SE5000-8 Security Target vehicle unit

Table of contents

1. DOCUMENT REVISION HISTORY

Rev: 1.0.0 **Date of issue: 2017-11-17** **Issued by: Jan Nordenholm**

Released.

Rev: 1.0.1 **Date of issue: 2017-11-24** **Issued by: Jan Nordenholm**

Added abstract heading in chapter 4 and enhanced the text. Clarified that SE5000 may not be connected to an external GNSS facility.

Added Appendix A and added list of cryptographic functions and their purpose to it.

Reviewed and approved.

Rev: 1.0.2 **Date of issue: 2017-12-13** **Issued by: Jan Nordenholm**

Removed erroneous reference to Annex 1B requirement RLB_201 in Table 16 - Suitability of the SFRs.

Clarified discrepancy between ref. [2] CC Part 2 and ref. [6] PP regarding dependencies for requirements FCS_CKM.2(1) and FCS_CKM.2(2).

Removed TSF.ROS.SDI, updated and moved contents to TSF.SDA.SDI.

Updated chapters 11.1.2 Relevant Platform TSFs and 11.1.3 Compatibility of Security Functional Requirements with references to RSA functionality and SE5000 TOE SFR FCS_COP.1(5:RSA).

Updated chapter 12 Appendix A – Cryptographic Mechanisms. Added use of TDES for internal integrity verification of TDES and AES cryptographic keys.

Reviewed and approved.

Rev: 1.0.3 **Date of issue: 2018-01-12** **Issued by: Jan Eriksson**

Added references 20-26.

Added **g)** to FCS_COP.1(1:AES)

The tables in chapter 12 Appendix A – Cryptographic Mechanisms have been reworked for clarity.

Rev: 1.0.4 **Date of issue: 2018-02-23** **Issued by: Jan Eriksson**

Crossed out FDP_ITT.1 as SE5000-8 has no physically separated parts.

Updates of Appendix A after comments from BSI.

Replaced numbered references with named references in section 2.

Updated number of retries for authentication in FIA_AFL.

Rework of chapter 10. New set of TSF to match better with design

Rev: 1.0.5 **Date of issue: 2018-03-28** **Issued by: Jan Eriksson**

Editorial changes

Crossed out FDP_ITT.1 in every reference to FDP_ITT.1.

SFR not by TSF is removed and requirements moved to other TSF:s

Rev: 02 **Date of issue: 2018-06-04** **Issued by: Jan Eriksson**

Editorial changes

Additional SFR:s covered by TSF.CRYPTO.

Added Motion Sensor identification data handling to TSF.CRYPTO.

Rev: 03 **Date of issue: 2018-06-26** **Issued by: Jan Eriksson**

Corrected references to Certification Report and Security Target Lite for Infineon Security Controller M7893 B11.

Rev: 04 **Date of issue: 2018-11-16** **Issued by: Mikael Måhl**

Corrected document properties and updated fields in chapter 4.1. These references broke when importing document into PLM system

Updated chapter 10.6 bullet 4 and chapter 11 regarding used libraries from Infineon.

Rev: 05 **Date of issue: 2019-02-19** **Issued by: Tomas Ellingsson**

Updated TOE Version number to B

Rev: 06 **Date of issue: 2019-11-22** **Issued by: Clas Jönsson**

Updated TOE Version number to C

Updated reference to Infineon M7893 Public Security Target

Updated reference to Certification report

Rev: 07 **Date of issue: 2020-05-04** **Issued by: Clas Jönsson**

Updated TOE Version number to E

Rev: 08 **Date of issue: 2020-05-27** **Issued by: Clas Jönsson**

Updated TOE Version number to F.

Removed document self-reference “ST Reference”.

Rev: 09 **Date of issue: 2020-09-01** **Issued by: Clas Jönsson**

Updated TOE Version number to G.

2. RELEVANT DOCUMENTS

The documents listed below are of essential value for the understanding of this document.

Document

Ref.	Title
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
[4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
[5]	Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, Annex 1 C
[6]	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 1C), Version 1.0, 9 May 2017, BSI-CC-PP-0094
[7]	A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011
[FIPS_180-4]	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
[PKCS_1]	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. October 1998.
[FIPS_46-3]	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 1999
[FIPS_197]	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
[FIPS_186-4]	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
[BSI_TR-03111]	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28
[NIST_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
[ISO_10116]	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an n- bit block cipher. Third edition, 2006-02-01
[16]	Public Security Target M7893 B11, Common Criteria CCv3.1 EAL6 augmented (EAL6+), Resistance to attackers with HIGH attack potential, Version 3.7, 2020-02-03
[ISO_16844-3]	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
[18]	ISO 16844-4:2015, Road Vehicles – Tachograph Systems – Part 4: CAN interface

[19] Certification Report BSI-DSZ-CC-0879-V4-2020 for Infineon Security Controller M7893 B11 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01, SCL v2.02.010 libraries and Toolbox v2.03.008 and with specific IC dedicated software (firmware)

[ANSI_X9_19] ANSI X9.19

[NIST_SP_800-67] National Institute of Standards and Technology (NIST), Special Publication 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revision 2

[ISO_9796-2] ISO/IEC 9796-2 Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997

[ISO_9797-1] ISO/IEC 9797-1 Information Technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-11.

[ISO_9798-3] ISO/IEC 9798-3 Information Technology – Security Techniques – Entity authentication. Second edition, 1998-10-15

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

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

3. TERMS AND ABBREVIATIONS

3.1. Terms

Terms used in this document and defined in reference [5] (Annex 1C) shall take the meaning defined in that document. Terms used in this document and not defined in reference [5] have the meaning specified in this chapter.

Term	Definition
Activity data	Activity data include user activities data, events and faults data and control activity data. Activity data are part of User Data.
Application note	Informative part of the ST containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE.
Approved Workshops	Fitters and workshops installing, calibrating and (optionally) repairing VU, and being approved to do so by an EU Member State, so that the assumption A.Approv_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 ST, 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 a 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.

Term	Definition
European Root Certification Authority (ERCA)	An organisation 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, 2749 21027 Ispra (VA), Italy
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.
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).

Term	Definition
Motion data	The data exchanged from the Motion Sensor to the VU, representative of speed and distance travelled.
Motion Sensor	A part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Motion sensor identification data	Data identifying the motion sensor: name of manufacturer, serial number, approval number, embedded security component identifier and operating system identifier. Motion sensor identification data are part of security data. These are stored in clear in the motion sensor's permanent memory.
Motion sensor pairing data	Motion sensor pairing data contains encrypted information about the date of pairing, VU type approval number, and VU serial number of the vehicle unit with which the motion sensor was paired.
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 control 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 1C, Appendix 13, [5]).
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.
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).

Term	Definition
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 [5] Annex 1C.
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.
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 [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. The CC gives the following generic definitions for user data: Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
Vehicle Unit	The tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of Regulation 2016/799. The vehicle unit includes 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.

3.2. Abbreviations

Abbreviation	
AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
CC	Common Criteria
CMAC	Cipher-based Message Authentication Code
DES	Data Encryption Standard
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level (a pre-defined package in CC)
ECC	Elliptic Curve Cryptography
EGF	External GNSS Facility
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
GNSS	Global Navigation Satellite System
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))
OSP	Organisational Security Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
REDCR	Remote Early Detection Communication Reader
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Standard
SRE	Stoneridge Electronics AB
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

Abbreviation	
VU	Vehicle Unit

4. ST INTRODUCTION (ASE_INT)

Abstract

This document contains the security target for the SRE product SE5000. The SE5000 is a second generation tachograph (smart tachograph) as required by reference [5] (Annex 1C) and reference [6] (CC PP, Digital Tachograph – Vehicle Unit (VU PP)). This document is created in accordance with the principles and requirements stated by *"Common Criteria for Information Technology Security Evaluation, version 3.1, revision 5"*.

Throughout this document whenever the term "Target of Evaluation" or the abbreviation TOE is used it is the SE5000 product which is referred to. I.e. the SRE product SE5000 is the target of evaluation

4.1. TOE reference

Developer name:	Stoneridge Electronics AB
TOE name:	SE5000-8
TOE Version number:	G

4.2. SE5000 overview

4.2.1. SE5000 definition and operational usage

The SE5000 addressed by this security target is a second generation vehicle unit (VU) in the sense of [5] (Annex 1C), intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores human user activities data in its internal data memory. It also records human user activities data in tachograph cards. The VU outputs data to a display, to a printer and to external devices.

