[11] OE.Type_Approval_EGF may be regarded as trivially met when an internal GNSS facility is used.

5 Extended components definition

This security target uses a component that is defined as an extension to CC part 2.

The extended component is FCS_RNG.1 Random number generation. This component is fully defined and justified in *[FC_RNG]* Section 3.

The PP *[PP]* defines a restricted set of ways in which the extended component can be used in this security target. These are set out in chapter 11, and further information is provided in *[FC_RNG]*.

5.1 Rationale for extended component

CC Part 2[*CC_2]* defines two components FIA_SOS.2 and FCS_CKM.1 that are similar to FCS_RNG.1. However, FCS_RNG.1 allows the specification of requirements for the generation of random numbers in a manner that includes necessary information for intended use, as is required here. These details describe the quality of the generated data that other security services rely upon. Thus by using FCS_RNG a ST author is able to express a coherent set of SFRs that include the generation of random numbers as a security service.

5.2 Extended component definition

This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family (FCS_RNG) of the Class FCS (Cryptographic support).

5.2.1 FCS_RNG Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

64 There are no auditable events foreseen

FCS_RNG.1 Generation of random numbers

Hierarchical to: -

Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6 Security requirements

This section 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*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator.

The **note applicable for the TOE operation** is used and performed by the ST author when an optional feature is not implemented in the TOE. This text is italicised and crossed out like ~~*this*~~.

6.1 Security functional requirements for the TOE

This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications. Section 6.1.1 addresses requirements for the VU. Section 6.1.2 addresses the communication requirements for 2nd generation tachograph cards to be used with the TOE. Section 6.1.3 addresses the communication requirements for 1st generation tachograph cards to be used with the TOE.

6.1.1 Security functional requirements for the VU

6.1.1.1 Class FAU: Security Audit

6.1.1.1.1 FAU_GEN – Security audit data generation

FAU_GEN.1 **Audit data generation**

Hierarchical to: -

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record **and display a visual warning** 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 events listed in *[2016_799_IC]* Annex IC, section s 3.12.8 and 3.12.9]; *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[12]; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [the data to be recorded for each event type listed in [2016_799_IC]. Annex IC, sections 3.12.8 and 3.12.9; *no other audit relevant information*.

6.1.1.1.2 FAU_SAR – Security audit review

FAU_SAR.1 **Audit review**

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [anyone, subject to the requirements of [2016_799_IC]. Annex IC. Paragraph 13] with the capability to read [the information required to be recorded by FAU_GEN.1 and imported motion sensor audit data] from audit records.

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

6.1.1.1.3 FAU_STG – Security audit event storage

FAU_STG.1 **Protected audit trail storage**

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to *detect*[13] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 **Prevention of audit data loss**

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and *behave according to [2016_799_IC]. Annex IC, paragraph 104, 107, 112, 115 and 131* if the audit trail is full.

Application note 6-1 *As a minimum the data memory shall be able to hold events data as required by* [2016_799_IC] *section 3.12.8 without overwriting*

Application note 6-2 *The requirements in FAU_STG.1 and FAU_STG.4 apply equally to imported motion sensor audit data as to audit data generated by the TOE.*

[12] The outcome of the event need only be recorded where such a concept is relevant to the event.

[13] Audit records are "events/faults" defined in *[2016_799_IC]* Annex 1C, sections 3.9, 3.12.8 and 3.12.9. A compromised audit record will trigger a "(code:14H) Stored user data integrity error", see Appendix 1, 2.70 "EventFaultType".

6.1.1.2 Class FCO Communication

6.1.1.2.1 FCO_NRO.1 Non-repudiation of origin

FCO_NRO.1 **Selective proof of origin**

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for [data downloads to external media and DSRC transmissions to the remote early detection communication reader] at the request of the [originator[14]] **in accordance with [2016_799_IC], Annex IC, Appendix 11, section 14 and 13, respectively.**

FCO_NRO.1.2 The TSF shall be able to relate the [identity (VU private key (VU_Sign.SK) and VU DSRC key (VU_{DSRC}_MAC))] of the originator **(vehicle unit)** of the information, and the [user data to be downloaded to external media and remote tachograph monitoring data transmitted to the remote early detection communication reader] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [the recipient] given [that the digital signature or the MAC can be verified (see [2016_799_IC], Annex IC, Appendix 11, Chapters 14 and 13].

6.1.1.3 Class FDP: User Data Protection

6.1.1.3.1 FDP_ACC – Access control policy (1: FIL)

FDP_ACC.1(1:FIL) **Subset access control**

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

FDP_ACC.1.1(1: FIL) The TSF shall enforce the [File_Structure SFP][15] on .

Subjects:

- *Human and technical users of the TOE*

Objects

- *application and data files structure as required in* Application note 6-3

Operations

- *Read, write, modify, delete.*

Application note 6-3 *Tachograph application and data files structure shall be created during the manufacturing process and then locked against any future modification or deletion. This SFR iteration relates to application and data file structures themselves.*

6.1.1.3.2 FDP_ACF – Access control function (1:FIL)

FDP_ACF.1(1:FIL) **Security attribute based access control**

Hierarchical to: -

[14] The originator is the vehicle unit.

[15] As defined in FDP_ACC.1(1:FIL) and FDP_ACF.1.1(1:FIL)

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1:FIL) The TSF shall enforce the [File_Structure SFP] to objects based on the following

Subjects:
- *Human and technical users of the TOE*

Objects
- *application and data files structure as required in* Application note 6-3

FDP_ACF.1.2(1: 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(1: FIL) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4(1:FIL) The TSF shall explicitly deny access of subjects to objects based on the following additional rules [application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion].

6.1.1.3.3 FDP_ACC – Access control policy (2: FUN)

FDP_ACC.1(2:FUN) Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

FDP_ACC.1.1(2:FUN) The TSF shall enforce the [Function SFP][16] on

Subjects:

- *Human and technical users of the TOE*

Objects

- *Operational modes, calibration functions, time adjustment, manually entry of data and tachograph card removal as required in Application note 6 4*

Operations

-access to.

Application note 6-4: *The assignment in this iteration relates to control over access to operational modes, calibration functions, time adjustment, manually entry of data, and tachograph card removal.*

6.1.1.3.4 FDP_ACF – Access control functions (2: FUN)

FDP_ACF.1 (2:FUN) Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (2:FUN) The TSF shall enforce [Function SFP] to objects based on the following

Subjects:

- *Human and technical users of the TOE*

[16] As defined in FDP_ACC.1(2:FUN) and FDP_ACF.1.1(2:FUN)

Objects

- *Operational modes, calibration functions, time adjustment, manually entry of data and tachograph card removal as required in Application note 6 4*

FDP_ACF.1.2 (2:FUN) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- the rules listed in [2016_799_IC], Annex IC, section 2.3 related to mode of operation;
- before its activation the VU shall give access to the calibration function, even if not in calibration mode
- after its activation the VU shall fully enforce functions and data access rights as follows:
  - a) the calibration function shall be accessible in the calibration mode only,
  - b) the roadside calibration checking function shall be accessible in the control mode only,
  - c) the company locks management function shall be accessible in the company mode only,
  - d) the monitoring of control activities function shall be operational in the control mode only,
  - e) the downloading function shall not be accessible in the operational mode, with the following exceptions
    - i. as an optional feature, the recording equipment may, in any mode of operation, download data through any another means to a company authenticated through this channel (in such a case, company mode data access rights shall apply to this download),
    - ii. downloading a driver card when no other card type is inserted into the VU;
- the time adjustment function shall also allow for triggered adjustment of the current time, in calibration mode;
- driver activity and location data, stored on valid driver and/or workshop cards, shall be updated with activity and location data manually entered by the cardholder only for the period from last card withdrawal to current insertion;
- the release of tachograph cards shall function only when the vehicle is stopped and after the relevant data have been stored on the cards, and the release of the card shall require positive action by the human user].

FDP_ACF.1.3(2:FUN) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:[none].

FDP_ACF.1.4(2:FUN) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- The TOE shall deny access to first generation tachograph cards if their use has been suppressed by a workshop].

6.1.1.3.5 FDP_ACC – Access control policy (3: DAT)

FDP_ACC.1 (3:DAT) Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

FDP_ACC.1.1 (3:DAT) The TSF shall enforce the access control [DATA SFP][17] on

Subjects:

[17]As defined in FDP_ACC.1(3:DAT) and FDP_ACF.1.1(3:DAT)

- *Human and technical users of the TOE*

Objects

- *to VU identification data, MS identification data, calibration mode data, security data and MS audit records as required in Application note 6-5*

Operations

- *access to.*

Application note 6-5: *The assignment in this iteration relates to control over access to VU identification data, MS identification data, External GNSS Facility identification data, calibration mode data, security data and MS audit records.*[18]

6.1.1.3.6 FDP_ACF – Access control functions (3: DAT)

FDP_ACF.1 (3: DAT) Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (3:DAT) The TSF shall enforce the *[Data* SFP] to objects based on the following

Subjects:

- Human and technical users of the TOE

Objects

- to VU identification data, MS identification data, calibration mode data, security data and MS audit records as required in Application note 6-5

FDP_ACF.1.2 (3:DAT) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- vehicle unit identification data is stored by the manufacturer and cannot be modified (except for software version related data and the approval number which may be changed in case of a software upgrade);
- the vehicle unit is able to record and store in its data memory the serial number, approval number and pairing date related to the 20 most recent pairings of motion sensors [19];
- ~~*the vehicle unit is able to record and store in its data memory, and prevent unauthorised modification of the serial number, approval number and coupling date related to the 20 most recent coupled external GNSS facilities (if applicable)*~~ [20];
- the vehicle unit is able to record and store in its data memory, and prevent unauthorised modification of known calibration parameters at the moment of activation, and data relevant to the first calibration following activation, the first calibration in the current vehicle, the five most recent calibrations (if several calibrations happen in the same day ~~only the last one of the day shall be saved~~ *only the first and the last one of the day shall be saved*[21]);

[18] These data are generated by the Motion Sensor, rather than by the TOE. Hence they represent, from the point of view of the TOE, just a kind of data to be stored.

[19] This shall be done as a minimum on pairing.

[20] This shall be done as a minimum on coupling.

[21] As required by [2016_799_IC], Annex IC, req. 119

- the vehicle unit is able to record and store in its data memory and prevent unauthorised modification of data relevant to the most recent time adjustment and the five largest time adjustments outside the frame of a regular calibration;
- the vehicle unit is able to store, and prevent unauthorised modification of the keys and certificates identified in Annex A, managed by the manufacturer;
- the vehicle unit is able to store in its data memory, and prevent unauthorised modification of the name of the manufacturer, address of the manufacturer, part number, serial number, software version number, software version installation date, year of manufacture, approval number;
- the vehicle unit is able to record and store in its data memory, and prevent unauthorised modifications of audit records generated by the motion sensor;
- the vehicle unit is able to record and store in its data memory, and prevent unauthorised modifications of audit records generated by the external GNSS facility (if applicable)] ***Note: not applicable for the TOE***.

FDP_ACF.1.3 (3:DAT) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (3:DAT) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- The TSF shall prevent access to secret cryptographic keys, other than for use by the TSF in its cryptographic operations.]

6.1.1.3.7 FDP_ACC – Access control policy (4: UDE)

FDP_ACC.1(4:UDE) Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

FDP_ACC.1.1(4:UDE) The TSF shall enforce the [User_Data_Export SFP [22]] on

Subjects:

- *Human and technical users of the TOE*

Objects

- *data exported to a tachograph card that is related to the cardholder for the period of insertion as required in* Application note 6-6

Operations

- *access to.*

Application note 6-6: *The assignment in this iteration relates to control over access to data exported to a tachograph card that is related to the cardholder for the period of insertion.*

6.1.1.3.8 FDP_ACF – Access control functions (4: UDE)

FDP_ACF.1(4:UDE) Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

[22] As defined in FDP_ACC.1(4:UDE) and FDP_ACF.1.1(4:UDE)

FDP_ACF.1.1(4:UDE) The TSF shall enforce [User_Data_Export SFP] to objects based on the following [

Subjects:

- *Human and technical users of the TOE*

Objects

- *data exported to a tachograph card that is related to the cardholder for the period of insertion as required in* Application note 6-6

FDP_ACF.1.2(4:UDE) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- the vehicle unit shall update data stored on valid driver, workshop*, company*[23] and control cards with all necessary data relevant to the period while the card is inserted and relevant to the cardholder[24]~~:~~
- the recording equipment shall update driver activity and places data stored on valid driver and/or workshop cards, with activity and places data manually entered by the cardholder],
- only a controller *or a workshop*[25] can read remote early detection communication facility data].

FDP_ACF.1.3(4:UDE) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none ~~[~~

- ~~*If the TOE is equipped with an ITS interface, as specified in [2016_799_IC] Annex IC, Appendix 13, allowing the data recorded or produced by tachograph to be used in operational or calibration mode, by an external facility, personal data may only be made available if the verifiable consent of the driver, accepting his personal data can leave the vehicle network, is enabled.*~~
- ~~*Pairing of the TOE with an external device via an ITS interface shall be protected by a dedicated and random PIN of at least 4 digits, recorded in and available through the display of each vehicle unit].*~~]

FDP_ACF.1.4(4:UDE) The TSF shall explicitly deny access of subjects to objects based on the *following additional rules*: [

- In operational mode the TOE shall not output to display, printer or external devices any personal identification[26] or card number[27] unless they correspond to an inserted tachograph card;
- In company mode driver related data shall only be output for periods where no lock exists or no other company holds a lock;
- When no card is inserted driver related data shall be output relating only to the current and previous 8 calendar days].

6.1.1.3.9 FDP_ACC – Access control policy (5: IS)

FDP_ACC.1(5:IS) Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

[23] As required by [2016_799_IC] Annex IC

[24] As defined in FDP_ACC.1(4:UDE) and FDP_ACF.1.1(4:UDE)

[25] As required by [2016_799_IC] Annex IC

[26] Personal identification (surname and first name) shall be blanked.

[27] Card number shall be partially blanked (every odd character).

FDP_ACC.1.1(5:IS) The TSF shall enforce the [Input_Sources SFP[28]] on

Subjects:

- *the TOE*

Objects

- *vehicle motion data*
- *VU's real time clock data*
- *Recording equipment calibration parameters*
- *Tachograph card data*
- *User inputs*
- *Operations*
- *use of data – only from a valid source.*
- *Prevention of acceptance as executable code*

Application note 6-7: The assignment in this iteration relates to control over use of data only from a valid source. This covers vehicle motion data, the VU's real time clock, recording equipment calibration parameters, tachograph cards and user inputs. It also covers prevention of external inputs being accepted as executable code.

6.1.1.3.10 FDP_ACF – Access control functions (5: IS)

FDP_ACF.1(5:IS) Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(5:IS) The TSF shall enforce [Input_Sources SFP] to objects based on the following:

Subjects:

- *the TOE*

Objects

- *vehicle motion data*
- *VU's real time clock data*
- *Recording equipment calibration parameters*
- *Tachograph card data*

User inputs

FDP_ACF.1.2(5:IS) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- the vehicle unit shall ensure that data related to vehicle motion, the real-time clock, recording equipment calibration parameters, tachograph cards and user's inputs may only be processed from the right input sources]

[28] As defined in FDP_ACC.1(5:IS) and FDP_ACF.1.1(5:IS)

FDP_ACF.1.3(5:IS) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (5:IS) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- inputs from external sources shall not be accepted as executable code].