The SE5000 is connected to a motion sensor from 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.

The SE5000 ~~*may be connected*~~ *connects* 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.*~~

The SE5000 hosts a GNSS receiver. This receiver connects to an internal embedded antenna but may also be connected to a suitable external antenna. The GNSS receiver allows for recording of the position of the vehicle at certain points during the daily working period and provides 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*~~ *The* GNSS receiver is *deployed* within the same physical boundary as the VU~~*.*~~ *and therefore* 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*~~ *The* VU is used with an external remote early detection communication facility~~*, the latter*~~ *which* 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.*~~

Human users identify themselves to the SE5000 by using tachograph cards.

The physical scope of the SE5000 is a device to be installed in a vehicle. The SE5000 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 manual(s).

The SE5000 must also support external connections or interfaces to the following:

a. a motion sensor (MS);
b. two smart cards;
c. a power supply;
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 SE5000 supports connection to GNSS ~~*either*~~ through equipment contained within the SE5000 enclosure~~.~~ ~~*or through connection to an external device supporting the connection.*~~

The SE5000 receives motion data from the motion sensor and activity data via the facilities for entry of user data. It stores all these user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces.

The SE5000 has four modes of operation:

- operational mode,
- control mode,
- calibration mode,
- company mode.

The SE5000 switches to the appropriate mode of operation according to the valid tachograph cards inserted into the card interface devices, as shown in Table 1 below. The modes of operation are significant in that certain operations can be carried out only whilst in certain modes of operation (see [5] Annex 1C, 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*
	Workshop card	*Calibration*	*Calibration*	*Operational*	*Calibration*	*Operational*
	Company card	*Company*	*Company*	*Operational*	*Operational*	*Company*

Table 1 - Mode of operation

4.2.2. SE5000 configuration

The SE5000 is depicted in Figure 1 below. It should be noted that although the printer mechanism is part of the TOE, the paper documents that it produces are not.

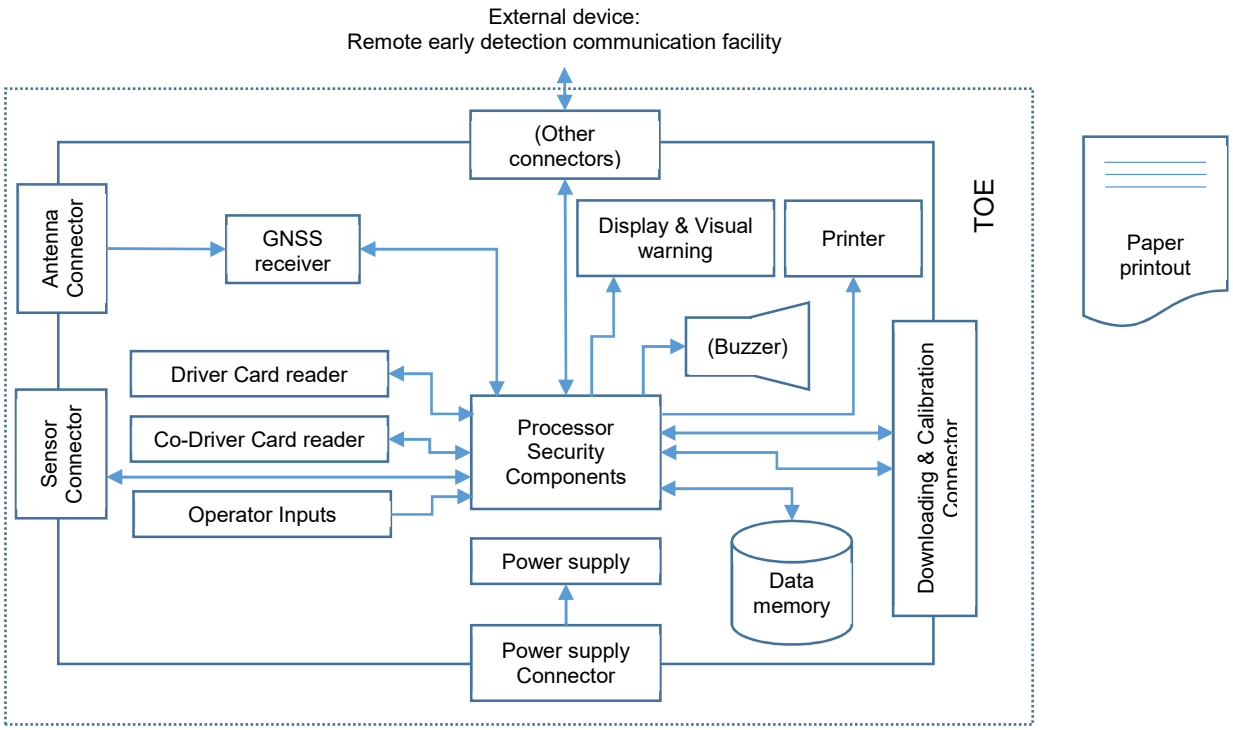

Figure 1 - SE5000, VU configuration

The SE5000 conforms to “Configuration 2” as defined by [6] (CC PP). I.e. the SE5000 has an internal GNSS receiver and interfaces an external remote early detection communication facility. This is visualized in Figure 1 above.

4.2.3. SE5000 major security features for operational use

The SE5000 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.

These main security features are provided by the security services described in the following sub-chapters.

4.2.3.1. Identification and authentication

The SE5000 identifies and authenticates tachograph cards and motion sensors. ~~*The SE5000 identifies and authenticates the external GNSS facility, if no internal GNSS receiver is present.*~~

4.2.3.2. Access control to functions and stored data

The SE5000 controls access to stored data and functions based on the mode of operation.

The SE5000 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 SE5000-specific decryption key can be derived.

4.2.3.3. Accountability of users

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

4.2.3.4. Audit of events and faults

The SE5000 detects and records a range of events and faults.

4.2.3.5. Residual information protection for secret data

Encryption keys and certificates are deleted from the SE5000 when no longer needed, such that the information can no longer be retrieved.

4.2.3.6. Integrity and authenticity of exported data

The integrity and authenticity of user data exported (downloaded) to an external storage medium, in accordance with [5] Annex 1C, Appendix 7, is assured through the use of digital signatures.

4.2.3.7. Stored data accuracy

Data stored in the SE5000 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)*~~).

4.2.3.8. Reliability of services

The SE5000 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.

4.2.3.9. 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 [5] Annex 1C, Appendix 11.

4.2.4. SE5000 TOE type

The SE5000 TOE type is a second-generation digital 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 life cycle of the SE5000 is depicted in Figure 2 below.

The TSP defined by this ST 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 SE5000 in its operational phase, are also considered. The SE5000 distinguishes between its calibration and operational phases by modes of operation as defined in [5]: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the SE5000.

By definition the transition from the manufacturing to the calibration phase occurs at delivery of the SE5000 from SRE to the customer.

[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 recognise the distinction when an external GNSS facility is present.

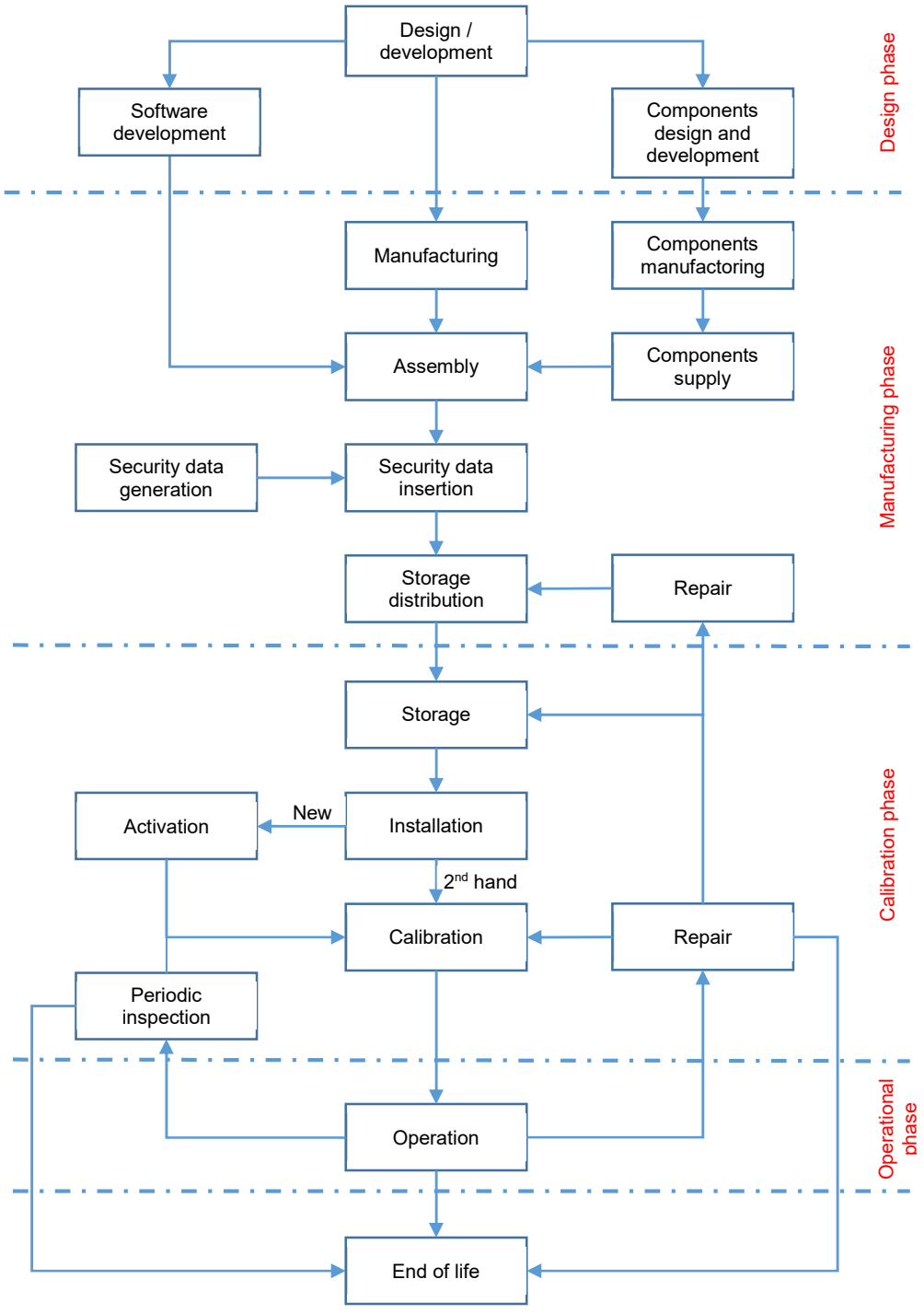

Figure 2 – SE5000 lifecycle

Note that “Repair” in the “Manufacturing phase” in Figure 2 above may include refurbishment, in which case depersonalisation may be required. “Repair” in the “Calibration phase” is strictly limited to changing removable parts of the printer which are external to the SE5000 sealed casing.

4.2.5. SE5000 connectivity

The vehicle unit's operational environment is depicted in Figure 3 below.

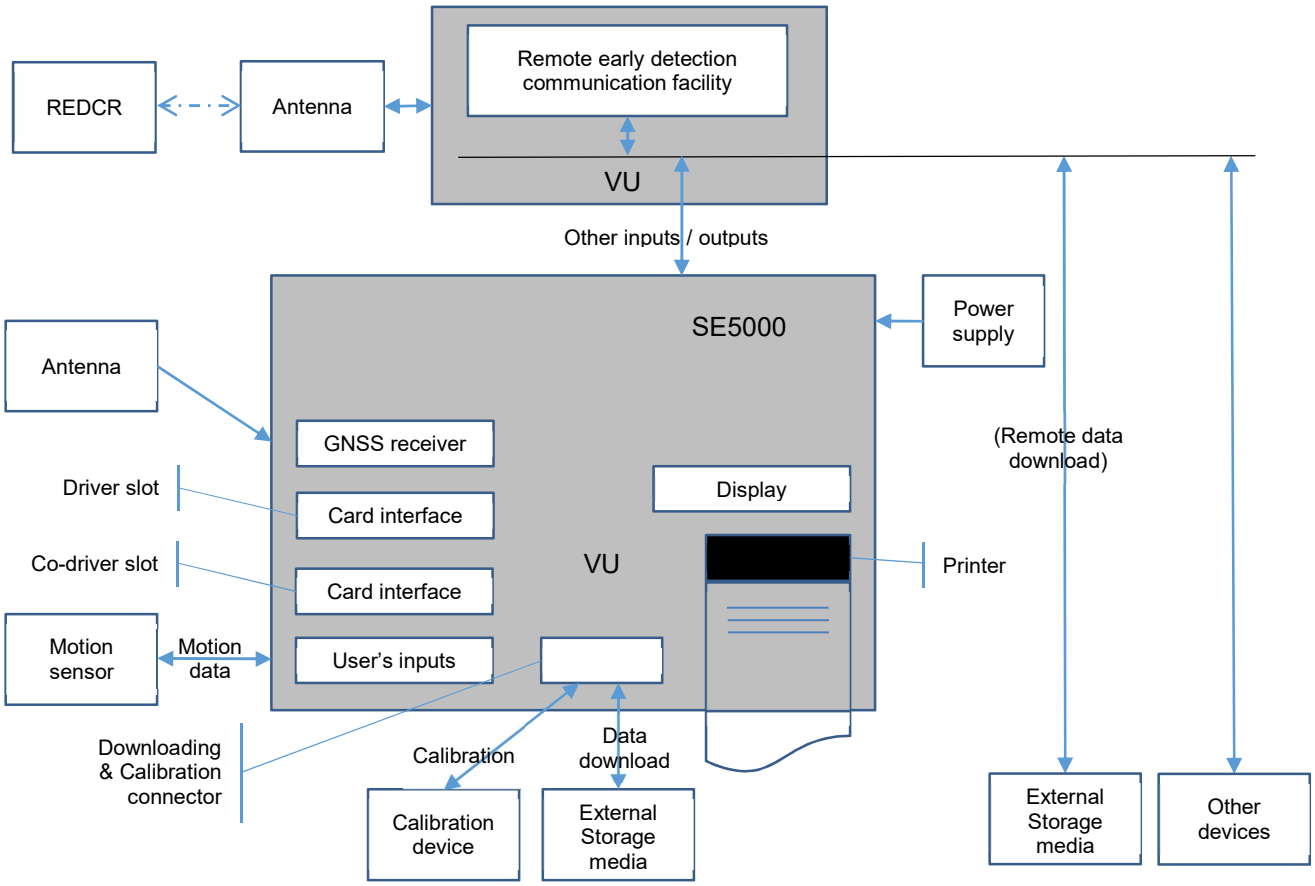

Figure 3 – SE5000 operational environment (external remote early detection communication facility / internal GNSS receiver)

The following SE5000-external components are

a) *mandatory* for a proper SE5000 operation:
   - power supply (e.g. from the vehicle in which the TOE is installed)
   - motion sensor
   - access to GNSS signals (provided within the SE5000 (see [5] Annex 1C, Appendix 12))
   - DSRC connection to a remote early detection communication reader (provided through an external remote early detection communication facility (see [5] Annex 1C, 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 SE5000 operation, but not required:
   - connection to the vehicle network (e.g. CAN-connection, see [18]).
   - connection to ITS systems (see [5] Annex 1C, Appendix 13).

Application note 1: The SE5000 will verify whether the connected motion sensor*, and* tachograph cards ~~*and external GNSS facility (if applicable)*~~ possess appropriate credentials showing that they belong to the digital tachograph system. A security certification according to [5], Annex 1C, Appendix 10 is a prerequisite for the type approval of a motion sensor and of tachograph cards.

Application note 2: Due to the necessity of ensuring a smooth transition between the 1st generation digital tachograph system and the 2nd generation specified in [5], Annex 1C, the SE5000 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 [5] Annex 1C 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 SE5000 with 2nd generation motion sensors.