6.1.1.3.11 FDP_ACC – Access control policy (6: SW-Upgrade)

FDP_ACC.1(6:SW-Upgrade) Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security based access control

FDP_ACC.1.1(6:SW-Upgrade) The TSF shall enforce the *SW-Upgrade SFP* on

Subjects:

- *the TOE*

Objects

- *upgrade file data*
- *Operations*
- *use of data – only from a valid source.*

6.1.1.3.12 FDP_ACF – Access control functions (6: SW-Upgrade)

FDP_ACF.1(6:SW-Upgrade) Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(6:SW-Upgrade) The TSF shall enforce *SW-Upgrade SFP* to objects based on the following:

Subjects:

- *the TOE*

Objects

- *upgrade file data*

FDP_ACF.1.2(6: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*.

FDP_ACF.1.3(6:SW-Upgrade) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4(6: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*.

Application note 6-8: This iteration was added to define the SFR for access, authenticity and integrity of the SW-Update.

6.1.1.3.13 FDP_ETC – Export from the TOE

FDP_ETC.2 **Export of user data with security attributes**

Hierarchical to: -

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

FDP_ETC.2.1 The TSF shall enforce the [User_Data_Export SFP] 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: [

- tachograph cards data update shall be such that, when needed and taking into account card actual storage capacity, most recent data replace oldest data;
- the vehicle unit shall export data to tachograph cards with associated security attributes such that the card will be able to verify its integrity and authenticity;
- the vehicle unit shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified].

6.1.1.3.14 FDP_ITC – Import from outside of the TOE

FDP_ITC.1 **Import of user data without security attributes**

Hierarchical to: -

Dependencies: [FDP_ACC.1 subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [Input_Sources SFP] 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: [

- the vehicle unit shall ensure that data related to recording equipment calibration parameters, human user's inputs and GNSS data may only be processed from the right input sources].

FDP_ITC.2 **Import of user data with security attributes**

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1sunset information flow control]
[FTP_ITC.1 import of user data without security attributes or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter TSF basic TSF data consistency

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

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

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

- the vehicle unit shall ensure that data related to vehicle motion, tachograph cards ~~*and external GNSS facility (if applicable)*~~ may only be processed from the right input sources;
- the vehicle unit shall verify the integrity and authenticity of motion data and audit data imported from the motion sensor;
- upon detection of a motion data integrity or authenticity error the TOE shall generate an audit record, and continue to use the imported data;
- the vehicle unit shall verify the integrity and authenticity of data imported from tachograph cards;
- upon detection of a card data integrity or authenticity error the TOE shall generate an audit record, and not use the data;
- ~~*the vehicle unit shall verify the integrity and authenticity of data imported from the external GNSS facility (if applicable*~~,);
- upon detection of an external GNSS facility data integrity or authenticity error the TOE shall generate an audit record, and not use the data;
- inputs from external sources shall not be accepted as executable code;
- if software updates are permitted they shall be verified by cryptographic security attribute before being implemented].

Application note 6-9 *If software can be updated only in the manufacturing phase then the requirement for verified software updates is not applicable.*

6.1.1.3.15 FDP_ITT – Internal TOE transfer

FDP_ITT.1 ~~***Basic internal transfer protection***~~

~~*Hierarchical to:* -~~

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

FDP~~*_ITT.1.1 The TSF shall enforce the [Data SFP] to prevent [modification] of user data when it is transmitted between physically-separated parts of the TOE.*~~

6.1.1.3.16 FDP_RIP – Residual information protection

FDP_RIP.1 **Subset residual information protection**

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: [

- Temporarily stored cryptographic keys that are listed in Table 16. Table 10-3, Table 10-4 and Table 10-5;
- 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 TK (at most by the end of the software upgrade)*]

Application note 6-10: *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 the keys in Annex A – Key & certificate tables are marked as having to be made unavailable at decommissioning the TOE is a matter of the related organisational policy.*

Application note 6-11 *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. Applied to cryptographic keys, FDP_RIP.1 requires a quality metric ('any previous information content of a resource is made unavailable') for key destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.*

6.1.1.3.17 FDP_SDI – Stored data integrity

FDP_SDI.2(1) **Stored data integrity monitoring and action**

Hierarchical to: -

Dependencies: -

FDP_SDI.2.1(1) The TSF shall monitor user data stored in **the TOE's data memory** ~~containers controlled by the TSF~~ for [integrity errors] ~~on all objects, based on the following attributes: user data attributes.~~

FDP_SDI.2.2(1) Upon detection of a data integrity error, the TSF shall generate an audit record.

FDP_SDI.2(2) **Stored data integrity monitoring and action**

Hierarchical to: -

Dependencies: -

FDP_SDI.2.1(2) The TSF shall monitor user data stored in containers controlled by the TSF~~.~~ For [inconsistency between motion data and GNSS data, [assignment: *no other **motion data** integrity errors*]] on all objects, based on the following attributes [selection: *vehicle speed,~~ distance travelled~~*].

FDP_SDI.2.2(2) Upon detection of a data integrity error, the TSF shall generate an audit record.

6.1.1.4 Class FIA: Identification and Authentication

6.1.1.4.1 FIA_AFL – Authentication failures

FIA_AFL.1(1:TCL) **Authentication failure handling**

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(1:TCL) The TSF shall detect when [5] unsuccessful authentication attempts occur related to [local tachograph card authentication].

FIA_AFL.1.2(1:TCL) When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [

a) generate an audit record of the event,

b) warn the human user,

c) assume the human user to be an unknown user and the card to be non-valid].

Application note 6-12 *A vehicle unit has to perform a mutual authentication procedure with a company card independent of* whether this card is connected locally or remotely. Therefore, the functional security requirements *concerning identification and authentication of the company card are independent of the physical card location. The only difference is in the required reaction to an unsuccessful authentication attempt.*

FIA_AFL.1(2:TCR) Authentication failure handling

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(2:TCR) The TSF shall detect when [5] unsuccessful authentication attempts occur related to [remote tachograph company card authentication].

FIA_AFL.1.2(2:TCR) When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [warn the remotely connected company].

Application note 6-13 *FIA_AFL.1.2 (2:TCR) is only applicable if the TOE provides a remote download facility (see [2016_799_IC] Annex 1C paragraph 193).*

FIA_AFL.1(3:MS) Authentication failure handling

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(3:MS) The TSF shall detect when [1] unsuccessful authentication attempts occur related to [motion sensor authentication].

FIA_AFL.1.2(3:MS) When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall[

a) generate an audit record of the event,

b) warn the user,

c) continue to accept and use non secured motion data sent by the motion sensor].

Application note 6-14 *The positive integer number expected in FIA_AFL.1.1 (3::MS) and FIA_AFL.1.1 (4:EGF) shall be ≤ 20 during a calibration. Outside of a calibration any authentication failure shall generate the actions in FIA_AFL.1.2 (3:MS) and FIA_AFL.1.2(4:EGF), respectively.*

~~***FIA_AFL.1 (4:EGF) Authentication failure handling***~~

~~*Hierarchical to: -*~~

~~*Dependencies: FIA_UAU.1 Timing of authentication*~~

FIA_AFL.1.1 (4:EGF) ~~*The TSF shall detect when[assignment: integer number] unsuccessful authentication attempts occur related to [external GNSS facility authentication].*~~

FIA_AFL.1.2(4:EGF) ~~When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall [generate an audit record of the event].~~

Application note 6-15 *Not applicable for the TOE, because the TOE has an internal GNSS receiver.*

6.1.1.4.2 FIA_ATD – User attribute definition

FIA_ATD.1(1:TC) **User attribute definition**

Hierarchical to: -

Dependencies: -

FIA_ATD.1.1(1:TC) The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **tachograph cards**:[

a) User group:

i. Driver (driver card)

ii. Controller (control card,

iii. Workshop (workshop card),

iv. Company (company card),

v. Unknown (no card inserted);

b) User ID:

i. The card issuing member state code and the card number,

ii. Unknown if the user group is Unknown].

Application note 6-16: *For further details see [2016_799_IC] Annex IC, section 3.12.13 and Appendix 1 2.73 and 2.74.*

6.1.1.4.3 FIA_UAU – User authentication

FIA_UAU.3 **Unforgeable authentication**

Hierarchical to: -

Dependencies: -

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

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

Application note 6-17: *This requirement relates to the motion sensor, tachograph cards, management device and, ~~if applicable, the external GNSS facility~~).*

FIA_UAU.5 **Multiple authentication mechanisms**

Hierarchical to: -

Dependencies: -

FIA_UAU.5.1 The TSF shall provide [authentication using the methods described in [2016_799_IC], Appendix 11, Chapter 10 (certificate chain authentication and PIN)] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [rule: if the card is a workshop card then authentication using both certificate chain authentication and a PIN of at least 4 digits is required].

Application note 6-18: FIA_UAU.5 applies only to authentication using a workshop card, where a PIN is required.

FIA_UAU.6 Re-authenticating

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1 The TSF shall re-authenticate the ~~user~~ **tachograph card** under the conditions [at power supply recovery, when the secure messaging session is aborted as described in [2016_799_IC] Annex 1C, Appendix 11 *[assignment: no list of **other** conditions where re-authentication is required]*].

6.1.1.4.4 FIA_UID – User identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: -

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

6.1.1.5 Class FMT Security Management

6.1.1.5.1 FMT_MSA – Management of security attributes

FMT_MSA.1 Management of security attributes

Hierarchical to: -

Dependencies: [FDP_ACC.1Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1: security roles
FMT_SMF.1: specification of management functions

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

FMT_MSA.3(1:FIL) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1(1:FIL) The TSF shall enforce the [FILE STRUCTURE FUNCTION SFP] to provide (restrictive) default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1: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 (2:FUN) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1 (2:FUN) The TSF shall enforce the [FUNCTION SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (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 (3:DAT) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1 (3:DAT) The TSF shall enforce the [DATA SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (3: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 (4: UDE) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1 (4:UDE) The TSF shall enforce the [USER DATA EXPORT SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (4: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 (5: IS) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1 (5::IS) The TSF shall enforce the (INPUT SOURCES SFP] to provide (restrictive) default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (5 :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 (6: SW-Upgrade) Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: Management of security attributes
FMT_SMR.1: security roles

FMT_MSA.3.1 (6: SW-Upgrade) The TSF shall enforce the *SW-Upgrade SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (6: SW-Upgrade) The TSF shall allow *nobody* to specify alternative initial values to override the default values when an object or information is created.

6.1.1.5.2 FMT_MOF – Management of functions in TSF

FMT_MOF.1 (1) Management of security functions behaviour

Hierarchical to: -

Dependencies: FMT_SMR.1: Security roles
FMT_SMF.1: Specification of managements functions

FMT_MOF.1.1 (1) The TSF shall restrict the ability to [enable] the functions [all commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU] to [nobody].

FMT_MOF.1 (2) Management of security functions behaviour

Hierarchical to: -

Dependencies: FMT_SMR.1: Security roles
FMT_SMF.1: Specification of managements functions

FMT_MOF.1.1 (2) The TSF shall restrict the ability to [enable] the functions [calibration] to [workshop].

Application note 6-19: The calibration mode functions include the deactivation of the TOE's ability to use first generation tachograph cards.

FMT_MOF.1 (3) Management of security functions behaviour

Hierarchical to: -

Dependencies: FMT_SMR.1: Security roles
FMT_SMF.1: Specification of managements functions

FMT_MOF.1.1 (3) The TSF shall restrict the ability to [enable] the functions [manage company locks] to [company].

FMT_MOF.1 (4) Management of security functions behaviour

Hierarchical to: -

Dependencies: FMT_SMR.1: Security roles
FMT_SMF.1: Specification of managements functions

FMT_MOF.1.1 (4) The TSF shall restrict the ability to [enable] the functions [performing control activities] to [controller].

FMT_MOF.1 (5) Management of security functions behaviour

Hierarchical to: -

Dependencies: FMT_SMR.1: Security roles
FMT_SMF.1: Specification of managements functions

FMT_MOF.1.1 (5) The TSF shall restrict the ability to [enable] the functions [downloading when [VU is in operational mode [to [remotely authenticated company] (if applicable) ,or driver (downloading driver card with no other card inserted)].

6.1.1.5.3 FMT_MTD – Management of TSF data

FMT_MTD.1 Management of TSF data

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to [manually change] the [clock time] to [workshop (calibration mode)].

6.1.1.5.4 FMT_SMF – Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: -

Dependencies: -

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) Calibration (workshop card inserted);

b) Time adjustment (workshop card inserted);

c) Company locks management (company card inserted);

d) Performance of control activities (control card inserted);

e) VU data downloading to external media (control, workshop or company card inserted)].

6.1.1.5.5 FMT_SMR – Security management roles

FMT_SMR.1 Security management roles

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

a) Driver (driver card),

b) Controller (control card),

c) Workshop (workshop card),

d) Company (company card),

e) Unknown (no card inserted).

f) Motion sensor

g) ~~*External GNSS facility (if applicable*~~)

h) Intelligent dedicated equipment]

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

6.1.1.6 Class FPT: Protection of the TSF

6.1.1.6.1 FPT_FLS – Fail secure

FPT_FLS.1 **Failure with preservation of secure state**

Hierarchical to: -

Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state[29] when the following types of failures occur: [

a) Detection of an internal fault;

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

c) Transaction stopped before completion;

d) Any other reset condition].

6.1.1.6.2 FPT_PHP – TSF physical protection

FPT_PHP.2 **Notification of physical attack**

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

Dependencies: FMT_MOF.1 Management of security functions behaviour

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

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [Power supply] the TSF shall monitor the devices and elements and notify [the user] when physical tampering with the TSF's devices or TSF's elements has occurred.

Application note 6-20 *In FPT_PHP.2.3 physical tampering means deviation from the specified values of electrical inputs to the power supply, including cut-off. Data stored into the TOE data memory shall not be affected by an external power supply cut-off of less than twelve months in type approval conditions.*

Application note 6-21 *If the TOE is designed so that it can be opened, the TOE shall detect any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the TOE shall generate an audit record (it is acceptable that the audit record is generated and stored after power supply reconnection). If the TOE 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). The TOE is designed so that it cannot be opened. Physical tampering attempts are easily detectable i.e. through visual inspection of secure seals. The secure seals are conformant to security level 1 of BSI–TL03415 [TL-03415]. After its activation, the TOE shall detect specified hardware sabotage (details to be provided by the ST author, none).*

FPT_PHP.3 **Resistance to physical attack**

Hierarchical to: -

Dependencies: -

[29] A secure state is defined in CC as a state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

FPT_PHP.3.1 The TSF shall resist [physical tampering attacks] to the [TSF software and TSF data after the TOE activation] by responding automatically such that the SFRs are always enforced.

6.1.1.6.3 FPT_STM – Time stamps

FPT_STM.1 Reliable time stamps

Hierarchical to: -

Dependencies: -

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

Application note 6-22 *Time stamps are derived from the internal clock of the vehicle unit. Requirements on time measurement and time adjustment are defined in [2016_799_IC] Annex IC, Chapter 2, Sections 3.3 and 3.23.*

6.1.1.6.4 FPT_TST – TSF self test

FPT_TST.1 TSF testing

Hierarchical to: -

Dependencies: -

FPT_TST.1.1 The TSF shall run a suite of self-tests ([during initial start-up, periodically during normal operation and at the request of an operator/External equipment] to demonstrate the correct operation of [data memory, card interface devices, remote early detection communication facility, *link to external GNSS facility (if applicable)*, link to motion sensor, link to IDE for data downloading].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of (data memory).

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of (TSF software).

Application note 6-23: *If the facility to provide a link to an external GNSS is not provided by the TOE, then this may be omitted from FPT_TST.1.1 and FPT_TST.1.3 in the ST.*

Application note 6-24: *Self-test of the link to IDE for data downloading required by FPT_TST.1 need only be carried out during downloading.*

6.1.1.7 Class FTP Trusted path/channels

6.1.1.7.1 FTP_ITC – Inter-TSF trusted channel

FTP_ITC.1(1:MS) Inter-TSF trusted channel (1:MS)

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1(1:MS) The TSF shall provide a communications channel between itself and a~~another trusted IT product~~ **the motion sensor** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(1:MS) The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3(1:MS) The TSF shall initiate communication via the trusted channel for [all data exchange[30]].

Application note 6-25: *Details of the communication channel can be found in [2016_799_IC],] Appendix 11, Chapter 12.*

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

The security functional requirements in this section are required to support communications specifically with 2nd generation tachograph cards, 2nd generation motion sensors, external GNSS facilities (if applicable) and remote early detection communication readers.

6.1.2.1 Class FCS Cryptographic support

6.1.2.1.1 FCS_CKM – Cryptographic key management

FCS_CKM.1(1) **Cryptographic key generation**

Hierarchical to: -

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

FCS_CKM.1.1(1) The TSF shall generate keys in accordance with a specified key generation algorithm [assignment: *RSA: rsagen1 (PKCS v2.1 RFC3447; Elliptic Curve EC: specified in ANSI X9.62- 2005 and ISO/IEC 15946-1:2002*] and specified cryptographic key sizes [for the keys indicated in Table 10-4 and Table 10-5 as being generated by the TOE the key sizes required by[2016_799_IC]] Annex 1C, Appendix 11, Part B of those keys] that meet the following: [Reference [FC_RNG] predefined RNG class [selection: *PTG.2*, PTG.3, DRG.2, DRG.3, DRG.4, NTG.1]].

Application note 6-26: *The ST author selects one of the permitted predefined RNG classes from [FC_RNG], and completes the operations in FCS_CKM.1(1) and FCS_RNG.1 as required. The permitted RNG classes are included in Annex B.*

Application note 6-27: *The function FCS_RNG.1/PSL from the underlying platform (see **[ST_Inf]**) is used.*

FCS_CKM.2(1) **Cryptographic key distribution**

Hierarchical to: -

Dependencies: FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.2.1(1) The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [secure messaging AES session key agreement as specified in [2016_799_IC] Annex 1C, Appendix 11, Part B] that meets the following [[2016_799_IC] Annex 1C, Appendix 11, Part B].

Application note 6-28: *FCS_CKM.1 (1) and FCS_CKM.2 (1) relate to AES session key agreement with the motion sensor, tachograph cards, ~~and external GNSS facility (if applicable).~~*

FCS_CKM.4(1) **Cryptographic key destruction**

Hierarchical to: -

[30] A trusted channel is not required for motion pulses

Dependencies: FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting with value 0xFF*] that meets the following [

- Requirements in Table 10-4 and Table 10-5;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[31];
- *[no **further** standards]]*.

6.1.2.1.2 FCS_COP – Cryptographic operation

FCS_COP.1(1:AES) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1:AES) The TSF shall perform [the following:

a) pairing of a vehicle unit and a motion sensor;

b) mutual authentication between a vehicle unit and a motion sensor;

c) ensuring confidentiality, authenticity and integrity of data exchanged between a vehicle unit and a motion sensor;

d) ensuring authenticity and integrity of data exchanged between a vehicle unit and a tachograph card;

e) where applicable, ensuring confidentiality of data exchanged between a vehicle unit and a tachograph card;

f) ~~*ensuring authenticity and integrity of data exchanged between a vehicle unit and an external GNSS facility*~~]

in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128, 192, 256 bits] that meet the following: [FIPS PUB 197: Advanced Encryption Standard] and [2016_799_IC]; Appendix 11, Part B).

FCS_COP.1(2:SHA-2) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

[31] Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

FCS_COP.1.1(2:SHA-2) The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication (FIPS) PUB 180-4: Secure Hash Standard (SHS)].

FCS_COP.1(3:ECC) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(3:ECC) The TSF shall perform [the following cryptographic operations:

a) digital signature generation;

b) digital signature verification;

c) cryptographic key agreement;

d) mutual authentication between a vehicle unit and a tachograph card;

e) ~~coupling of a vehicle unit and an external GNSS facility~~[32];

f) ~~mutual authentication between a vehicle unit and an external GNSS facility;~~

g) ensuring authenticity, integrity and non-repudation of data downloaded from a vehicle unit]

in accordance with a specified cryptographic algorithm [2016_799_IC], Annex IC, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [2016_799_IC], Appendix 11, Part B] that meet the following: [2016_799_IC], Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the standardised domain parameters in Table 6-1:

Name	Size (bits)	Object identifier
NIST P-256	256	secp256r1
BrainpoolP256r1	256	brainpoolP256r1
NIST P-384	384	secp384r1
BrainpoolP384r1	384	brainpoolP384r1
BrainpoolP512r1	512	brainpoolP512r1
NIST P-521	521	secp521r1

Table 6-1: Standardised domain parameters

Application note 6-29: Where a symmetric algorithm, an asymmetric algorithm and/or a hashing algorithm are used together to form a security protocol, their respective key lengths and hash sizes shall be of (roughly) equal *strength. Table 6-2 shows the allowed cipher suites. ECC keys sizes of 512 bits and 521 bits are considered to be equal in strength for all purposes within this ST.*

[32] Items e) and f) are only applicable where the TOE supports connection to an external GNSS facility.

Cipher suite Id	ECC key size (bits)	AES key length (bits)	Hashing algorithm	MC length (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Table 6-2: Cipher suites

6.1.2.1.3 FCS_RNG – Random number generation

FCS_RNG.1 **Random number generation**

Hierarchical to: -

Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, ~~non-physical true, deterministic, hybrid physical~~, ~~hybrid deterministic~~*] random number generator that implements: [assignment: *class PTG.2 according to [FC_RNG] and to chapter 11. Annex B; PTG 2.1 to PTG2.5*].

(PTG.2.1)	*A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
(PTG.2.2)	*If a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source~~, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy~~].*
(PTG.2.3)	*The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
(PTG.2.4)	*The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
(PTG.2.5)	*The online test procedure checks the quality of the raw random number sequence. It is triggered [selection: ~~externally, at regular intervals,~~ continuously, ~~applied upon specified internal events~~]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *class PTG.2 according to [FC_RNG] and to chapter 11. Annex B; PTG 2.6 to PTG2.7)*.

*Application note 6-30: The function FCS_RNG.1/PSL from the underlying platform (see **[ST_Inf]**) is used.*

(PTG.2.6)	*Test procedure A[33] [as defined in [FC_RNG]] does not distinguish the internal random numbers from output sequences of an ideal RNG.*
(PTG.2.7)	*The average Shannon entropy per internal random bit exceeds 0.997.*

6.1.2.2 Class FIA Identification and authentication

6.1.2.2.1 FIA_ATD – User attribute definition

FIA_ATD.1(2:MS) User attribute definition

Hierarchical to: -

Dependencies: -

FIA_ATD.1.1(2:MS) The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **generation 2 motion sensors**:[

a) Motion sensor identification data:

i. Serial number

ii. Approval number

b) Motion sensor pairing data:

i. Pairing date].

Application note 6-31: For further details see [[2016_799_IC] Annex IC, section 3.12.1.2, and Appendix 1 2.140 and 2.144.

FIA~~_ATD.1(3:EGF) User attribute definition~~

~~Hierarchical to: -~~

~~Dependencies: -~~

FIA_ATD.1.1(3:EGF) ~~The TSF shall maintain the following list of security attributes belonging to individual users~~ ~~**external GNSS facilities**~~ :[

~~a) External GNSS facility identification data:~~

~~i. Serial number~~

~~ii. Approval number~~

~~b) External GNSS facility coupling data:~~

i. ~~Coupling date~~].

Application note 6-32: For further details see [2016_799_IC]] Annex IC, section 3.12.1.3, and Appendix 1 2.133 and 2.134.

6.1.2.2.2 FIA_UAU – User authentication

FIA_UAU.1(1: TC) Timing of authentication (1: TC)

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of Identification

[33] See *[FC_RNG]* Section 2.4.4.

FIA_UAU.1.1(1:TC) The TSF shall allow [reading out of audit records] on behalf of the user to be performed before the ~~user~~ **tachograph card** is authenticated.

FIA_UAU.1.2(1:TC) The TSF shall require each ~~user~~ **tachograph card** to be successfully authenticated **using the method described in [2016_799_IC] Annex 1C, Appendix 11, Part A, Section 10** before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 (2: MD) Timing of authentication

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1 (2:MD) The TSF shall allow [MD identification] on behalf of the user to be performed before the user is authenticated

FIA_UAU.1.2 (2: MD) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

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

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.2.1 (1:MS) The TSF shall require each ~~user~~ **motion sensor** to be successfully authenticated **using the method described in *[2016_799_IC]* Annex 1C, Appendix 11, Section 12** before allowing any other TSF-mediated actions on behalf of that user.

~~FIA_UAU.2 (2:EGF) User authentication before any action (2:EGF)~~

~~Hierarchical to: FIA_UAU.1 Timing of authentication~~

~~Dependencies: FIA_UID.1 Timing of Identification~~

~~FIA_UAU.2.1 (2:EGF) *The TSF shall require each user e**xternal GNSS facility** to be successfully authenticated **using the method described in [2016_799_IC] Annex 1C, Appendix 11, Section 11** before allowing any other TSF-mediated actions on behalf of that user*.~~

6.1.2.3 Class FPT Protection of the TSF

6.1.2.3.1 FPT_TDC – Inter-TSF TSF data consistency

FPT_TDC.1 (1) Inter-TSF basic TSF data consistency

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1 (1) The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [2016_799_IC] Annex IC, Appendix 11] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 (1) The TSF shall use [the interpretation rules (communication protocols) as defined by [2016_799_IC] Annex IC, Appendix 11] when interpreting the TSF data from another trusted IT product.

Application note 6-33: ~~*"Trusted IT product" in this requirement refers to generation 2 tachograph cards, motion sensor, external GNSS facility (if applicable)*~~.

6.1.2.4 Class FTP Trusted path/channels

6.1.2.4.1 FTP_ITC – Inter-TSF trusted channel

FTP_ITC.1(2:TC) **Inter-TSF trusted channel**

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1(2:TC) The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **each tachograph card** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(2:TC) The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3(2:TC) The TSF shall initiate communication via the trusted channel for [all commands and responses exchanged with a tachograph card after successful chip authentication and until the end of the session].

Application note 6-34: Details of the communication channel can be found in [2016_799_IC] Appendix 11, Chapter 10.

~~***FTP_ITC.1(3:EGF)***~~ ~~***Inter-TSF trusted channel***~~

~~*Hierarchical to: -*~~

~~*Dependencies: -*~~

~~*FTP_ITC.1.1(3:EGF)*~~ ~~*The TSF shall provide a communications channel between itself and another trusted IT product* **the external GNSS facility** *that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.*~~.

~~*FTP_ITC.1.2(3:EGF)*~~ ~~*The TSF shall permit [the TSF] to initiate communication via the trusted channel*~~..

~~*FTP_ITC.1.3(3:EGF)*~~ ~~*The TSF shall initiate communication via the trusted channel for [all data exchange].*~~

Application note 6-35: Details of the communication channel can be found in [2016_799_IC] Appendix 11, Chapter 11.

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

The following requirements shall be met only when the TOE is communicating with 1st generation driver, company and control tachograph cards.

6.1.3.1 Class FCS Cryptographic Support

6.1.3.1.1 FCS_CKM – Cryptographic key management

FCS_CKM.1 (2) **Cryptographic key generation**

Hierarchical to: -

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

FCS_CKM.1.1 (2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [cryptographic key derivation algorithms for the session key] and specified

cryptographic key sizes [112 bits] that meet the following: [two-key TDES as specified in [2016_799_IC] Annex IC, Appendix 11 Part A, Chapter 3].

FCS_CKM.2 (2) Cryptographic key distribution

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2mport of user data with security attributes or
FCS_CKM.1]: cryptographic key operation

FCS_CKM.2.1 (2) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [for triple DES session key as specified in [2016_799_IC] Annex IC, Appendix 11 Part A] that meets the following [[2016_799_*IC]* Annex IC, Appendix 11 Part A, Chapter 3]

FCS_CKM.4 (2) Cryptographic key destruction

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 (2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment, : *overwriting with value 0xFF*] that meets the following [

- Requirements in Table 10-1 and Table 10-2;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[34];
- [assignment: *list of further standards [none*]].

6.1.3.1.2 FCS_COP – Cryptographic operation

FCS_COP.1 (4:TDES) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4: Cryptographic key destruction

FCS_COP.1.1 (4:TDES) The TSF shall perform the cryptographic operations (encryption, decryption, Retail-MAC) in accordance with a specified cryptographic algorithm Triple DES in CBC mode and cryptographic key size [112 bits] that meet the following: [[2016_799_IC] Annex IC, Appendix 11 Part A, Chapter 3].

FCS_COP.1(5:RSA) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of data with security attributes or

[34] Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

FCS_CKM.1 Cryptographic key operation]
FCS_CKM.4:Cryptographic key destruction

FCS_COP.1.1 (5:RSA) The TSF shall perform [the cryptographic operations (decryption, verification)] in accordance with a specified cryptographic algorithm (RSA) and cryptographic key size [1024 bits] that meet the following: [[2016_799_IC] Annex IC, Appendix 11 Part A, Chapter 3].

FCS_COP.1 (6:SHA-1) Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes or
FDP_ITC.2 Import of data with security attributes or
FCS_CKM.1 Cryptographic key operation]
FCS_CKM.4:Cryptographic key destruction

FCS_COP.1.1(6:SHA-1) The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS)].

6.1.3.2 Class FIA Identification and authentication

6.1.3.2.1 FIA_UAU – User authentication

FIA_UAU.1 (2: TC) Timing of authentication

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1 (2::TC) The TSF shall allow [reading out of audit records] on behalf of the user to be performed before the ~~user~~ **tachograph card** is authenticated.

FIA_UAU.1.2 (2: TC) The TSF shall require each ~~user~~ **tachograph card** to be successfully authenticated **using the method described in [2016_799_IC] Annex IC, Appendix 11, Chapter 5** before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 Class FPT Protection of the TSF

6.1.3.3.1 FPT_TDC – Inter-TSF TSF data consistency

FPT_TDC.1 (2) Inter-TSF basic TSF data consistency

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1 (2) The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [2016_799_IC] Annex IC, Appendix 11 Part A, Chapter 5] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 (2) The TSF shall use [the interpretation rules (communication protocols) as defined by [2016_799_IC] Annex IC, Appendix 11 Part A, Chapter 5] when interpreting the TSF data from another trusted IT product.

Application note 6-36: "Trusted IT product" in this requirement refers to generation 1 tachograph cards and motion sensor.

6.1.3.4 Class FTP Trusted path/channels

6.1.3.4.1 FTP_ITC – Inter-TSF trusted channel

FTP_ITC.1 (4: TC) Inter-TSF trusted channel

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1 (4:TC) The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **each tachograph card** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 (4: TC) The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 (4: TC) The TSF shall initiate communication via the trusted channel for [data import from and export to a tachograph card in accordance with [2016_799_IC] Appendix 2].

Application note 6-37: Details of the communication channel can be found in [2016_799_IC] Appendix 11, Chapters 4 and 5.

6.2 Security assurance requirements for the TOE

The assurance level for this protection profile is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [*CC_3]*.
These security assurance requirements are derived from [2016_799_IC*]* Annex IC, Appendix 10 (SEC_006).