The capability of the SE5000 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 SE5000. 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 SE5000 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 SE5000.

Full details of inter-generational operability requirements are in [5], Annex 1C, Appendix 15.

4.3. SE5000 description

The SE5000 is thoroughly described in chapter 4.2 SE5000 overview.

5. CONFORMANCE CLAIMS (ASE_CCL)

5.1. CC conformance claim

This security target claims conformance to ***Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5***:

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

as follows:

- Part 2 extended,
- Part 3 conformant.

5.2. PP conformance claim

This Security Target claims strict conformance to the following protection profile:

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 1C)
Version 1.0, 9 May 2017
BSI-CC-PP-0094

5.3. Package conformance claim

This Security Target claims conformance to EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

5.4. Conformance claim rationale

This Security Target claims conformance only to the one single PP stated in chapter 5.2 above. The information within this Security Target is, except from chapter 10 and chapter 11, without changes fetched from ref. [6]. Hence this ST is strictly conformant to the PP stated in chapter 5.2 above.

Note that the SFR's listed below is not applicable to the SE5000 tachograph as it conforms to "Configuration 2" as defined by [6] (CC PP), i.e. the SE5000 has an internal GNSS receiver:

- FIA_AFL.1(4:EGF)
- FIA_ATD.1(3:EGF)
- FIA_UAU.2(2:EGF)
- FTP_ITC.1(3:EGF)

Similarly the following SFR's has been altered by excluding parts concerning external GNSS facility:

- FDP_ACC.1.1(3:DAT)
- FDP_ACF.1.2(3:DAT)
- FDP_ITC.2.5
- FMT_SMR.1.1
- FCS_COP.1.1(1:AES)
- FCS_COP.1.1(3:ECC)

Also note that throughout the rest of this document texts regarding EGF has been excluded compared to the PP.

6. SECURITY PROBLEM DEFINITION (ASE_SPD)

6.1. Introduction

6.1.1. Assets

The primary assets to be protected by the SE5000 are:

No.	Asset	Definition
1.	user data (recorded by or stored in the SE5000)	Any data, other than security data (keys and certificates, see ref. [6], Annex A) recorded or stored by the VU, as required by of [5], Annex 1C, Section 3.12.
2.	user data transferred between the SE5000 and an external connected device [2]	All user data being transferred from or to the SE5000. A SE5000 communication partner can be: – a motion sensor, – a tachograph card – ~~*an external GNSS facility[3] (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 2 – 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 SE5000 in order to achieve a sufficient protection of the primary assets are:

No.	Asset	Definition
3.	SE5000 design and software code	Design information and source code (uncompiled or reverse engineered) for the SE5000 that could facilitate an attack.
4.	SE5000 hardware	Hardware used to implement and support SE5000 functions.
5.	SE5000 immanent secret security data	Secret security elements (i.e. symmetric and private keys) used by the SE5000 in order to enforce its security functionality (see ref. [6], Annex A).
6.	SE5000 immanent non-secret security data	Non-secret security elements (i.e. certificates and public keys) used by the SE5000 in order to enforce its security functionality (see ref. [6], 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.

[2] 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.
[3] Not applicable as the SE5000 uses an internal GNSS receiver.

Table 3 – Secondary assets

Application note 3: The workshop card requires authentication of a human user by requiring him to present 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 calibration phase (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 TSF and TSF-data in the sense of the CC.

6.1.2. 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 legitimate human user of the SE5000. The legitimate human users of the VU comprise drivers, controllers, workshops and companies. A human 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 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*~~[5]	~~*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.

[4] See ref. [6] Annex A for definitions of European level (EUR) keys and certificates.
[5] Not applicable as the SE5000 uses an internal GNSS receiver.

No.	Role	Definition
(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 for which 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 ST, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might assume any subject role recognised by the SE5000.

Table 4 – Subjects and external entities

The table above defines the subjects in the sense of the CC that can be recognised by the SE5000 independent of their nature (human or connected entity). Where a successful appropriate identification and authentication process takes place, the SE5000 creates – for each of those respective external entities – an ‘image’ inside, and ‘works’ then with this SE5000 internal image (also called subject in the CC). From this point of view, the SE5000 itself does not distinguish 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 SE5000.

6.2. Threats

This section describes the threats to be averted by the SE5000 independently or in collaboration with its IT environment. These threats arise from the assets protected by the SE5000 and the method of SE5000'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 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, data during output (print, display or download).

Table 5 –Threats addressed solely by the SE5000.

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 a miscalibrated SE5000 (through calibration data[6] modification, or through organisational weaknesses) to misrepresent driver activities (user data).
T.Clock	Attackers could try to modify the internal clock of the SE5000, and interfere with the correct operation of the SE5000.
T.Design	Attackers could try to gain illicit knowledge of the SE5000 design and software code, either from manufacturer's material (e.g. through theft or bribery) or from reverse engineering, interfere with the correct operation of the SE5000.
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 card ~~or external GNSS facility~~) to the SE5000 to misrepresent driver activities (user data at rest or being transferred between the SE5000 and an external connected device).
T.Hardware	Attackers could try to modify SE5000 hardware, and interfere with the correct operation of the SE5000.
T.Identification	Human users could try to use several identities or no identity to misrepresent driver activities (user data).
T.Motion_Sensor	Attackers could try to modify motion data (addition, modification, deletion, replay of signal), part of user data, to misrepresent driver activities (user data).
~~***T.Location_Data***~~[7]	~~*Attackers could try to modify location data when transmitted by an external GNSS facility (addition, modification, deletion, replay of signal) to misrepresent driver activities (user data).*~~

[6] Part of user data. For definition of calibration data see [5] Annex 1C, Chapter 3.12.10.
[7] T.Location_Data is not applicable as the SE5000 uses an internal GNSS receiver.

Label	Threat
T.Power_Supply	Attackers could try to interfere with the recording or transmission of user data by modifying (cutting, reducing, increasing) the SE5000'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 SE5000 software in order to interfere with the correct operation of the SE5000.
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 6 – Threats addressed by the SE5000 and its operational environment

6.3. Assumptions

This section describes the assumptions that are made about the operational environment in order to be able to provide the security functionality. If the SE5000 is placed in an operational environment that does not uphold these assumptions it may be unable to operate in a secure manner.

The assumptions are provided in the following table.

Short name	Assumption
A.Activation	Vehicle manufacturers and fitters or workshops activate the SE5000 after its installation at the latest before the vehicle is used in scope of Regulation (EC) N° 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 SE5000 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 [5] Annex 1C, Chapter 3).
A.Controls	Law enforcement controls of the SE5000 will be performed regularly and randomly, and must include security audits (as well as visual inspection of the SE5000).
A.Driver_Card_Unique	A driver possesses, at one time, one valid driver card only.
A.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.
A.Inspections	Recording equipment will be periodically inspected and calibrated.
A.Compliant_Drivers	Drivers use their cards in accordance with provided guidance, and properly select their activity for those that are manually selected.
A.Type_Approved_Dev	The SE5000 will only be operated together with a motion sensor ~~*and an external GNSS facility[8] (if applicable)*~~ that are type approved according to [5] Annex 1C.[9]
A.Bluetooth	Bluetooth pairing and Bluetooth connection of the ITS interface are sufficiently secure not to compromise the objectives of this ST.

Table 7 – Assumptions

6.4. Organisational security policies

This section shows the organisational security policies that are to be enforced by the SE5000, its operational environment, or a combination of the two.

The organisational security policies are provided in the following table.

Short name	Organisational Security Policy
P.Crypto	The cryptographic algorithms described in [5] Annex I C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

Table 8 – Organisational security policy

[8] Not applicable as the SE5000 uses an internal GNSS receiver.
[9] Type approval requirements include Common Criteria certification against the relevant digital tachograph protection profile.

7. SECURITY OBJECTIVES (ASE_OBJ)

This section identifies the security objectives for the SE5000 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.

7.1. Security objectives for the SE5000

The SE5000 security objectives address the protection to be provided by the SE5000, independent of the SE5000 environment, and are listed in the table below.