7 Rationale

7.1 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.

	T.Card_Data_Exchange	T.Remote_Detect_-Data	T.Output_Data	T.Access	T.Calibration_Parameters	T.Clock	T.Design	T.Environment	T.Fake_Devices	T.Hardware	T.Identification	T.Motion_Sensor	T.~~Location_Data~~	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	.Tests	T.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Cert_Infrastrucure	A.Controls	A.Driver_Card_Unique	A.Faithful_Calibration	A.Inspections	A.Compliant_Drivers	A.Type_Appoved_Dev	P.Crypto	P.Management_Device
O.Access				x	x	x			x						x		X													x	
O.Authentication				x	X	x			x		x	~~X~~	x																	X	
O.Accountability											X																				
O.Audit	x	x	x	x					x	x	x	~~X~~	x	x		x	X														
O.Integrity					x												X													X	
O.Output			x							x						x	X														
O.Processing	x				x	x		x	x	x					x	X															
O.Reliability	x						x	x	x	x		~~X~~		x	x	x	X	x													
O.Secure_Ex-change	x	x							x			~~x~~	x		x																
O.Software_-Update																X															X
OE.Deve-lopment							X									x															
OE.Manufacturin g							x											x													
OE.Data_Ge-nera-tion															x								X								
OE.Data_Transp ort															x								x							x	
OE.Delivery															x								X								
OE.Software_Up grade															x		X														X
OE.Data_Strong																	x						x							x	
OE.Test. Points																		x													
OE.Activation				x															X												

	T.Card_Data_Exchange	T.Remote_Detect_-Data	T.Output_Data	T.Access	T.Calibration_Parameters	T.Clock	T.Design	T.Environment	T.Fake_Devices	T.Hardware	T.Identification	T.Motion_Sensor	~~T.Location_Data~~	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	.Tests	T.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Cert_Infrastrucure	A.Controls	A.Driver_Card_Unique	A.Faithful_Calibration	A.Inspections	A.Compliant_Drivers	A.Type_Appoved_Dev	P.Crypto	P.Management_Device
OE.Approved_Workshops					x	x														X						x					
OE.Faithful_Calibration					x	x																				x					
OE.Card_Availability											x										x										
OE.Card_Tra-ceability											x											X									
OE.Controls					x	x		x	x	x				x	x	x	x						x								
OE.Driver_Card_Unique											x														x						
OE.Compliant_Drivers																												x			
OE.Manage-ment device																															X
OE.Regular_Inspections					x				x	X		X		x		x											x				
OE.Type_Approved_ MS[35]									x																				x		
~~OE.Type-Approved_EGF~~									~~x~~																				~~x~~		
OE.EOL							x								x																

Table 7-1 Security Objectives rationale

[35] Identification and authentication of the motion sensor depends on the motion sensor having implemented the required mechanisms to support it.

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

T.Card_Data_Exchange is addressed by O.Secure_Exchange. O.Audit contributes to address the threat by recording events related to card data exchange integrity or authenticity errors. O.Reliability , O.Processing.

T.Remote_Detect_Data is addressed through O.Secure_Exchange, which requires secure data exchange with the remote early detection facility; and through O.Audit, which requires audit of attempts to undermine system security.

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

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.Design is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Reliability . OE.EOL helps to safeguard access to the TOE design through secure disposal of equipment at end of life.

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, contribute to address the threat (OE.Regular_Inspections). Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the VU, which helps addressing the threat.

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, , OE.Faithful_Calibration contributes 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 O.Authentication , O.Audit , O.Processing, O.Reliability and O.Secure_Exchange. OE.Type_Approval_MS and OE.Type_Approcal_EGF help addressing the threat through visual inspection of the whole installation and visible type approval seals.

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_Sensor is addressed by O.Authentication, O.Reliability , O.Secure_Exchange and OE.Regular_Inspections. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

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.Data_Generation, OE.Data_Strong, OE.Data_Transport, OE.Delivery, OE.Software_Upgrade and OE.Controls objectives for the environment. It is also addressed by the O.Access, O.Processing and O..Secured_Data_Exchange objectives to ensure appropriate protection while stored in the VU. O.Reliability also helps in addressing the threat, and OE.EOL helps to safeguard access to the security data through secure disposal of equipment at end of life.

T.Software is addressed in the operational phase 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 data integrity errors. O_Software_Update addresses the possibility of unauthorised software updates. During design and manufacture, the threat is addressed by the OE.Development objective. OE.Controls, OE.Regular_Inspections (checking for the audit records related) also contribute.

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 is included such 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.

T.Tests is addressed by O.Reliability, OE.Manufacturing and OE.Test_Points. If the TOE provides a reliable service as required by O.Reliability 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. OE.Test_Points requires removal of commands, actions and test points before the end of the manufacturing phase, ensuring that they cannot be used zo attack the TOE during the operational phase.Hence, the related threat will be eliminated.

A.Activation is upheld by OE.Activation.

A.Approv_Workshops is upheld by OE.Approv_Workshops.

A.Card_Availability is upheld by OE.Card_Availability

A.Card_Traceability is upheld by OE.Card_Traceability.

A.Cert_infrastructure is upheld by OE.Data_Generation, OE.Data_Transport, OE.Delivery and OE.Data_Strong.

A.Controls is upheld by OE.Controls.

A.Driver_Card_Unique is upheld by OE.Driver_Card_Unique.

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

A.Compliant_Drivers is upheld by OE.Compliant_Drivers.

A.Inspections is upheld by OE.Regular_Inspections.

A.Type_Approved_Dev is upheld by OE.Type_Aprroval_MS ~~*and OE_Type_Approval_EGF*~~.

P.Crypto is addressed through the cryptographic methods used to fulfil O.Access, O.Authentication, O.Integrity, O.Secure_Exchange, OE.Data_Transport and OE.Data_Strong.

P.Management_Device is addressed to fulfil O.Software_Update, OE.Software_Upgrade and OE.Management_Device.

7.2 Security requirements rationale

7.2.1 Rationale for SFRs' dependencies

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

SFR	Dependencies	Rationale
VU Core		
FAU_GEN.1	FPT_STM.1	Satisfied by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Satisfied by FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Satisfied by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Satisfied by FAU_STG.1
FCO_NRO.1	FIA_UID.1	Satisfied by FIA_UID.2

SFR	Dependencies	Rationale
FDP_ACC.1(1:FIL)	FDP_ACF.1)	Satisfied by FDP_ACF.1(1:FIL)
FDP_ACF.1(1:FIL)	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(1:FIL) and FMT_MSA.3 (1:FIL)
FDP_ACC.1(2:FUN)	FDP_ACF.1	Satisfied by FDP_ACF.1(2:FUN)
FDP_ACF.1(2:FUN)	FDP_ACC.1 . FMT_MSA.3	Satisfied by FDP_ACC.1(2:FUN) and FMT_MSA.3 (2: FUN)
FDP_ACC.1(3:DAT)	FDP_ACF.1	Satisfied by FDP_ACF.1(3:DAT)
FDP_ACF.1(3:DAT)	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(3:DAT) and FMT_MSA.3 (3:DAT)
FDP_ACC.1(4:UDE)	DP_ACF.1	Satisfied by FDP_ACF.1(4:UDE)
FDP_ACF.1(4:UDE)	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(4:UDE) and FMT_MSA.3 (4: UDE)
FDP_ACC.1(5:IS)	FDP_ACF.1	Satisfied by FDP_ACF.1(5:IS)
FDP_ACF.1(5:IS)	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(5:IS) and FMT_MSA.2 (5: IS)
DP_ACC.1 (6: Software Upgrade)	FDP_ACF.1	Satisfied by FDP_ACF.1(6: Software Upgrade)
FDP_ACF.1 (6: Software Upgrade	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(6: Software Upgrade) and FMT_MSA.3 (6: Software Upgrade)
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1 S	Satisfied by FDP_ACC.1 (4:UDE)
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(5:IS) and FMT_MSA.3 (5: IS)
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1, FPT_ITC.1 or FTP_TRP.1, FPT_TDC.1	Satisfied by FDP_ACC.1 (5: IS), FPT_ITC.1 (1: MS, 2: TC, ~~3: EGF &~~ 4: TC), FTP_TRP.1 and FPT_TDC.1 (1 & 2)
FDP_RIP.1	-	-
FDP_SDI.2 (1)	-	-
FDP_SDI.2 (2)	-	-
FIA_AFL.1(1:TCL)	IFA_UAU.1	Satisfied by FIA_UAU.1(1:TC)
FIA_AFL.1(2:TCR)	FIA_UAU.1	Satisfied by FIA_UAU.1(1:TC)
FIA_AFL.1(3:MS)	FIA_UAU.1	Satisfied by FIA_UAU.2(2:MS)
~~FIA_AFL.1(4:EGF)~~	~~FIA_UAU.1)~~	~~Satisfied by FIA_UAU.2(3:EGF)~~
FIA_ATD.1(1:TC)	-	-
IA_UAU.3	-	-
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA_UID.2	-	-
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Satisfied by FDP_ACC.1 2: FUN), FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3(1:FIL)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1

SFR	Dependencies	Rationale
FMT_MSA.3(2:FUN)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
FMT_MSA.3(3:DAT)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
FMT_MSA.3(4:UDE)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
FMT_MSA.3(5:IS)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
FMT_MSA.3 [6: SW-Upgrade)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
FMT_MOF.1(1)	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_MOF.1(2)	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_MOF.1(3)	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_MOF.1(4)	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_MOF.1(5)	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	Satisfied by FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2
FPT_FLS.1	-	-
FPT_PHP.2	FMT_MOF.1	Not applicable as there is no management of the list of users to be notified or list of devices that should notify
FPT_PHP.3	-	-
FPT_STM.1	-	-
FPT_TDC.1(1)	-	-
FPT_TST.1	-	-
FTP_ITC.1(1:MS)	-	-
2nd generation specific		
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2 (1), FCS_COP.1 (1:AES & 3: ECC) and FCS_CKM.4 (1)
FCS_CKM.2(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1 (1) and FCS_CKM.4 (1)
FCS_CKM.4(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1 (1)
FCS_COP.1(1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1
FCS_COP.1(2:SHA-2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-2
FCS_COP.1(3:ECC)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2, FCS_CKM.1 (1) and FCS_CKM.4 (1)
FCS_RNG.1[36]	-	-
FIA_ATD.1(2:MS)	-	-
~~FIA_ATD.1(3:EGF)~~	-	-
FIA_UAU.1(1:TC)	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.2(1:MS)	FIA_UID.1	Satisfied by FIA_UID.2
~~FIA_UAU.2(3:EGF)~~	~~FIA_UID.1~~	~~Satisfied by FIA_UID.2~~
FPT_TDC.1(2)	-	-
~~FTP_ITC.1(3:EGF)~~	-	-
1st generation specific		
FCS_CKM.1(2)F	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2, FCS_COP.1 and FCS_CKM.4
FCS_CKM.2(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FCS_CKM.1
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1
FCS_COP.1(4:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1
FCS_COP.1(5:RSA)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1

[36] Extended component

SFR	Dependencies	Rationale
FCS_COP.1(6:SHA1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1
FIA_ATD.1(4:MS)	-	-
FIA_UAU.1(2:TC)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(3)	-	-
FTP_ITC.1 (4: TC)	-	-

Table 7-2 SFR's dependencies

7.2.2 Security functional requirements rationale

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

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Data_Exchange		O.Software_Upgdate
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		
FDP_ACC.1	Subset access control (1:FIL)	x										
FDP_ACF.1	Security attribute based access control (1: FIL)	x										
FDP_ACC.1	Subset access control (2: FUN)	x						x	x	x		
FDP_ACF.1	Security attribute based access control (2: FUN)	x						x	x	x		
FDP_ACC.1	Subset access control (3: DAT)	x										
FDP_ACF.1	Security attribute based access control (3. DAT)	x										
FDP_ACC.1	Subset access control (4: UDE)	x										
FDP_ACF.1	Security attribute based access control (4: UDE)	x										
FDP_ACC.1	Subset access control (5: IS)	x						x	x			
FDP_ACF.1	Security attribute based access control)5:IS)	x						x	x			
FDP_ACC.1	Subset access control)6: Software Upgrade)	x						x	x			x
FDP_ACF.1/	Security attribute based access control (6: Software Upgrade)	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	Import of user data with security attributes							x	x	X		
								x	x			
FDP_RIP.1	Subset residual information protection	x						x	x			
FDP_SDI.2	Stored data integrity monitoring and action(/1)			x		x	x		x			

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Data_Exchange		O.Software_Upgdate
FDP_SDI.2	Stored data integrity monitoring and action (2)			x				x	x			
FIA_AFL.1	Authentication failure handling (1: TCL)			x	x							
FIA_AFL.1e	Authentication failure handling (2: TCR)			x	x							
FIA_AFL.1	Authentication failure handling (3: MS)			x	x				x			
~~***FIA_AFL.1***~~	~~Authentication failure handling (4: EGF)~~			~~x~~	~~x~~				~~x~~			
FIA_ATD.1	User attribute definition (1:TC)			x						x		
FIA_UAU.1/TC	Timing of authentication				x					x		
FIA_UAU.1/PIN	Timing of authentication				x							
FIA_UAU.1 (2: MD)	Timing of authentication				x							
					x					X		
FIA_UAU.3	Unforgeable authentication				x							
FIA_UAU.5	Multiple authentication mechanisms	x			x					x		
FIA_UAU.6	Re-authenticating				x					x		
FIA_UID.2	User identification before any action	x	x	x	x					x		
FMT_MSA.1	Management of security attributes	x								X		
FMT_MSA.3	Static attribute initialisation (1: FIL)	x						x	x	X		
FMT_MSA.3	Static attribute initialisation (2:FUN)	x						x	x	x		
FMT_MSA.3	Static attribute initialisation (3:DAT)	x										
FMT_MSA.3	Static attribute initialisation (4: UDE)	x										
FMT_MSA.3	Static attribute initialisation (5: IS)	x						x	x			
FMT_MSA.3	Static attribute initialisation)6: Software Upgrade)	x						x	x			x
FMT_MOF.1	Management of security functions (1)	x				x	x	x	x			
FMT_MOF.1	Management of security functions (2)	x						x				
FMT_MOF.1	Management of security functions (3)	x			X							
FMT_MOF.1	Management of security functions (4)	x			X							
FMT_MOF.1	Management of security functions (5)	x			x							
FMT_MTD.1	Management of TSF Data	x			x	x		x	X			
FMT_SMF.1	Specification of Management Functions	x								x		

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Data_Exchange		O.Software_Upgdate
FMT_SMR.1	Security roles	x								x		
FPT_FLS.1	Failure with preservation of secure state.									X		
FPT_PHP.2	Notification of physical attack								x			
FPT_PHP.3	Resistance to physical attack						x	x	X			
FPT_STM.1	Reliable time stamps		x	x				X	x			
FPT_TDC.1	Inter-TSF basic TSF data consistency (1)							x	x			
FPT_TST.1	TSF testing			x					x			
FPT_ITC.1	Inter-TSF trusted channel (1:MS)									x		
FCS_CKM.1	Cryptographic key generation (1)				x					x		
FCS_CKM.2	Cryptographic key distribution (1)				x					x		
FCS_CKM.4	Cryptographic key destruction (1)				x					x		
FCS_COP.1	Cryptographic operation (1: AES)				x					x		
FCS_COP.1	Cryptographic operation (2: SHA-2)				x					x		
FCS_COP.1	Cryptographic operatiom (3:ECC)				x					x		
FCS_RNG.1	Random Number Generation				x					x		
FIA_ATD.1)	User attribute definition (2:MS)				x					x		
~~***FIA_ATD.1)***~~	~~User attribute definition (3:EGF)~~				~~x~~					~~x~~		
FIA_UAU.1	FIA_UAU.1 Timing of authentication (1:TC)				x					x		
FIA_UAU.2	User authentication before any action (1:MS)				x					x		
~~***FIA_UAU.2***~~	~~User authentication before any action (2:EGF)~~				~~x~~					~~x~~		
FPT_TDC.1)	Inter-TSF basic TSF data consistency (1)							x	x			
FTP_ITC.1)	Inter-TSF trusted channel (2: TC)									x		
~~***FTP_ITC.1)***~~	~~Inter-TSF trusted channel (3: EGF)~~									~~x~~		
FCS_CKM.1	Cryptographic key generation (2)									x		
FCS_CKM.2	Cryptographic key distribution (2)									x		
FCS_CKM.4	Cryptographic key destruction (2)									x		
FCS_COP.1	Cryptographic operation (4:TDES)									x		
FCS_COP.1	Cryptographic operation (5:RSA)									x		
FCS_COP.1	Cryptographic operation (6:SHA-1)									x		
FIA_UAU.1	Timing of authentication (2: TC)				x					x		
FPT_TDC.1	Inter-TSF basic TSF data consistency (2)							x	x			

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Data_Exchange		O.Software_Upgdate
FTP_ITC.1)	Inter-TSF trusted channel (4: TC)									**x**		

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

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

Security objectives	SFR	Rationale
O.Access	***FDP_ACC.1 (1: FIL)*** ***FDP_ACF.1 (1: FIL)***	The File structure SFP defines the policy for restricting modification or deletion of application and data files structure and access conditions.
	FDP_ACC.1(2: FUN) ***FDP_ACF.1(2: FUN)***	Function SFP defines the policy for control of access to specific functions (e.g. in calibration mode only).
	FDP_ACC.1 (3: DAT) ***FDP_ACF.1(3: DAT)***	The DATA SFP defines the policy for control of access to cryptographic keys and vehicle identification data. It also defines data that must be stored by the VU.
	FDP_ACC.1 (4: UDE) ***FDP_ACF.1(4: UDE)***	The User_Data_Export SFP defines the policy for data storage on tachograph cards, for use of the ITS interface, for output of driver related data, and for printing and display.
	FDP_ACC.1 (5: IS) ***FDP_ACF.1 (5: IS)***	The Input Sources SFP defines policy to ensure at data is processed only from the right input sources. This restricts attempts to undermine TOE security through use of incorrect input sources (e.g. input and execution of unauthorised code).
	FDP_ACC.1 (6:Sodtware Upgrade ***DP_ACF.1 (6: /Software-Upgrade)***	The SFP SW-Upgrade for the upgrade of the software in the TOE
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon the deallocation of the resource
	FIA_UID.2	Connected devices have to be successfully identified before allowing any other action
	FMT_MSA.1	Supports the Function *SFP by* restricting the ability to change default the security attributes User Group, User ID to nobody**.**
	FMT_MSA.3 (1: FIL)	Supports 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 (2: FUN)	Supports the Function SFP 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(3: DAT)	Supports the Data SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.

Security objectives	SFR	Rationale
	FMT_MSA.3(4: UDE)	Supports the User Data Export SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3(5: IS)	Supports the Input Sources SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3 (6: Software Upgrade)	Provides the SW_Upgrade SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MOF.1 (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_MOF.1 (2)	Restricts the ability to enter calibration mode to workshop cards.
	FMT_MOF.1 (3)	Restricts the ability to carry out company locks to company cards
	FMT_MOF.1 (4)	Restricts the ability monitor control activities to control cards.
	FMT_MOF.1 (5)	Restricts access to the download functions.
	FMT MTD.1	Restricts the ability to carry out manual time setting to workshop cards.
	FMT_SMF.1	Identifies the capability to carry out specified management functions.
	FMT_SMR.1	Defines the management roles that provide the basis for access control.
O.Accountability	***FAU_GEN.1***	Generates correct audit records
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behaves correctly 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	Devices are 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

Security objectives	SFR	Rationale
	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 correctly if the audit trail is full.)
	FDP_SDI.2 (1)	Monitors stored user data for integrity errors
	FIA_AFL.1 (1:TCL)	Detects and records authentication failure events for the locale use of tachograph cards
	FIA_AFL.1 (2: TCR)	Detects and records authentication failure events for the remote card use (company card)
	FIA_AFL.1(3: MS)	Detects and records authentication failure events for the motion sensor
	~~***FIA_AFL.1(4: EGF)***~~	~~Detects and records authentication failure events for the external gateway facility.~~
	FIA_ATD.1 (1: TC)	Defines user attributes for tachograph cards to support traceability of audited events
	FIA_UID.2	Devices are successfully identified before allowing any other action, supporting the traceability of audit events
	FPT_STM.1	Provides accurate time to be recorded when audit records are generated
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
O.Authentication	***FDP_ACC.1(4:UDE)*** ***FDP_ACF.1(4:UDE)***	Restricts the ability to read remote early detection communication facility data to control cards
	FIA_AFL.1 (1: TCL)	Detects and records authentication failure events for the local use of tachograph cards
	FIA_AFL.1 (2: TCR)	Detects and reports authentication failure events for the remote use of company tachograph cards
	FIA_AFL.1(3: MS)	Detects and records authentication failure events for the motion sensor
	~~***FIA_AFL.1(4: EGF)***~~	~~Detects and records authentication failure events for the external GNSS facility.~~
	F***IA_ATD.1(2:MS)*** ~~***FIA_ATD.1(3:EGF)***~~	These attributes identify the motion sensor ~~*or external GNSS facility*~~ connected to the vehicle unit.
	FIA_UAU.1/TC	Allows TC identification before authentication
	FIA_UAU.1/PIN	Allows TC (Workshop Card) identification before authentication
	FIA_UAU.1 (2: /MD)	Allows MD identification before authentication
	FIA_UAU.3	Provides unforgeable authentication
	FIA_UAU.5	Multiple authentication mechanisms are required for use of workshop cards
	FIA_UAU.6	Periodically re-authenticate the tachograph cards

Security objectives	SFR	Rationale
	FIA_UID.2	Connected devices are successfully identified before allowing any other action
	FMT_MOF.1(3)	Restricts the ability to carry out company locks management to company cards.
	FMT_MOF.1(4)	Restricts the ability to monitor control activities to control cards.
	FMT_MOF.1(5)	Restricts access to the download functions
	FMT_MTD.1	Restricts the ability to carry out manual time setting to workshop cards.
	FCS_CKM.1(1)	Key generation to support the authentication process.
	FCS_CKM.2(1)	Key distribution to support the authentication process.
	FCS_CKM.4(1)	Key destruction when temporary keys are no longer required.
	FCS_COP.1(1:AES)	Cryptographic algorithm used to support authentication.
	FCS_COP.1(2:SHA-2)	Cryptographic algorithm used to support authentication.
	FCS_COP.1(3:ECC)	Cryptographic algorithm used to support authentication.
	FCS_RNG.1	Random numbers are generated in support of cryptographic key generation for authentication.
	FIA_UAU.1(1:TC & 2:TC)	A tachograph card has to be successfully authenticated.
	FIA_UAU.2(1:MS)	A motion sensor has to be successfully authenticated before allowing any action.
O.Integrity	~~***FIA_UAU.2(2:EGF)***~~	~~An external GNSS facility has to be successfully authenticated before allowing any action~~
	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 User_Data_Export SFP
	FDP_SDI.2(1)	monitors user data stored for integrity error
	FMT_MOF.1(1)	Prevents access to commands used in manufacturing that may be used to affect outputs.
	FMT_MTD.1	Prevents unauthorized time changes that may affect data integrity.
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. Data downloaded is protected by signature against undetected modification.
	FDP_SDI.2(1)	monitors user data stored for integrity error

Security objectives	SFR	Rationale
	FMT_MOF.1(1)	Prevents access to commands used in manufacturing that may be used to affect outputs.
	FPT_PHP.2 ***FPT_PHP.3***	Requites resistance to physical attack to the TOE software in the field, and detection of attempted attacks on the TOE, after the TOE activation
	FPT_TDC.1	Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer
O.Processing	***FDP_ACC.1 (2: FUN)*** ***FDP_ACF.1(2:FUN)***	The Function SFP defines the policy for control of access to specific functions (e.g. in calibration mode only).
	FDP_ACC.1 (: IS) ***FDP_ACF.1 (2: IS)***	The Input Sources SFP defines the policy to ensure that data is processed only from the right input sources. This restricts attempts to undermine TOE security through use of incorrect input sources (e.g. input and execution of unauthorised code).
	FDP_ACC.1 (6: Software Upgrade) ***DP_ACF.1 (6: Software Upgrade)***	Defines security attributes for SFP SW-Upgrade
	FDP_ITC.1	Implements the Input Sources SFP to control processing of data only from the correct input sources.
	FDP_ITC.2	Handles integrity and authenticity errors in data imported with security attributes.
	FDP_ITC.2	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_MSA.3(2: FUN)	Supports the Function SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FDP_MSA.3 (5: IS)	Supports the Input Sources SFP o 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 (6: Software 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.
	FDP_SDI.2(2)	Requires consistency between motion sensor data and GNSS data.

Security objectives	SFR	Rationale
	FMT_MOF.1(1)	Prevents access to commands used in manufacturing that may be used to interfere with accurate processing.
	FMT_MTD.1	Restricts the ability to carry out manual time setting to workshop cards
	FPT_PHP.3	Requires resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1 (1)	Requires correct interpretation of attributes and data between trusted products
	FPT_TDC.1(2)	Requires correct interpretation of attributes and data between trusted products.
	FPT_TDC.1	Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer
O.Reliability	***FDP_ACC.1 (2: FUN)*** ***FDP_ACF.1 (2:FUN)***	The Function SFP defines the policy for control of access to specific functions (e.g. in calibration mode only).
	FDP_SDI.2(1 & 2)	Requires consistency between motion sensor data and GNSS data
	FDP_ACC.1(5: IS) ***FDP_ACF.1 (5: IS)***	The Input Sources SFP defines policy to ensure that data is processed only the right input sources.
	FDP_ACC.1 (6: Software Upgrade) ***FDP_ACF.1 (6: Software Upgrade)***	Defines security attributes for SFP SW-Upgrade his restricts attempts to undermine TOE security through use of incorrect input sources (e.g. input and execution of unauthorised code)
	FDP_ITC.1	Implements the Input Sources SFP to control processing of data only from the correct input sources.
	FDP_ITC.2/	Handles integrity and authenticity errors in data imported with security attributes.
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon the deallocation of the resource
	FDP_SDI.2(1 & 2)	monitors user data stored for integrity error
	FIA_AFL.1 (1: TCL)	Detects and records authentication failure events for the local use of tachograph cards
	FIA_AFL.1 (2: TCR)	Detects and records authentication failure events for the remote use of company tachograph cards
	FIA_AFL.1(3: MS)	Detects and records authentication failure events for the motion sensor
	~~***FIA_AFL.1(4: EGF)***~~	~~Detects and records authentication failure events for the external GNSS facility~~
	FMT_MSA.3 (2: FUN)	Supports the Function SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify

Security objectives	SFR	Rationale
		alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3 (5: IS)	Supports the Input Sources SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3 (6: Software – Upgrade)	Provides the Software Upgrade SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MOF.1 (1)	Prevents access to commands used in manufacturing that may be used to interfere with accurate processing.
	FMT_MOF.1 (2)	Restricts the ability to enter calibration mode to workshop cards.
	FMT_MTD.1	Restricts the ability to carry out manual time setting to workshop cards.
	FPT_FLS.1	Preserves a secure state when the following types of failures occur.
	FPT_PHP.2	Detection of physical tampering (Power_Deviation) and generation of an audit record
	FPT_PHP.3	Requires resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
	FPT_TDC.1 (1)	Requires consistently between motion sensor data and GNSS data.
	FPT_TDC.1(2)	Requires correct interpretation of attributes and data between trusted products.
	FPT_TDC.1	Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer
O.Secure_Exchange	***FCO_NRO.1***	Generates an evidence of origin for the data to be downloaded to external media.
	FDP_ACC.1 (2: FUN) ***FDP_ACF.1 (2: FUN)***	The Function SFP defines the policy for control of access to specific functions (e.g. in calibration mode only).
	DP_ACC.1 (4:UDE) ***FDP_ACF.1 (4:UDE)***	Restricts the ability to read remote early detection communication facility data to control cards.
	FDP_ETC.2	Provides export of user data with security attributes using the User_Data_Export SFP.
	FDP_ITC.2	Handles integrity and authenticity errors in data imported with security attributes.
	FIA_ATD.1(1:TC)	Defines user attributes for tachograph cards.
	FIA_ATD.1(2:MS) ~~***FIA_ATD.1(3:EGF)***~~	These attributes identify the motion sensor ~~*or external GNSS facility*~~ connected to the vehicle unit.

Security objectives	SFR	Rationale
	FIA_UAU.6	Periodically re-authenticate the tachograph cards
	FIA_UID.2	Connected devices are successfully identified before allowing any other action
	FMT_MSA.1	Supports the *Function SFP* to restrict the ability to change default the security attributes User Group, User ID to nobody
	FMT_MSA.3(2: FUN)	Supports the *Function SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP and allows *nobody* to specify alternative initial values to override the default values when an object or information is created.
	FMT_MTD.1	Restricts the ability to carry out manual time setting to workshop cards.
	FMT_SMF.1	Identifies the capability to carry out specified management
	FMT_SMR.1	Defines the management roles that provide the basis for access control
	FCS_CKM.1 (1)	Key generation used to support authentication for the exchange.
	FCS_CKM.2 (1)	Key distribution to support authentication for the exchange
	FCS_CKM.4 (1)	Specifies the requirements for key destruction
	FCS_COP.1- (1: AES)	Cryptographic algorithm used to support authentication
	FCS_COP.1 (2: SHA-2)	Cryptographic algorithm used to support authentication
	FCS_COP.1 (3: ECC)	Cryptographic algorithm used to support authentication
	FCS_RNG.1	Random numbers are generated in support of cryptographic key generation
	FIA_UAU.1(1: TC)	Tachograph card has to be successfully authenticated.
	FIA_UAU.2(1: MS)	Motion sensor has to be successfully authenticated before allowing any action
	~~***FIA_UAU.2(2: EGF)***~~	~~External GNSS facility has to be successfully authenticated before allowing any action~~
	FTP_ITC.1(1:MS)	Provides a trusted channel for the motion sensor.
	FTP_ITC.1(2:TC)	Provides a trusted channel for generation 2 tachograph cards.
	~~***FTP_ITC.1(3:EGF)***~~	~~Provides a trusted channel for the external GNSS facility.~~
	FTP_ITC.1(4:TC)	Provides a trusted channel for generation 1 2 tachograph cards.
	FCS_CKM.1 (2)	Key generation used to support authentication for the exchange.
	FCS_CKM.2 (2)	Key distribution to support authentication for the exchange
	FCS_CKM.4 (2)	Specifies the requirements for key destruction

Security objectives	SFR	Rationale
	FCS_COP.1- (4: DES)	Cryptographic algorithm used to support authentication
	FCS_COP.1 (5: RSA)	Cryptographic algorithm used to support authentication
	FCS_COP.1 (6: SHA-1)	Cryptographic algorithm used to support authentication
	FIA_UAU.1(2: TC)	Tachograph card has to be successfully authenticated
O.Software_Update	***FDP_ITC.2***	Provides verification of imported software updates

Table 7-4 Suitability of the SFRs

7.2.3 Security Assurance Requirements Rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by *[2016_799_IC]* Annex I C, Appendix 10.