Short name	Security objective for the SE5000
O.Access	The SE5000 must control user access to functions and data on the basis of user type and identity.
O.Authentication	The SE5000 must authenticate users and connected entities (when a trusted path or trusted channel[10] needs to be established towards these users).
O.Accountability	The SE5000 must collect accurate accountability data.
O.Audit	The SE5000 must audit attempts to undermine system security and trace them to associated users.
O.Integrity	The SE5000 must maintain stored data integrity.
O.Output	The SE5000 must ensure that data output accurately reflects data measured or stored.
O.Processing	The SE5000 must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The SE5000 must provide a reliable service.
O.Secure_Exchange	The SE5000 must secure data exchanges with the motion sensor, with tachograph cards~~, with the external GNSS facility[11] (if applicable)~~ and with the remote early detection communication reader.
O.Software_Update	Where updates to SE5000 software are possible, the SE5000 must check their authenticity and integrity before installing them.[12]

Table 9 – Security objectives for the SE5000

[10] Trusted channel is referred to in [5], Annex 1C, Appendix 11 as a secure messaging session.
[11] Not applicable as the SE5000 uses an internal GNSS receiver.
[12] Note! Software installation and/or update is limited to the “Manufacturing phase” of the SE5000 lifecycle.

7.2. Security objectives for the operational environment

The security objectives for the operational environment address the protection that must be provided by the SE5000 environment, independent of the SE5000 itself, and are listed in the table below.

Specific phase	Short name	Security objective for the SE5000
Design phase	**OE.Development**	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security
Manufacturing phase	**OE.Manufacturing**	VU manufacturers must 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.Data_Generation	Security data generation algorithms must be accessible to authorised and trusted persons only.
	OE.Data_Transport	Security data must be generated, transported, and inserted into the SE5000, in such a way to preserve its appropriate confidentiality and integrity
	OE.Delivery	VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the SE5000 is done in a manner which maintains IT security.
	OE.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in the SE5000.
	OE.Data_Strong	Security data inserted into the SE5000 for compatibility with 2nd generation tachograph cards, motion sensors~~, EGFs[13] (if present)~~ and remote early detection communication readers must be as cryptographically strong as required by [5] Annex 1C, Appendix 11 Part B. Security data inserted into the SE5000 for compatibility with 1st generation tachograph cards and motion sensors must be as cryptographically strong as required by [5] Annex 1C, 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 must be disabled or removed before the end of the manufacturing process.
Calibration phase	**OE.Activation**	Vehicle manufacturers and fitters or workshops must activate the SE5000 after its installation before the vehicle is used in scope of Regulation (EC) N° 561/2006.
	OE.Approv_Workshops	Installation, calibration and repair of recording equipment must be carried out by trusted and approved fitters or workshops.
	OE.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.
Operational phase	**OE.Card_Availability**	Tachograph cards must be available to SE5000 human users and delivered by Member State Authorities to authorised persons only.

[13] Not applicable as the SE5000 uses an internal GNSS receiver.

Specific phase	Short name	Security objective for the SE5000
	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 must be performed regularly and randomly, and must include security audits.
	OE.Driver_Card_Unique	A driver must possess, at one time, one valid driver card only.
	OE.Compliant_Drivers	Drivers must use their cards in accordance with provided guidance, and must properly select their activity for those that are manually selected.
	OE.Regular_Inspection	Recording equipment must be periodically inspected and calibrated.
	OE.Type_Approval_MS[14]	The Motion Sensor of the recording equipment connected to the SE5000 must be type approved according to [5] Annex 1C.
	~~**OE.Type_Approval_EGF**~~	~~*The external GNSS facility connected to the TOE (if applicable) must be type approved according to [5] Annex 1C*~~[15]~~.~~
	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 SE5000 must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric and private cryptographic keys has to be safeguarded.

Table 10 – Security objectives for the operational environment

Please note that the design and the manufacturing phases are not the intended usage environments for the SE5000 (see chapter 4.2.4). The security objectives for these phases being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test_Points, OE.Delivery) are subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing phases do not address any potential *SE5000 user* and, therefore, cannot be reflected in the documents of the assurance class AGD. The remaining security objectives for the manufacturing phase (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 SE5000.

[14] Identification and authentication of the motion sensor depends on the motion sensor having implemented the required mechanisms to support it.
[15] OE.Type_Approval_EGF may be regarded as trivially met when an internal GNSS facility is used.

7.3. Security objectives rationale

7.3.1. Tracing between security objectives and the security problem definition

Table 11 below shows how the identified security objectives (ASE_OBJ) trace back to the threats, OSP's and assumptions described in the security problem definition (ASE_SPD).

	Threats																		Assumptions												OSPs
	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	T.Tests	A.Activation	A.Approv_Workshops	A.Card_Availability	A.Card_Traceability	A.Cert_Infrastructure	A.Controls	A.Driver_Card_Unique	A.Faithful_Calibration	A.Inspections	A.Compliant_Drivers	A.Type_Approved_Dev	A.Bluetooth	P.Crypto
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_Exchange	X	X							X			X	~~X~~		X																X
O.Software_Update																X															
OE.Development							X									X															
OE.Manufacturing							X											X													
OE.Data_Generation															X								X								
OE.Data_Transport															X								X								X
OE.Delivery															X								X								
OE.Software_Upgrade															X		X														
OE.Data_Strong															X								X								X
OE.Test_Points																		X													
OE.Activation				X															X												
OE.Approv_Workshops					X	X														X						X					
OE.Faithful_Calibration					X	X																				X					
OE.Card_Availability											X										X										
OE.Card_Traceability											X											X									
OE.Controls					X	X		X	X	X				X	X	X	X							X								
OE.Driver_Card_Unique											X														X							
OE.Compliant_Drivers																												X			
OE.Regular_Inspection					X				X	X		X		X		X											X				
OE.Type_Approval_MS									X																				X		
~~OE.Type_Approval_EGF~~									~~X~~																				~~X~~		
OE.Bluetooth																														X	
OE.EOL							X								X																

Table 11 - Tracing between security objectives and the security problem definition

7.3.2. Justification

A detailed justification required for *suitability* of the security objectives to cope with the security problem definition is given in the following sub-chapters.

7.3.2.1. T.Card_Data_Exchange

T.Card_Data_Exchange is addressed by O.Secured_Data_Exchange. O.Audit contributes to address the threat by recording events related to card data exchange integrity or authenticity errors. O.Reliability, O.Processing also contribute by providing for accurate and reliable processing.

7.3.2.2. T.Remote_Detect_Data

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.

7.3.2.3. T.Output_Data

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

7.3.2.4. T.Access

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 SE5000 after its installation ensures access of the user to functions.

7.3.2.5. T.Calibration_Parameters

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.Approv_Workshops, OE.Faithful_Calibration). Periodic inspections and calibration of the equipment contribute to addressing the threat (O.E Regular_Inspection). Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the VU, which helps addressing the threat.

7.3.2.6. T.Clock

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.Approv_Workshops). Periodic 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 in addressing the threat.

7.3.2.7. T.Design

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 SE5000 design through secure disposal of equipment at end of life.

7.3.2.8. T.Environment

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 in addressing the threat.

7.3.2.9. T.Fake_Devices

T.Fake_Devices is addressed by O.Access, O.Authentication, O.Audit, O.Processing, O.Reliability and O.Secured_Exchange. OE.Controls, OE.Regular_Inspections, ~~and~~ OE_Type_Approval_MS ~~and OE.Type_Approval_EGF~~ help addressing the threat through visual inspection of the whole installation and visible type approval seals.

7.3.2.10. T.Hardware

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

7.3.2.11. T.Identification

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_Unique, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.

7.3.2.12. T.Motion_Sensor

T.Motion_Sensor is addressed by O.Authentication, O.Reliability, O.Secured_Exchange and OE.Regular_Inspection. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

~~7.3.2.13. T.Location_Data~~[16]

~~T.Location_Data is addressed by O.Authentication, which requires that the source of location data is authenticated; and by O.Secure_Exchange, which requires that a secure channel is used. O.Audit also contributes through audit of attempts to undermine system security.~~

7.3.2.14. T.Power_Supply

T.Power_Supply is mainly addressed by O.Reliability to ensure appropriate behaviour of the VU against the attack. O.Audit contributes to addressing 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 to address the threat. OE.Regular_Inspection helps in addressing the threat through installations, calibrations, checks, inspections and repairs carried out by trusted fitters and workshops.