This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or TOE 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 3-3 Subjects and external entities, entry 'Attacker'). This decision represents a part of the conscious security policy for the recording equipment required by the regulation *[2016_799_IC]* 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 components, all dependencies are met or exceeded in the EAL4 assurance package:

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

Table 7-5 SAR Dependencies (additional to EAL 4 only)

7.2.4 Security Requirements – Internal Consistency

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

c) SFRs

The dependency analysis in section7.2.1 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current PP accurately reflects the requirements of Commission Implementing Regulation 2016/799 implementing Regulation 165/2014 of the European Parliament and of the Council, Annex IC *[2016_799_IC]*, which is assumed to be internally consistent

d) SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 7.2.3 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 7.2.1 and 7.2.3 Furthermore, as also discussed in section 7.2.3, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

8 TOE summary specification

The TOE provides the following security services.

8.1 TOE_SS.Identification_Authentication

The TOE identifies and authenticates tachograph cards and motion sensors. The TOE identifies and authenticates the workshop user by his card and additionally his PIN

Note: Identification and Authentication of an external GNSS facility is not applicable for the TOE.

Application note 8-1 *The vehicle unit is able to authenticate the connected motion sensor by MS approval number and MS serial number or by MS extended serial number at motion sensor pairing. At motion sensor re-connection and at power supply recovery the vehicle unit authenticates the connected motion sensor by the usage of the correct and valid session key. The use of copied or replayed authentication data is prevented and will be detected*

Security functional requirements concerned:

- FIA_UID.2: User Identification before any action
- (FIA_UAU.3, FIA_UAU.5, FIA_UAU.6): authentication
- FIA_UAU.1 (1: TCL): Timing of authentication
- FIA_AFL.1 (1: TC): Authentication failure handling: tachograph cards
- FIA_AFL.1 (2: TCR): Authentication failure handling: remote tachograph company card
- FIA_AFL.1 (3: MS): Authentication failure handling: motion sensor
- (FIA_ATD.1 (1:TC), FMT_SMR.1): User groups to be maintained by the TOE

FMT_MSA.3 (2: FUN): Static attribute initialization: (functions)

FDP_ACC.1 (2: FUN): subset access control: (functions

FIA_UID.2User Identification before any action

Supported by:

-
- 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: Management of security attributes
- FMT_SMF.1: Specification of management functions

8.2 TOE_SS.Access_Control

The TOE controls access to stored data and functions based on the mode of operation.

The TOE regularly sends its current remote early detection data to the internal or external remote early detection communication facility (REDCF). This data is encrypted and authenticated. The data can be accessed by any remote early detection communication reader that interrogates the REDCF, without any authentication being necessary. Access to remote early detection communication data is controlled on the basis of possession of the correct key from which the TOE-specific decryption key can be derived.

Security functional requirements concerned:

- FDP_ACC.1 (1:/FIL): Subset access control: (file structure)
- FDP_ACF.1 (1: FIL): Security attribute based access control: (file structure)
- FDP_ACC.1 (2: FUN): Subset access control (functions)
- FDP_ACF.1 (2: FUN): Security attribute based access control (functions)
- (FDP_ACC.1 (3: DAT): Subset access control: (data)

- FDP_ACF.1 (3: DAT): Security attribute based acess control (data)
- (FDP_ACC.1 (4: UDE) Subset access control: (user data export)
- FDP_ACF.1 (4: UDE): Security attribute based access control. (user data export)
- (FDP_ACC.1 (5: IS): Subset access control: (Input sources)
- FDP_ACF.1 (5:IS): Security attribute based access control: (Input sources)

Supported by:

- (FIA_UAU.2 (1: MS), FIA_UAU.3): Authentication: (motion sensor)
- (FIA_UAU.1 (1: TC), FIA_UAU.3, FIA_UAU.5, FIA_UAU.6): Authentication: tachograph cards)
- FMT_MSA.3 (1: FIL);): Static attribute initialization: (file structure)
- FMT_MSA.3 (2: FUN)): Static attribute initialization control: (functions)
- FMT_MSA.3 (3: DAT):): Static attribute initialization control: (data)
- FMT_MSA.3 (4: UDE):): Static attribute initialization: (user data export)
- FMT_MSA.3 (5: IS): (Input sources)
- (FMT_MSA.1: Management of security attributes
- FMT_SMF.1: Specification of management functions
- FMT_SMR.1: Security management roles

8.3 TOE_SS.Accountability of users

User activity is recorded such that users can be held accountable for their actions.

Security functional requirements concerned:

- FAU_GEN.1:Security audit data generation
- FAU_STG.1: Protected audit trail storage
- FAU_STG.4: Prevention of data loss
- FDP_ETC.2: Export of user data with security attributes

Supported by:

- (FDP_ACC.1 (3:DAT): Subset access control (data)
- FDP_ACF.1 (3: DAT): Security attribute based access control: (data)
- (FDP_ACC.1 (4:UDE):: Subset access control: (user data export)
- FDP_ACF.1 (4: UDE): Security attribute based access control: (user data export)
- FPT_STM.1: Reliable time stamp
- FCS_COP.1 (1: AES): for the motion sensor and the tachograph cards

8.4 TOE_SS.Audit of events and faults

The TOE detects and records a range of events and faults.

Security functional requirements concerned:

- FAU_GEN.1: Security audit data generation
- FAU_SAR.1: Audit review
- Supported by:
- (FDP_ACC.1 (3:DAT): Subset access control: (data)

- FDP_ACF.1 (3: DAT): Security attribute based access control: : (data)
- FDP_ETC.2 Export of user data with security attributes

8.5 TOE_SS.Residual information protection for secret data

Encryption keys and certificates are deleted from the TOE when no longer needed, such that the information can no longer be retrieved

Security functional requirements concerned:

- FDP_RIP.1 Subset residual information protection
- Supported by

FCS_CKM.4: Cryptographic key destruction

8.6 TOE_SS.Integrity and authenticity of exported data

The integrity and authenticity of user data exported (downloaded) to an external storage medium, in accordance with *[2016_799_IC]*, Annex IC, Appendix 7, is assured through the use of digital signatures.

Security functional requirements concerned:

- FCO_NRO.1 Selective proof of origin
- FDP_ETC.2 Export of user data with security attributes
- Supported by
- FCS_COP.1 (3: ECC): Cryptographic operation

8.7 TOE_SS.Stored_Data_Accuracy

Data stored in the TOE fully and accurately reflects the input values from all sources (motion sensor, VU real time clock, calibration connector, Tachograph cards, VU keyboard, external GNSS facility (if applicable- **Note: not applicable**)).

Security functional requirements concerned:

- FDP_ITC.1: import of user data without security attributes
- FDP_ITC.2:import of user data with security attributes
- FPT_TDC.1 (1): Inter-TSF basic TSF data consistency
- FPT_TDC.1 (2): Inter-TSF basic TSF data consistency
- FDP_SDI.2: Stored data integrity monitoring and action (1)
- FDP_SDI.2: Stored data integrity monitoring and action (2)

Supported by:

- (FDP_ACC.1 (5: IS): Subset access control: (input sources)
- FDP_ACF.1 (5: IS): Security attribute based access control: (input sources)
- (FDP_ACC.1(2: FUN): Subset access control: (functions)
- FDP_ACF.1(2: FUN Security attribute based access control: (functions)
- FAU_GEN.1 Security audit data generation
- FPT_STM.1: Reliable time stamps
- (FIA_UAU.2 (1: MS), FIA_UAU.3): Authentication: (motion sensor)
- (FIA_UAU.1 (1: TC), FIA_UAU.3, FIA_UAU.5, FIA_UAU.6): Authentication: tachograph cards)

8.8 TOE_SS.Reliability

The TOE provides features that aim to assure the reliability of its services. These features include but are not limited to self-testing, physical protection, control of executable code, resource management, and secure handling of events.

Security functional requirements concerned:

- FDP_ITC.2: Import of user data with security attributes
- F FPT_FLS.1: Failure with preservation of secure state
- FPT_PHP.2: Notification of physical attack
- FPT_PHP.3: Resistance to physical attack: stored data
- FPT_TST.1: TSF testing
- FDP_ACC.1 (6: SW-Upgrade) : Subset access control
- FDP_ACF.1 (6:SW-Upgrade): Security based access control
- FDP_ITC.2: Import of user data with security attributes
- FPT_TDC.1
- FMT_MSA.3 (6: SW-Upgrade) Static attribute initialization control: (Software 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 withdrawl

FMT_MOF.1: No test entry points

8.9 TOE_SS.Data_Exchange

The TOE provides this security service of data exchange with the motion senor and tachograph cards.

Security functional requirements concerned:

- FDP_ETC.2 Export of user data with security attributes: to the TC
- FDP_ITC.2 Import of user data with security attributes: from the MS and the TC
- Supported by:
- FCS_COP.1 (1: AES): for the motion sensor and the tachograph cards
-
- FCS_COP.1 (3: ECC): 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
- (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC
- FAU_GEN.1: Audit records: Generation

8.10 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 Appendix 11 of Annex IC *[2016_799_IC]*.

Security functional requirements concerned:

-
- FCS_COP.1 (1: AES) for the motion sensor and the tachograph cards and for Software Upgrade
- FCS_COP.1 (3: ECC): for data downloading to external media (signing) and for the Software Upgrade

- (FCS_CKM.1, FCS_CKM.2, FCS_CKM.4): cryptographic key management

9 Reference documents

Common Criteria

[CC_1] **Common Criteria** for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[CC_2] **Common Criteria** for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[CC_3] **Common Criteria** for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

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

Digital tachograph: directives and standards

[2016_799_IC] **Commission Implementing Regulation (EU) 2016/799** of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, Annex I C last amended by Commission Implementing Regulation (EU) 2018/502 of 28 February 2018

[2016_799_11] **Anlage 11** zum Anhang IC der Durchführungsverordnung (EU) 2016/799

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

[PP] **Common Criteria Protection Profile**, Digital Tachograph – Vehicle Unit (VU PP),, Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 Mary 2016 implementing Regulation (EU) 165/2014 (Annex IC), Version 1.0, 9th September 2016, DG JRC – Directorate E – Space, Security and Migration Cyber and Digital Citizens' Security Unit E3, BSI-CC-PP-0094, 9 May 2017

[16844-4] **ISO 16844-4:** 2015. Road Vehicles – Tachograph Systems- Part 4: CAN Interface

Other directives and standards

[2019_1213_EU] **Commission Implementing Regulation (EU) 2019/1213** of 12 July 2019 – laying down detailed provisions ensuring uniform conditions for the implementation of interoperability and compatibility of on-board weighing equipment pursuant to Council Directive 96/53/EC

[96_53_EC] **Council Directive 96/53/EC** of 25 July 1996 - laying down for certain road vehicles circulating within the Community the maximum authorized dimensions in national and international traffic and the maximum authorized weights in international traffic – last amended by Directive (EU) 2015/719 of the European Parliament and of the Council of 29 April 2015

[FC_RNG] A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011

[TL-03415] Anforderungen und Prüfbedingungen für Sicherheitsetiketten, BSI TL-03415, Bundesamt für Sicherheit in der Informationstechnik, Version: 1.4, Juli 2011

[PUB_46_3] **FIPS PUB 46-3 Federal Information Processing Standards Publication Data Encryption Standard (DES) Reaffirmed 1999 October 25**

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

[PKCS.1] **PKCS #1:** RSA Cryptography Specifications, Version 2.0. RSA Laboratories, September 1998

[SHS] **FIPS PUB 180-4:** Secure Hash Standard, NIST, March 2012

[*ISO_9797_1]* **ISO/IEC 9797-1,** Information technology -- Security techniques -- Message Authentication Codes (MACs), 2011

[*RFC_5639]* **RFC 5639** Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010

[PUB_197] **FIPS PUB 197,** U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES)

[*RFC_5480]* **RFC 5480** Elliptic Curve Cryptography Subject Public Key Information, March 2009

[RFC_5689] **RFC 5869** HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010

[TR_03111] **TR-03111**, Technical Guideline, Elliptic Curve Cryptography, BSI; version 2.00, 2012-06-28

[SP 800-38B] **SP 800-38B** National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005

[*PUB_186-4]* **FIPS PUB 186-4:** Digital Signature Standard (DSS), NIST, July 2013

[*ISO_10116]* **ISO 10116:** Information technology — Security techniques — Modes of operation of an n- bit block cipher. Third edition, 2006-02-01

[ISO_15946-1] **ISO 15946-1:2002** Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General

[ANSI X9.62] **ANSI X9.62:2005** Public Key Cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)

[ST_Inf] **Security Target Lite M9900, M9905, M9906** including optional Software Libraries RSA-EC-SCL-HCL-PSL, Infineon AG; version 3.6, 06.07.2018

[1381_StCo] **DTCO 1381**, Statement of compatibility, Revision 1.17. 09.10.2018, Continental Automotive GmbH

[SHA1] **FIPS PUB 180-1:** *Secure Hash Standard,* NIST, April 1995.

10 Annex A – Key & Certificate Tables

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

Table 10-1	First-generation asymmetric keys generated, used or stored by a VU
Table 10-2	First-generation symmetric keys generated, used or stored by a VU
Table 10-3	First-generation certificates used or stored by a VU
Table 10-4	Second-generation asymmetric keys generated, used or stored by a VU
Table 10-5	Second-generation symmetric keys generated, used or stored by a VU
Table 10-6	Second-generation certificates used or stored by a VU

In general, a vehicle unit will not be able to know when it has reached end of life and thus will not be able to make permanent secret keys unavailable. Therefore, for the purposes of the tables below, 'end of life' is defined as one of following circumstances:

a) When support for the Generation-1 cryptography is suppressed by a workshop, as described in Application note 1-3;

b) When the (Gen. 2) vehicle unit sign certificate has reached its end of validity. If other circumstances necessitate the decommissioning of a vehicle unit, making unavailable the permanently stored keys mentioned in this table, if feasible, is a matter of organisational policy.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
VU.SK	VU private key	Used by the VU to perform VU authentication towards tachograph cards and for signing downloaded data files	RSA	Generated ~~by VU or~~ VU manufacturer at the end of the manufacturing phase	~~See section 6.1.3.1.1 if done by VU~~. Otherwise, not in scope of this ST.	Made unavailable when the VU has reached end of life	non-volatile memory

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
SWUM.SK	SWUM private key	Used by the VU manufacturer for decrypting the transport key of the upgrade file	RSA	Generated by VU manufacturer at the end of the manufacturing phase	Not in scope of this ST	Made unavailable when the VU has reached end of life	non-volatile memory
SWUM.PK	SWUM public key	Used by the VU for encrypting the transport key of the upgrade file	RSA	Generated by VU manufacturer at the end of the manufacturing phase	Not in scope of this ST	Made unavailable when the VU has reached end of life	non-volatile memory
EUR.PK	Public key of ERCA	Used by VU to perform verification of MS certificates presented by (foreign) cards during mutual authentication. See also notes for EUR.KID in Table 10-3	RSA	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable	VU non-volatile memory
Card.PK (conditional, possibly multiple)	Card public key	Used by VU to perform card authentication (see also notes for Card.C contents in Table 10-3)	RSA	Generated by card or card manufacturer; obtained by VU in card certificate during mutual authentication	Out of scope for this ST	Not applicable	VU non-volatile memory
MS.PK (conditional, possibly multiple)	Public key of an MSCA other than the MSCA responsible for signing the VU certificate	Used by VU to perform verification of card certificates signed by this (foreign) MSCA. See also notes for MS.C contents in Table 10-3	RSA	Generated by (foreign) MSCA; obtained by VU in MS certificate presented by a card during mutual authentication	Out of scope for this ST	Not applicable	VU non-volatile memory