7.3.2.15. T.Security_Data

T.Security_Data is addressed by the 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_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.

7.3.2.16. T.Software

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 addressing the threat by recording events related to 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_Inspection (checking for the audit records related) also contribute.

[16] Not applicable as the SE5000 uses an internal GNSS receiver.

7.3.2.17. T.Stored_Data

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. 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 SE5000 to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU helping to address the threat.

7.3.2.18. T.Tests

T.Tests is addressed by O.Reliability, OE.Manufacturing and OE.Test_Points. If the SE5000 provides a reliable service as required by O.Reliability, and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the SE5000 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 to attack the SE5000 during the operational phase. Hence, the related threat will be mitigated.

7.3.2.19. A.Activation

A.Activation is upheld by OE.Activation.

7.3.2.20. A.Approv_Workshops

A.Approv_Workshops is upheld by OE.Approv_Workshops.

7.3.2.21. A.Card_Availability

A.Card_Availability is upheld by OE.Card_Availability.

7.3.2.22. A.Card_Traceability

A.Card_Traceability is upheld by OE.Card_Traceability.

7.3.2.23. A.Cert_infrastructure

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

7.3.2.24. A.Controls

A.Controls is upheld by OE.Controls.

7.3.2.25. A.Driver_Card_Unique

A.Driver_Card_Unique is upheld by OE.Driver_Card_Unique.

7.3.2.26. A.Faithful_Calibration

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

7.3.2.27. A.Compliant_Drivers

A.Compliant_Drivers is upheld by OE.Compliant_Drivers.

7.3.2.28. A.Inspections

A.Inspections is upheld by OE.Regular_Inspection.

7.3.2.29. A.Type_Approved_Dev

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

7.3.2.30. A.Bluetooth

A.Bluetooth is is upheld by OE. Bluetooth.

7.3.2.31. P.Crypto

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.

7.4. Security objectives conclusion

Based on the security objectives and the security objectives rationale, the following conclusion can be drawn: if all security objectives are achieved then the security problem as defined in Security problem definition (ASE_SPD) is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

8. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

This security target uses a component that is defined as an extension to CC Part 2 (ref. [2]).

The extended component is FCS_RNG.1 Random number generation. This component is fully defined and justified in [7] Section 3. Ref. [6], the PP, defines a restricted set of ways in which the extended component can be used in a security target. These are set out in [6] Annex B, and further information is provided in [7]. Within this ST the SFR FCS_RNG.1 is fully stated in chapter 9.1.2.1.7.

9. SE5000 SECURITY REQUIREMENTS (ASE_REQ)

This section defines the detailed security requirements that shall be satisfied by the SE5000. The statement of **SE5000 security requirements** defines the *functional* and *assurance* security requirements that the SE5000 needs to satisfy in order to meet the security objectives for the SE5000.

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

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

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted by 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 made by the ST author appear in square brackets and are [*double 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 that have been made by the PP author are denoted by 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*. Assignments made by the ST author appear in square brackets and are [*double underlined and italicised*].

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

Entire requirements and parts of requirements not applicable to the SE5000 are deleted from this security target by the ST author. These deletions appear as ~~*double underlined and italicised with a strikethrough.*~~

9.1. Security functional requirements for the SE5000

This section is subdivided to show security functional requirements that relate to the SE5000 itself, and those that relate to external communications. Section 9.1.1 addresses requirements for the VU. Section 9.1.2 addresses the communication requirements for 2nd generation tachograph cards to be used with the SE5000. Section 9.1.3 addresses the communication requirements for 1st generation tachograph cards to be used with the SE5000.

9.1.1. Security functional requirements for the VU

9.1.1.1. Class FAU Security Audit

9.1.1.1.1. FAU_GEN.1 Security 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 [5] Annex 1C, section 3.9].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of event, type of event, subject identity, and the outcome (success or failure) of the event[17], and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the data to be recorded for each event type listed in [5] Annex 1C, sections 3.12.8 and 3.12.9].

9.1.1.1.2. 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 [5] Annex 1C paragraph 13] with the capability to read [the information required to be recorded by FAU_GEN.1 and imported motion sensor audit data] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

9.1.1.1.3. 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*[18]] unauthorized modifications to the stored audit records in the audit trail.

[17] The outcome of the event need only be recorded where such a concept is relevant to the event.
[18] Audit records are “events/faults” defined in [5] 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”.

9.1.1.1.4. FAU_STG.4 Prevention of audit data loss

Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [overwrite the oldest stored audit records **when not in contradiction with the storage rules for events data and faults data stated in [5] Annex 1C chapters 3.12.8 and 3.12.9**] and [*fully comply with the storage rules for events data and faults data stated in [5] Annex 1C chapters 3.12.8 and 3.12.9*] if the audit trail is full.

Application note 4: As a minimum the data memory shall be able to hold events data as required by [5] Annex 1C, section 3.12.8 without overwriting.

Application note 5: 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 SE5000.

9.1.1.2. Class FCO Communication

9.1.1.2.1. 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[19]] **in accordance with [5], Annex 1C, 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 [5], Annex 1C, Appendix 11, section 14 and 13].

[19] The originator is the vehicle unit.

9.1.1.3. Class FDP User data protection

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

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1:FIL) The TSF shall enforce the [File Structure SFP[20]] on [

Objects: *- the application file structure*
- the data file structure

Subjects: *- all users*

Operations: *- modify*
- delete

].

Application note 6: 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.

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

Hierarchical to: -

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: [

Application file structure attributes: *- any*
Data file structure attributes: *- any*
User attributes: *- any*

].

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 authorize 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].

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

9.1.1.3.3. FDP_ACC.1 Subset access control (2:FUN)

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2:FUN) The TSF shall enforce the [Function SFP[21]] on [

Objects:
- *mode of operation*
- *calibration data*
- *time*
- *driver activity*
- *location data*
- *tachograph cards*

Subjects:
- *all users*

Operations:
- *change mode of operation*
- *store calibration data*
- *set time*
- *manual entry of driver activity*
- *manual entry of location data*
- *release of tachograph cards*

].

Application note 7: 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.

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

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

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 the [Function SFP] to objects based on the following: [

User attributes:	*- role*	*(Driver, Controller, Workshop, Company, Unknown)*
Tachograph card attributes:	*- generation*	*(1st , 2nd)*

].

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 [5], Annex 1C, 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 authorize 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].

9.1.1.3.5. FDP_ACC.1 Subset access control (3:DAT)

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(3:DAT) The TSF shall enforce the [Data SFP[22]] on [

Objects:
- *VU identification data*
- *MS identification data*
- *MS pairing data*
- *calibration data*
- *calibration activities data*
- *time adjustments activities data (outside calibration)*
- *keys and certificates*
- *manufacture data*
- *MS audit records*

Subjects:
- *all users*

Operations:
- *protection of VU identification data*
- *record and store MS identification data*
- *record and store MS pairing data*
- *record and store calibration data*
- *record and store calibration activities data*
- *record and store time adjustments activities data (outside calibration)*
- *store keys and certificates*
- *store manufacture data*
- *record and store MS audit records*

].

Application note 8: 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[23].

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

[23] 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.

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

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: [

Objects attributes: *- any*
Subjects attributes: *- any*].

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, and prevent unauthorised modification of the serial number, approval number pairing date related to the 20 most recent pairings of motion sensors[24];
- ~~*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)*~~;
- 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);
- 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 **ref. [6]** 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~~ **detect**[25] unauthorised modification of audit records generated by the motion sensor;
- ~~*the vehicle unit is able to record and store in its data memory, and prevent unauthorised modification of audit records generated by the external GNSS facility (if applicable)*~~].

FDP_ACF.1.3(3:DAT) The TSF shall explicitly authorize 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].

[24] This shall be done as a minimum on pairing.
[25] See 9.1.1.1.3 FAU_STG.1 Protected audit trail storage.

9.1.1.3.7. FDP_ACC.1 Subset access control (4:UDE)

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(4:UDE) The TSF shall enforce the [User Data Export SFP[26]] on [

Objects:
- *tachograph cards*
- *user data*
- *company locks*
- *ITS interface (optional)*
- *pairing PIN (optional)*

Subjects:
- *all users*

Operations:
- *user data export*

].

Application note 9: 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.

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

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

Hierarchical to: -

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

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

Tachograph card attributes: *- type (Driver, Controller, Workshop, Company)*
- holder info (name, number)

User attributes: *- role (Driver, Controller, Workshop, Company)*
- identification (name, number)
- driver consent to data export

].

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 and control cards with all necessary data relevant to the period while the card is inserted and relevant to the cardholder[27];
- 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 can read remote early detection communication facility data].

FDP_ACF.1.3(4:UDE) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

- If the TOE is equipped with an ITS interface, as specified in [5] Annex 1C, 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[28] or card number[29] 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].

[27] See [5] Annex 1C, Chapters 3.14.1 and 3.14.2.
[28] Personal identification (surname and first name) shall be blanked.
[29] Card number shall be partially blanked (every odd character).

9.1.1.3.9. FDP_ACC.1 Subset access control (5:IS)

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(5:IS) The TSF shall enforce the [Input Sources SFP[30]] on [

Objects:
- *vehicle motion data*
- *RTC data*
- *recording equipment calibration parameters data*
- *tachograph cards data*
- *human user's inputs data*

Subjects:
- *all users*

Operations:
- *data import*

].

Application note 10: 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 human user inputs. It also covers prevention of external inputs being accepted as executable code.

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

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 the [Input Sources SFP] to objects based on the following: [

Vehicle motion data attributes:	*- identity and authenticity*
RTC data attributes:	*- none*
Recording equipment calibration parameters data attributes:	*- none*
Tachograph cards data attributes:	*- identity and authenticity*
User's inputs data attributes:	*- none*

].

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 human user's inputs may only be processed from the right input sources].

FDP_ACF.1.3(5:IS) The TSF shall explicitly authorize 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].

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

9.1.1.3.11. 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 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].

9.1.1.3.12. 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].

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

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FPT_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 of the TOE: [

- the vehicle unit shall ensure that data related to vehicle motion~~,~~ *and* 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*~~[31]].

Application note 11: If software can be updated only in the manufacturing phase then the requirement for verified software updates is not applicable.

~~9.1.1.3.14. FDP_ITT.1 Basic internal transfer protection~~[32]

~~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.~~

[31] Not applicable as software installation and/or update is limited to the “Manufacturing phase” of the SE5000 lifecycle.
[32] FDP_ITT.1 is not applicable as the SE5000-8 TOE has no physically separated parts.

9.1.1.3.15. 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 **ref. [6]** Table 18, Table 19, Table 21 and Table 22;
- 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);

[*There are no further objects to list.*]].

Application note 12: 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 **ref. [6]** Annex A – Key & Certificate Tables that are marked as having to be made unavailable at decommissioning the TOE is a matter of the related organisational policy.

Application note 13: The functional family FDP_RIP possesses 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.

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

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 [assignment: user data attributes]~~.

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

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

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, [*and no other monitoring for motion data integrity errors needed*]] on all objects, based on the following attributes [*vehicle speed*].

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

9.1.1.4. Class FIA Identification and authentication

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

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(1:TCL) The TSF shall detect when [5] **consecutive** 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 [**met or** 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 14: 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.

9.1.1.4.2. FIA_AFL.1 Authentication failure handling (2:TCR)

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(2:TCR) The TSF shall detect when [1] **consecutive** 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 [**met or** surpassed], the TSF shall [warn the remotely connected company].

Application note 15: FIA_AFL.1(2:TCR) is only applicable if the TOE provides a remote download facility (see [5] Annex 1C paragraph 193).

9.1.1.4.3. FIA_AFL.1 Authentication failure handling (3:MS)

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(3:MS) The TSF shall detect when [*3*] 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 [**met or** 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 16: 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*~~.

~~*9.1.1.4.4. FIA_AFL.1 Authentication failure handling (4:EGF)*~~[33]

~~*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].*~~

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

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 17: For further details see [5] Annex 1C~~, *section 3.12.13 and*~~ Appendix 1 2.73 and 2.74.

9.1.1.4.6. 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 18: This requirement relates to the motion sensor~~,~~ *and* tachograph cards~~*, and, if applicable, the external GNSS facility*~~.

[33] FIA_AFL.1(4:EGF) is not applicable as the SE5000 uses an internal GNSS receiver.

9.1.1.4.7. FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: -

Dependencies: -

FIA_UAU.5.1 The TSF shall provide [authentication using the methods described in [5], Annex 1C, Appendix 11, Section 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 19: FIA_UAU.5 applies only to authentication using a workshop card, where a PIN is required.

9.1.1.4.8. 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 [5] Annex 1C, Appendix 11
[*at recovery from reset with other cause than power supply interruption,*
when any of the session keys are about to expire,
at least once per day]

].

9.1.1.4.9. 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.

9.1.1.5. Class FMT Security management

9.1.1.5.1. FMT_MSA.1 Management of security attributes

Hierarchical to: -

Dependencies: [FDP_ACC.1 Subset 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].

9.1.1.5.2. FMT_MSA.3 Static attribute initialization (1:FIL)

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.

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

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.

9.1.1.5.4. FMT_MSA.3 Static attribute initialization (3:DAT)

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.

9.1.1.5.5. FMT_MSA.3 Static attribute initialization (4:UDE)

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.

9.1.1.5.6. FMT_MSA.3 Static attribute initialization (5:IS)

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.

9.1.1.5.7. FMT_MOF.1 Management of security functions behaviour (1)

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management 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].

9.1.1.5.8. FMT_MOF.1 Management of security functions behaviour (2)

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MOF.1.1(2)	The TSF shall restrict the ability to [enable] the functions [calibration] to [workshop].

Application note 20: The calibration mode functions include the deactivation of the TOE's ability to use first generation tachograph cards.

9.1.1.5.9. FMT_MOF.1 Management of security functions behaviour (3)

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MOF.1.1(3)	The TSF shall restrict the ability to [enable] the functions [manage company locks] to [company].

9.1.1.5.10. FMT_MOF.1 Management of security functions behaviour (4)

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MOF.1.1(4)	The TSF shall restrict the ability to [enable] the functions [performing control activities] to [controller].

9.1.1.5.11. FMT_MOF.1 Management of security functions behaviour (5)

Hierarchical to: -

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management 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)].

9.1.1.5.12. 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)].

9.1.1.5.13. 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)].

9.1.1.5.14. FMT_SMR.1 Security ~~*management*~~ roles

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of ~~*user*~~ 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 (if applicable)].

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

9.1.1.6. Class FPT Protection of the TSF

9.1.1.6.1. FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -

Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state[34] 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].

9.1.1.6.2. 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 21: 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 22: 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). After its activation, the TOE shall detect specified hardware sabotage ~~*(details to be provided by the ST author)*~~.

9.1.1.6.3. FPT_PHP.3 Resistance to physical attack

Hierarchical to: -

Dependencies: -

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

[34] 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.

9.1.1.6.4. 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 23: Time stamps are derived from the internal clock of the vehicle unit. Requirements on time measurement and time adjustment are defined in [5] Annex 1C, Chapter 2, Sections 3.3 and 3.23.

9.1.1.6.5. 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 24: 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 25: Self-test of the link to IDE for data downloading required by FPT_TST.1 need only be carried out during downloading.

9.1.1.7. Class FTP Trusted path/channels

9.1.1.7.1. FTP_ITC.1 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 ~~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[35]].

Application note 26: Details of the communication channel can be found in [5] Appendix 11, Chapter 12.

[35] A trusted channel is not required for motion pulses.

9.1.2. 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.

9.1.2.1. Class FCS Cryptographic support

9.1.2.1.1. FCS_CKM.1 Cryptographic key generation (1)

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 [1) *Ephemeral ECC key generation as stated by section 10.4 in [5] Annex 1C, Appendix 11, Part B for session keys with tachograph cards.* 2) *Random number generation for session keys with motion sensors.*] and specified cryptographic key sizes [for the keys indicated in **ref. [6]** tables 21 and 22 as being generated by the TOE the key sizes required by [5] Annex 1C, Appendix 11, Part B for those keys] that meet the following: [Reference [7] predefined RNG class [*PTG.2*]].