Table 10-1 First-generation asymmetric keys generated, used or stored by a VU

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
	Secure Messaging session key Agreed between VU and card during mutual authentication	Session key for data protection between VU and a card during a Secure Messa-ging session	TDES	Agreed between VU and card during mutual authenticcation	See section 6.1.3.1.1	Made unavailable when the Secure Messaging session is aborted	Not permanently stored

Table 10-2 First-generation symmetric keys generated, used or stored by a VU

Certificate Symbol	**Description**	**Purpose**	**Source**	**Stored in**	**Note**
VU.C	VU certificate for signing and Mutual Authentication	Used by cards or IDE to obtain and verify the VU.PK that they will subsequently use to perform VU authentica-tion or verification of sig-natures created by the VU	Created and signed by MSCA based on VU manufacturer input; inserted by manufactu-rer at the end of the manufacturing phase	VU general non-volatile memory	
MS.C	Certificate of MSCA responsible for signing VU certificate	Used by cards or IDE to obtain and verify the MS.PK that they will subsequently use to verify the VU.C	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
Card.C contents (conditional, possibly multiple)	CHR and other card certificate contents	*If a VU has verified a card certificate before, it may store the public key (see Table 10-1), the* CHR and possibly the validity period and other data in order to authenticate that card again in the future	Created and signed by MSCA based on card manufacturer input; inserted in card by card manufacturer; obtained and stored by VU during a previous successful card authentication.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store card certificate contents for future reference and has encountered cards in the past. The VU may store the

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
					contents of multiple Card.C.
MS.C contents (conditio-nal, possibly multiple	CHR and other MS certificate contents	If a VU has verified a MS certificate before, it may store the public key (see Table 10-1), the CHR and possibly the validity period and other data in order to verify card certifcates based on that MS certificate in the future	Created and signed by ERCA based on MSCA input, inserted in card by card manufacturer; obtained and stored by VU after successful verification during a previous mutual authentication process with a (foreign) card.	VU general non-volatile memory.	Presence in VU is conditional; only if VU is de-signed to store MSCA certificate contents for future reference and has encountered cards containing a foreign MS certificate in the past. The VU may store the contents of multiple MS.C
EUR.KID Key	Key Identifier for public key of ERCA	This identifier will be used by the VU to reference the European root public key during mutual authentication towards cards ~~*or EGFs*~~	Inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	

Table 10-3 First-generation certificates used or stored by a VU

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
VU_MA.SK	VU private key for Mutual Au-thentication	Used by the VU to perform VU authentication towards tachograph cards and ex-ternal GNSS facilities	ECC	Generated by ~~VU or~~ VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
VU_Sign.-SK	VU private key for signing	Used by the VU to sign downloaded data files	ECC	Generated by ~~VU or~~ VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	SecDEV PC in the production
SecDev.SK	SecDev private key	Used for verification of the Management Device certificate and for verification of the signature of the upgrade file	ECC	Generated by VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	SecDEV PC in the production
SecDev.PK	SecDev public key	Used for generating the corresponding signatures	ECC	Generated by VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory
MD.SK	Management device private key	used for generating the response for the challenge during management device authentication	ECC	Generated by VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory
MD.PK	Management device public key	used for verification of the response of the management device	ECC	Generated by VU manufacturer at the end of the manufacturing phase	not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory
EUR.PK (current)	The current public key of ERCA (at the time of issuing of VU)	Used by the VU for the verification of MSCA certificates issued under the cur-rent ERCA root certificate. See also notes for EUR.C (current con-tents in Table 10-6.	ECC	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable	VU non-volatile memory
EUR.PK (previous)	The previous public key of ERCA (at the ti-me of is-suing of VU)	Used by the VU to verify MSCA certificates issued under the previous	ECC	Generated by ERCA; inserted in VU by manufacturer at the end	Out of scope for this ST	Not applicable	VU non-volatile memory (conditional; only present if existing at

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
		ERCA root certificate. See also notes for EUR.C (previous) contents in Table 10-6		of the manufacturing phase			time of VU issuance)
EUR.Link.PK	The public key of ERCA following the public key that was current at the time of issuing of the VU	Used by the VU to verify MSCA certificates issued under the next ERCA root certificate. Note that EUR.Link.PK is the same as the next EUR.PK. See also Application note 6-37: And notes for EUR.Link.C contents in Table 10-6.	ECC	Generated by ERCA; inserted by manufacturer in a card ~~or EGF~~ issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by VU du-ring mutual authentication towards such card ~~or EGF~~	Out of scope for this ST	Not applicable	VU general nonvo-latile memory (con-ditional; only if the VU has success-fully authenticated a next-generation card ~~or EGF~~)
VU.SKEPH	VU ephemeral private key	Used by the VU to perform session key agreement with a tachograph card or external GNSS facility	ECC	Generated by VU during mutual authentication with a card or EGF	See section 6.1.2.1.1	Made unavailable at the latest when the Secure Messaging session is aborted	Not permanently stored
VU.PKEPH	VU ephemeral public key	Used by tacho-graph cards or external GNSS facilities to per-form session key agreement with the VU	ECC	Generated by VU during mutual authentication with a card or EGF, together with VU.SKeph	See section 6.1.2.1.1	Not applicable	Not permanently stored
Card_MA.PK	Card public key for Mutual Authentication	Used by VU to perform card authentication and session key agreement (See also notes for Card_MA.C	ECC	Generated by card or card manufac-turer; obtained by VU in card certi-ficate during mu-tual authentication	Out of scope for this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
		contents in Table 10-6)					
EGF_MA. PK	EGF public key for Mutual Authentication	Used by VU to perform EGF authentication and session key agreement (See also notes for Card_MA.C contents in Table 10-6)	ECC	Generated by EGF or EGF manufacturer; obtained by VU in EGF certificate during mutual authentication as part of the coupling process	Out of scope for this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)
MSCA _Card.PK	Public key of MSCA responsi-ble for signing card certificates	Used by VU to verify the certifi-cate of a card signed by this (foreign) MSCA. See also notes for MSCA-_Card.C contents in Table 10-6)	ECC	Generated by MSCA ; obtained by VU in MSCA-_Card certificate during mutual authentication	Out of scope for this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)
VUEGF.PK	Public key of MSCA responsi-ble for signing VU and EGF certificates	Used by VU to verify the certificate of an EGF signed by this (foreign) MSCA. See also notes for MSCA_VUEGF.C contents in Table 10-6.	ECC	Generated by MSCA ; obtained by VU in MSCA_VU-EGF certificate during coupling to an EGF	Out of scope for this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)

Table 10-4 Second-generation asymmetric keys generated, used or stored by a VU

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
Km-vu	Motion sensor master key – VU part	Allowing a VU to derive the Motion Sensor Master Key if a work-shop card is inserted into the VU	AES	Generated by ERCA; inserted by VU manufacturer at the end of the manufacturing phase.	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU non-volatile Memory

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
				Note: as explained in [*[2016_799_IC]*; Annex 1C, Appendix 11, section 12.2, a VU contains only one Km-vu.			
Km-wc	Motion sensor master key – workshop card part	Allowing a VU to derive the Motion Sensor Master Key if a work-shop card is inserted into the VU	AES	Generated by ERCA; retrieved by VU from inserted workshop card. Note: as explained in *[2016_799_IC]*; Annex 1C, Appendix 11, section 12.2, a workshop card may contain up to three keys Km-wc (of consecutive key generations). However, a VU will retrieve only one of these keys during the pairing process.	Out of scope for this ST	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2nd generation mo-tion sensor
Km	Motion sensor master key	Key used for au-thentication bet-ween the VU and a motion sensor during pairing	AES)	Derived by the VU from Km-vu and Kmwc	Not independently generated	Made unavailable at the latest by end of calibration phase	Not permanently stored; (only during pairing to a 2nd generation motion sensor)
Kp	Motion sensor pairing key	Key used for encrypting the motion sensor session key when sending it to the motion sensor during pairing	AES	Generated by the motion sensor manufacturer; stored in motion sensor (encrypted under Km) at the end of the manufac-turing phase; obtained and decrypted by VU during pairing	Out of scope for this ST	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2nd generation motion sensor

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
Kid	Motion sensor identification key	Key used for authentication between the VU and a motion sensor during pairing	AES	Derived by VU from Km and a constant vector	Not independently generated	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2nd generation motion sensor conditio-nal
KS	Motion sensor session key[37]	Session key for confidentiality between VU and motion sensor in operational phase	AES	Generated by VU during pairing to a motion sensor	See section 6.1.2.1.2	Made unavailable when the VU is paired to another (or the same) motion sensor.	VU non-volatile memory (conditional, only if the VU has been paired with a motion sensor)
Kmac	Secure Messaging session key for authenticity	Session key for authenticity between VU and a card or EGF during a Secure Messaging session	AES	Agreed between VU and card or EGF during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored
Kenc	Secure Messaging session key for confidentiality	Session key for confidentiality between VU and a card or EGF during a Secure Messaging session	AES	Agreed between VU and card or EGF during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored
$K_VU_{DSRC}_ENC$	VU-specific DSRC key for confidentiality	To ensure confi-dentiality of data sent over a remote communication channel between a VU and a remote early detection communication reader	AES	Derived by MSCA based on DSRC Master Key and VU serial number received from VU manufacturer; inserted by VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory

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

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
$K_VU_{DSRC}_MAC$	VU-specific DSRC key for authenticity	To ensure integrity and authenticity of data sent over a remote communication channel between a VU and a remote early detection communication reader	AES	Derived by MSCA based on DSRC Master Key and VU serial number received from VU manufacturer; inserted by VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory
TK	Transport key for upgrade file	To ensure confidentiality of the upgrade file	AES	Generated by the VU manufacturer	Out of scope of this ST	Made unavailable when the VU has reached end of life	Not permanently stored
CBC-MAC	CBC-MAC key	To protect the SWUM.SK, the SecDev.PK, the curve parameters of the underlying elliptic curve and the CBC-MAC key itself	AES	Generated by the VU manufacturer	Out of scope of this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory
Kvu	Individual device key	Key used to calculate MACs for the data integrity control of user data records	AES	Generated by the VU manufacturer	Out of scope of this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory

Table 10-5 Second-generation symmetric keys generated, used or stored by a VU

Certificate Symbol	Description	Purpose	Source	Stored in	Note
VU_MA.C	VU certificate for Mutual Authentication	Used by card or EGF to obtain and verify the VU_MA.PK they will subsequently use to perform VU authentication	Created and signed by MSCA based on VU manufacturer input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
VU_Sign.C	VU certificate for signing	Used by IDE or control card to obtain and verify the VU_Sign.PK they will subsequently use to verify the signature over a data file signed by the VU.	Created and signed by MSCA based on VU manufacturer input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
MSCA_VU-EGF.C	Certificate of MSCA responsible for signing the VU_MA and VU_Sign certificates	Used by a card, EGF or IDE to obtain and verify the MSCA_VUEGF.PK they will subsequently use to verify the VU_MA or VU_Sign certificate	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
EUR.Link.C	Link Certificate signed by previous EUR.SK (see Application Note below)	Used by a card, EGF or DIE issued under the previous ERCA root certificate to obtain and verify the current EUR.PK they will subsequently use to verify the MSCA_VU-EGF certificate	Created and signed by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile-memory	Presence in VU is conditional; only if a previous ERCA root certificate existed at the moment of VU manufacturing
EUR.C (current) Contents	CHR and other con-tents of current European root certificate	This CHR will be used by the VU to reference the current European root public key during verification of the VU certification chain by a card or EGF. The VU will also read this CHR from the MSCA certificate of a card or EGF issued under the current European root public key during verification of the card or EGF certificate chain. The CHR then serves to reference the VU's EUR.PK (current) key (see Table 10-4. The VU may store the validity period	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
		and other certificate data as well.			
EUR.C (previous) contents	CHR and other contents of previous European root certificate	The VU will read this CHR from the MSCA certificate of a card or EGF issued under the previous European root key during verification of the card or EGF certificate chain. The CHR serves to reference the VU's EUR.PK (previous) key (see Table 10-4. The VU may store the validity period and other certificate data as well.	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	Presence in VU is conditional; only if a previous ERCA root certificate existed at the moment of VU manufacturing
EUR.Link.C contents	CHR and other contents of next European root certificate	The VU will read this CHR from the MSCA certificate of a card or EGF issued under the next European root key during verification of the card or EGF certificate chain. The CHR serves to reference the VU's EUR.Link.PK key (see Table 10-4). The VU may store the validity period and other certificate data as well.	Generated by ERCA; inserted by manufacturer in a card or EGF issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by VU during mutual authentication towards such card or EGF	VU general non-volatile memory	Presence in VU is conditional; only if the VU has successfully authenticated a next generation card or EGF
Card_MA.C contents	CHR and other contents of Card certificate for Mutual Authentication	f a VU has verified a Card_MA certificate before, it may store the public key (see Table 10-4, the CHR and possibly the validity period and other data in order to authenticate that card again in the future	Created and signed by MSCA based on card manufacturer input; inserted in card by card manufacturer; obtained and stored by VU du-ring mutual authentication after successful verification.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store card certificate contents for future reference and has encountered cards in the

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
					past. The VU may store the contents of multiple Card_MA.C.
EGF_MA.C content	CHR and other contents of EGF certificate for Mutual Authentication	f a VU has verified an EGF_MA certificate before, it may store the public key (see Table 10-4), the CHR and possibly the validity period and other data in order to authenticate that EGF again in the future	Created and signed by MSCA_VU-EGF based on EGF manufacturer input, inserted in EGF by EGF manufacturer, obtained and stored by VU during mutual authentication after successful verification.	VU general non-volatile memory	Presence in VU is condi-tional; only if VU has been coupled to an EGF. The VU shall store the contents of only one EGF_MA.C at any given time
MSCA_Card.C contents	CHR and other contents of certificate of MSCA responsible for signing card certificates	If a VU has verified a MSCA certificate before, it may store the public key (see Table 10-4), the CHR and possibly the validity period and other data in order to verify card certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in card by card manufacturer obtained and stored by VU after successful verification during a previous mutual authentication process with a card.	VU general non-volatile memory	Presence in VU is condi-tional; only if VU is designed to store card certificate contents for future referen-ce and has encountered cards in the past. The VU may store the contents of multiple MSCA_Card. C, e.g. different MSCAs

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
					and/or generations
MSCA_VU-EGF.C Contents	CHR and other of certificate of MSCA responsible for signing VU and EGF certificates	If a VU has verified a MSCA certificate before, it may store the public key (see Table 10-4), the CHR and possibly the validity period and other data in order to verify EGF certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in EGF by EGF manufacturer; obtained and stored by VU after successful verification during a previous mutual authentication process with a card.	VU general non-volatile memory	Presence in VU is conditional; only if VU has been coupled to an EGF and is designed to store MSCA certificate contents for future reference

Table 10-6 Second-generation certificates used or stored by a VU

Application note 10-1 During its lifetime, the VU can be confronted with two different link certificates:

- *If at the time of issuance of the VU, there are cards or EGFs in the field that are issued under a previous EUR.C, then the VU shall be issued with both the previous EUR.C and a EUR.Link.C signed with the previous EUR.SK. The VU will need the first one to check the authenticity of the old cards. The VU will need the second one to prove its authenticity towards old cards.*

- *If, after the issuance of the VU, a new EUR.C is generated and cards or EGFs are issued under this new root certificate, then such a new card or EGF will present the VU with a EUR.Link.C signed by the current EUR.SK to prove its authenticity. The VU can check this certificate with its current EUR.PK. If correct, the VU shall store the EUR.Link.PK as a new trust point.*

ell as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for
ant of a patent, utility model or design.

11 Annex B – Operations for FCS_RNG.1

This annex provides further information on the use of FCS_RNG.1 and FCS_CKM.1 (1) in compliant security targets. The security target author should select one of these classes, as appropriate to the TOE, to complete the selection in FCS_CKM.1 (1), and should complete the operations in FCS_RNG.1 correspondingly. Further information on the application of these classes can be found in*[FC_RNG]*.

11.1 Class PTG.2

Functional security requirements of the class PTG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.2)

FCS_RNG.1.1 The TSF shall provide a [physical] random number generator that implements:

	(PTG.2.1)	*A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
	(PTG.2.2)	*If a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy].*
	(PTG.2.3)	*The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
	(PTG.2.4)	*The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
	(PTG.2.5)	*The online test procedure checks the quality of the raw random number sequence. It is triggered [selection: externally, at regular intervals, continuously, applied upon specified internal events]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

FCS_RNG.1.2 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet:

	(PTG.2.6)	*Test procedure A[38] [assignment: additional standard test suites] does not distinguish the internal random numbers from output sequences of an ideal RNG.*
	(PTG.2.7)	*The average Shannon entropy per internal random bit exceeds 0.997.*

11.2 Class PTG.3

Functional security requirements of the class PTG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.3)

FCS_RNG.1.1 The TSF shall provide a [hybrid physical] random number generator that implements:

	(PTG.3.1)	A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

[38] See *[FC_RNG]* Section 2.4.4.

	(PTG.3.2)	If a total failure of the entropy source occurs while the RNG is being operated, the RNG [*selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy*].
	(PTG.3.3)	The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.
	(PTG.3.4)	The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
	(PTG.3.5)	The online test procedure checks the raw random number sequence. It is triggered [*selection: externally, at regular intervals, continuously, upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
	(PTG.3.6)	The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

FCS_RNG.1.2 The TSF shall provide [*selection: bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet:

	(PTG.3.7)	Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A35 [*assignment: additional test suites*].
	(PTG.3.8)	The internal random numbers shall [*selection: use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work*]].

11.3 Class DRG.2

Functional security requirements of the class DRG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.2)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

	(DRG.2.1)	If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].
	(DRG.2.2)	The RNG provides forward secrecy.
	(DRG.2.3)	The RNG provides backward secrecy.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

	(DRG.2.4)	The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].
	(DRG.2.5)	Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A35 [*assignment: additional test suites*].

11.4 Class DRG.3

Functional security requirements of the class DRG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.3)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

(DRG.3.1)	If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].
(DRG.3.2)	The RNG provides forward secrecy.
(DRG.3.3)	The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.3.4)	The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].
(DRG.3.5)	Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A35 [*assignment: additional test suites*].

11.5 Class DRG.4

Functional security requirements of the class DRG.4 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.4)

FCS_RNG.1.1 The TSF shall provide a [hybrid deterministic] random number generator that implements:

(DRG.4.1)	The internal state of the RNG shall [*selection: use PTRNG of class PTG.2 as random source, have [assignment: work factor], require [assignment: guess work]*].
(DRG.4.2)	The RNG provides forward secrecy.
(DRG.4.3)	The RNG provides backward secrecy even if the current internal state is known.
(DRG.4.4)	The RNG provides enhanced forward secrecy [*selection: on demand, on condition [assignment: condition], after [assignment: time]*].
(DRG.4.5)	The internal state of the RNG is seeded by an [*selection: internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3, [other selection]*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.4.6)	The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].
(DRG.4.7)	Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A35 [*assignment: additional test suites*].

11.6 Class NTG.1

Functional security requirements of the class NTG.1 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class NTG.1)

FCS_RNG.1.1 The TSF shall provide a [non-physical true] random number generator that implements:

(NTG.1.1)	The RNG shall test the external input data provided by a non-physical entropy source in order to estimate the entropy and to detect non-tolerable statistical defects under the condition [*assignment: requirements for NPTRNG operation*].
(NTG.1.2)	The internal state of the RNG shall have at least [*assignment: Min-entropy*]. The RNG shall prevent any output of random numbers until the conditions for seeding are fulfilled.
(NTG.1.3)	The RNG provides backward secrecy even if the current internal state and the previously used data for reseeding, resp. for seed-update, are known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(NTG.1.4)	The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].
(NTG.1.5)	Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A [*assignment: additional test suites*].
[NTG.1.6)	The average Shannon entropy per internal random bit exceeds 0.997.

12 Annex C – List of used cryptographic methods

12.1 Annex C.1 - General

This annex lists the cryptographic methods that are provided by the Digital Tachograph DTCO 1381 Rel. 4.0e and 4.0ed at its external interfaces.

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

12.2 Annex C.2 – List of cryptographic mechanisms

No.	Purpose of case	Cryptographic mechanism	Implementing standard	key length	Application standard	Validity period
First-generation tachograph system						
1	Secure messaging authenticated mode DTCO 1381 <-> tachograph card TOE_SS.Identification_Authentication, TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	Retail-MAC	ANSI X9.19	112	[2016_799_11], sec. 5.3 *[ISO_9797_1], [2016_799_11]* sec. 2.2.3	No requirements in the EU regulation*[2016_799_IC]*
2	Secure messaging encrypted mode DTCO 1381 <-> tachograph card TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	Triple-DES in CBC mode	*[PUB_46_3]* *[NIST]*	112	*[2016_799_11]*, sec. 5.4 *[2016_799_11]*, sec. 2.2.3	No requirements in the EU regulation[2016_799_IC]
3	Mutual authentication and session key agreement DTCO 1381 <-> tachograph card TOE_SS.Identification_Authentication, TOE_SS.Cryptographic_support	RSA	[PKCS.1]	1024	*[2016_799_11]*, CSM_020 2016_799_11], sec. 2.2.1 (see Application note 2)	No requirements in the EU regulation[2016_799_IC
		SHA-1	[SHA1]	n/a	*[2016_799_11]*, CSM_020 *[2016_799_11]*, 2.2.2	No requirements in the EU regulation[2016_799_IC
4	digital signature for downloading to external media TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	SHA-1	[SHA1]	n/a	*[2016_799_11]*, CSM_034 *[2016_799_11]*, 2.2.2	No requirements in the EU regulation[2016_799_IC
		RSA	[PKCS.1] [2016_799_11], sec. 2.2.1 (see Application note 2)	1024	*[2016_799_11]*, CSM_020	No requirements in the EU regulation[2016_799_IC

No.	Purpose of case	Cryptographic mechanism	Implementing standard	key length	Application standard	Validity period
Second-generation tachograph system						
5	Secure messaging DTCO 1381 <-> Motion Sensor TOE_SS.Identification_Authentication, TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	AES in CBC mode	[PUB_197] *[NIST]*	128, 192 and 256	*[2016_799_11]*, CSM 42 *[16844-3]*, sec. 7.6	No requirements in the EU regulation[2016_799_IC
6	Secure messaging encryption DTCO 1381 <-> tachograph card TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	AES in CBC mode	*[PUB_197]* *[ISO_10116]*	128, 192 and 256	*[2016_799_11]*, CSM 40 CSM_186	No requirements in the EU regulation[2016_799_IC
7	Secure messaging authentication DTCO 1381 <-> tachograph card TOE_SS.Identification_Authentication, TOE_SS.Data_Exchange, TOE_SS.Cryptographic_support	AES in CMAC mode	*[SP 800-38B]*	128, 192 and 256	CSM_187	No requirements in the EU regulation[2016_799_IC
8	Certificate Chain Verification by DTCO 1381 depending on Domain parameters	ECDSA Signature Verification and Validation	NIST P-256, *PUB_186-4]*, *[RFC_5480]*, *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_48, CSM_160	No requirements in the EU regulation[2016_799_IC
			BrainpoolP256r1, *PUB_186-4]*, *[RFC_5639]* , *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_48, CSM_160	No requirements in the EU regulation[2016_799_IC
			NIST P-384, *PUB_186-4]*, *[RFC_5480]* , *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_48, CSM_160	No requirements in the EU regulation[2016_799_IC
			BrainpoolP384r1, *PUB_186-4]*, *[RFC_5639]* , *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_48, CSM_160	No requirements in the EU regulation[2016_799_IC
			BrainpoolP512r1, *PUB_186-4]*, *[RFC_5639]* , *[SHS]* (SHA-512)	512	*[2016_799_11]*, CSM_48, CSM_160	No requirements in the EU regulation[2016_799_IC

No.	Purpose of case	Cryptographic mechanism	Implementing standard	key length	Application standard	Validity period
			NIST P-521, *PUB_186-4]*, [*RFC_5480]*, , *[SHS]* (SHA-512)	521	*[2016_799_11]*, CSM_48, CSM_160	No require-ments in the EU regulation[2016_799_IC
9	Mutual authentication DTCO 1381 <-> tachograph card depending on Domain parameters TOE_SS.Identifi-cation_Authenti-cation, TOE_SS.Crypto-graphic_support	Ephemeral ECDH key pair generation depending on cards domain parameters	- According to the appendix A4.3 in [ANSI X9.62, the cofactor h is not supported; - According to section 6.1 (not 6.1.1) in [ISO_15946-1 see also FCS_CKM.1/EC_PSL in *[ST_Inf]* (underlying platform)	256 (NIST P-256)	*[2016_799_11]*, CSM_162	during mutual authentication for one (actual) session
				256 (BrainpoolP265r1)	*[2016_799_11]*, CSM_162	
				384 (NIST P-384)	*[2016_799_11]*, CSM_162	
				384 (BrainpoolP384r1)	*[2016_799_11]*, CSM_162	
				512 (BrainpoolP512r1)	*[2016_799_11]*, CSM_162	
				521 (NIST P-521)	*[2016_799_11]*, CSM_162	
		ECDSA signing algorithm depending on domain parameters of DTCO 1381	NIST P-256, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_173, CSM_174	No require-ments in the EU regulation[2016_799_IC
			BrainpoolP256r1, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_173, CSM_174	
			NIST P-384, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_173, CSM_174	
			BrainpoolP384r1, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_173, CSM_174	
			BrainpoolP512r1, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-512)	512	*[2016_799_11]*, CSM_173, CSM_174	
			NIST P-521, *PUB_186-4]*, *[TR_03111]*, *[SHS]* (SHA-512)	521	*[2016_799_11]*, CSM_173, CSM_174	
		ECKA (ECDH) key agreement algorithm depending on cards domain parameters	NIST P-256, *[TR_03111]*	256	*[2016_799_11]*, CSM_176	during mutual authentication for one (actual) session
			BrainpoolP256r1, *[TR_03111]*	256	*[2016_799_11]*, CSM_176	
			NIST P-384, *[TR_03111]*	384	*[2016_799_11]*, CSM_176	

No.	Purpose of case	Cryptographic mechanism	Implementing standard	key length	Application standard	Validity period
			BrainpoolP384r1, *[TR_03111]*	384	*[2016_799_11]*, CSM_176	
			BrainpoolP512r1, *[TR_03111]*	512	*[2016_799_11]*, CSM_176	
			NIST P-521, *[TR_03111]*	521	*[2016_799_11]*, CSM_176	
		Session key derivation depending on cards domain parameters	*[TR_03111]*, *[SHS]* (SHA-256)	-	*[2016_799_11]*, CSM_179	during mutual authentication for one (actual) session
			[TR_03111], *[SHS]* (SHA256)	-	*[2016_799_11]*, CSM_179	
			[TR_03111], *[SHS]* (SHA-384)	-	*[2016_799_11]*, CSM_179	
			[TR_03111], *[SHS]* (SHA-384)	-	*[2016_799_11]*, CSM_179	
			[TR_03111], *[SHS]* (SHA-512)	-	*[2016_799_11]*, CSM_179	
			[TR_03111], *[SHS]* (SHA-512)	-	*[2016_799_11]*, CSM_179	
10	Authenticity and confidentiality of data communicated from a vehicle unit to a control authority over a DSRC remote communication channel TOE_SS.Data-_Exchange, TOE_SS.Crypto-graphic_support	AES (in CBC Mode, CMAC mode)	[PUB_197] *[ISO_10116]* *[SP 800-38B]*	128, 192 and 256	*[2016_799_11]*, CSM_119, CSM_226	No require-ments in the EU regulation[2016_799_IC
11	Signature for downloading data TOE_SS.Integrity and authenticity of exported data, TOE_SS.Crypto-graphic_support	ECDSA signing algorithm depending on domain parameters of DTCO 1381	NIST P-256, *PUB_186-4]*, *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_233,	No require-ments in the EU regulation[2016_799_IC
			BrainpoolP256r1, *PUB_186-4]*, *[SHS]* (SHA-256)	256	*[2016_799_11]*, CSM_233,	
			NIST P-384, *PUB_186-4]*, *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_233,	
			BrainpoolP384r1, *PUB_186-4]*, *[SHS]* (SHA-384)	384	*[2016_799_11]*, CSM_233,	
			BrainpoolP512r1, *PUB_186-4]*, *[SHS]* (SHA-512)	512	*[2016_799_11]*, CSM_233,	
			NIST P-521, *PUB_186-4]*, *[SHS]* (SHA-512)	521	*[2016_799_11]*, CSM_233,	

No.	Purpose of case	Cryptographic mechanism	Implementing standard	key length	Application standard	Validity period
12	De-/encrypting the transport key of the upgrade file (SWUM) TOE_SS.Crypto-graphic_support	RSA	*[PKCS.1]* (see Application note 2)	2048	-	-
13	Digital signature of the upgrade file for the software upgrade TOE_SS.Crypto-graphic_support	ECDSA verification	brainpoolP256r1, [RFC_5639] *[PUB_186-4], [SHS],*	256	-	-
14	Confidentiality of the upgradefile	AES in CBC mode	[PUB_197]	128	AES key update after 20 AES block decryptions for enhancing DPA resistance	-
15	Protection of the SWUM.SK, the SecDev.PK, the curve parameters of the underlying elliptic curve and the CBC-MAC key itself TOE_SS.Crypto-graphic_support	AES in CBC mode	[PUB_197]	128	*[ISO_9797_1],* Using 32 MB of checksum	
16	Authentication of the management device TOE_SS.Identifi-cation_Authenti-cation, TOE_SS.Crypto-graphic_support	ECC	brainpoolP256r1, [RFC_5639]	256	-	-

Application note 2 For the method of PKCS'1 [PKCS.1] are used the corresponding methods of the secure controller SLI 97 underlying platform) [ST_Inf]:

Encryption:

According to section 5.1.1 RSAEP in PKCS v2.1 RFC3447, without 5.1.1.1.

Decryption (with or without CRT):

According to section 5.1.2 RSADP in PKCS v2.1 RFC3447

for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.1.2.2.b (ii)&(v), without 5.1.2.1. 5.1.2.2.a, only supported up to n < 22048.

Signature Generation (with or without CRT):

According to section 5.2.1 RSASP1 in PKCS v2.1 RFC3447

for u = 2, i.e., without any (r_i, d_i, t_i), i >2,

therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1.

5.2.1.2.a, only supported up to n < 22048.

Signature Verification:

According to section 5.2.2 RSAVP1 in PKCS v2.1 RFC3447, without 5.2.2.1.