Application note 27: The ST author selects one of the permitted predefined RNG classes from [7], and completes the operations in FCS_CKM.1(1) and FCS_RNG.1 as required. The permitted RNG classes are included in **ref. [6]** Annex B.

9.1.2.1.2. FCS_CKM.2 Cryptographic key distribution (1)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction[36]
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 [5] Annex 1C, Appendix 11, Part B] that meets the following [[5] Annex 1C, Appendix 11, Part B].

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

[36] Deviation from ref. [6] (PP). FCS_CKM.4 is stated as dependency in ref. [2] (CC part 2) but removed in ref. [6] (PP).

9.1.2.1.3. FCS_CKM.4 Cryptographic key destruction (1)

Hierarchical to: -

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

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroisation*] that meets the following [

- Requirements in **ref. [6]** Table 21 and Table 22;
- 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[37];
- [*No further standards needed*]].

9.1.2.1.4. FCS_COP.1 Cryptographic operation (1:AES)

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 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~~]
g) **ensuring confidentiality, authenticity, and integrity of data sent to an External DSRC 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 [5] Appendix 11, Part B].

[37] 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.

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

Hierarchical to: -

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

FCS_COP.1.1(2:SHA2) 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)].

9.1.2.1.6. FCS_COP.1 Cryptographic operation (3:ECC)

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 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[38];~~
~~f) mutual authentication between a vehicle unit and an external GNSS facility;~~
g) ensuring authenticity, integrity and non-repudiation of data downloaded from a vehicle unit]

in accordance with a specified cryptographic algorithm [[5], Annex 1C Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [5], Appendix 11, Part B] that meet the following: [[5] 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 12

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 12 - Standardised domain parameters

].

Application note 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

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

shall be of (roughly) equal strength. Table 13 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.

Cipher suite Id	ECC key size (bits)	AES key length (bits)	Hashing algorithm	MAC 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 13 - Cipher suites

9.1.2.1.7. FCS_RNG.1 Random number generation

Hierarchical to: -

Dependencies: -

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 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.

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 continuously. 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 [*numbers in the format 8- or 16-bit*] that meet [

PTG.2.6

Test procedure A, as defined in [7], 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

].

9.1.2.2. Class FIA Identification and authentication

9.1.2.2.1. FIA_ATD.1 User attribute definition (2:MS)

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 30: For further details see [5] Annex 1C, section ~~*3.1.12.2*~~ *3.12.1.2*, and Appendix 1 ~~*2.140 and 2.144*~~ *2.145*.

~~*9.1.2.2.2. FIA_ATD.1 User attribute definition (3:EGF)*~~[39]

~~*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 31: For further details see [5] Annex 1C, section 3.12.1.3, and Appendix 1 2.133 and 2.134.*~~

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

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of Identification

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 [5] Annex 1C, Appendix 11, Section 10** before allowing any other TSF-mediated actions on behalf of that user.

[39] FIA_ATD.1(3:EGF) is not applicable as the SE5000 uses an internal GNSS receiver.

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

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 [5] Annex 1C, Appendix 11, Section 12** before allowing any other TSF-mediated actions on behalf of that user.

~~*9.1.2.2.5. FIA_UAU.2 User authentication before any action (2:EGF)*~~[40]

~~*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 **external GNSS facility** to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Section 11** before allowing any other TSF-mediated actions on behalf of that user.*~~

9.1.2.3. Class FPT Protection of the TSF

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

Hierarchical to:	-
Dependencies:	-
FPT_TDC.1.1(1)	The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [5] Annex 1C, 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 [5] Annex 1C, Appendix 11] when interpreting the TSF data from another trusted IT product.

Application note 32: "Trusted IT product" in this requirement refers to generation 2 tachograph cards~~*, and*~~ motion sensor~~*, external GNSS facility (if applicable)*~~.

[40] FIA_UAU.2(2:EGF) is not applicable as the SE5000 uses an internal GNSS receiver.

9.1.2.4. Class FTP Trusted path/channels

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

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 33: Details of the communication channel can be found in [5] Appendix 11, Chapter 10.

~~*9.1.2.4.2. FTP_ITC.1 Inter-TSF trusted channel (3:EGF)*~~[41]

~~*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 34:* Details of the communication channel can be found in [5] Appendix 11, Chapter 11.~~

[41] FTP_ITC.1(3:EGF) is not applicable as the SE5000 uses an internal GNSS receiver.

9.1.3. 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.

9.1.3.1. Class FCS Cryptographic support

9.1.3.1.1. FCS_CKM.1 Cryptographic key generation (2)

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 keys in accordance with a specified 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 [5] Annex 1C, Appendix 11 Part A, Chapter 3].

9.1.3.1.2. FCS_CKM.2 Cryptographic key distribution (2)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction[42]
FCS_CKM.2.1(2)	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [for triple DES session key as specified in [5] Annex 1C, Appendix 11 Part A] that meets the following [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

9.1.3.1.3. FCS_CKM.4 Cryptographic key destruction (2)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1(2)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroisation*] that meets the following [- Requirements in **ref. [6]** Table 18 and Table 19; - 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[43]; - [*No further standards needed*]].

[42] Deviation from ref. [6] (PP). FCS_CKM.4 is stated as dependency in ref. [2] (CC part 2) but removed in ref. [6] (PP).
[43] 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.

9.1.3.1.4. FCS_COP.1 Cryptographic operation (4:TDES)

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 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 sizes [112 bits] that meet the following: [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

9.1.3.1.5. FCS_COP.1 Cryptographic operation (5:RSA)

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 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 sizes [1024 bits] that meet the following: [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

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

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

9.1.3.2. Class FIA Identification and authentication

9.1.3.2.1. FIA_UAU.1 Timing of authentication (2:TC)

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 [5] Annex 1C, Appendix 11, Part A, Section 5** before allowing any other TSF-mediated actions on behalf of that user.

9.1.3.3. Class FPT Protection of the TSF

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

Hierarchical to:	-
Dependencies:	-
FPT_TDC.1.1(2)	The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [5] Annex 1C, 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 [5] Annex 1C, Appendix 11 Part A, Chapter 5] when interpreting the TSF data from another trusted IT product.

Application note 35: "Trusted IT product" in this requirement refers to generation 1 tachograph cards ~~*and motion sensor*~~.

9.1.3.4. Class FTP Trusted path/channels

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

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 [5] Appendix 2].

Application note 36: Details of the communication channel can be found in [5] Appendix 11, Chapters 4 and 5.

9.2. Security assurance requirements

The assurance level for this security target is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [3].

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

9.3. Security requirements rationale

9.3.1. 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
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)	FDP_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.3(5:IS)
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	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) and FPT_TDC.1(1&2)
~~FDP_ITT.1~~	~~FDP_ACC.1 or FDP_IFC.1~~	~~Satisfied by FDP_ACC.1(3:DAT)~~
FDP_RIP.1	-	-
FDP_SDI.2(1)	-	-
FDP_SDI.2(2)		
FIA_AFL.1(1:TCL)	FIA_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)	-	-
FIA_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

SFR	Dependencies	Rationale
FMT_MSA.3(1:FIL)	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1 and FMT_SMR.1
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_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, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.1(1) and FCS_CKM.4(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 and FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_RNG.1[44]	-	-
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(2:EGF)~~	~~FIA_UID.1~~	~~Satisfied by FIA_UID.2~~
FPT_TDC.1(1)	-	-
FTP_ITC.1(2:TC)	-	-
~~FTP_ITC.1(3:EGF)~~	~~-~~	~~-~~

[44] Extended component

SFR	Dependencies	Rationale
1st generation specific		
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2(2), FCS_COP.1(4:TDES & 5:RSA) and FCS_CKM.4(2)
FCS_CKM.2(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2 and FCS_CKM.1(2)
FCS_COP.1(4:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_COP.1(5:RSA)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_COP.1(6:SHA-1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-1
FIA_UAU.1(2:TC)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(2)	-	-
FTP_ITC.1(4:TC)	-	-

Table 14 - SFRs' dependencies

9.3.2. 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.

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Exchange	O.Software_Update
FAU_GEN.1	Security 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			X					X	
FDP_ACF.1	Security attribute based access control (4:UDE)	X			X					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_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
~~FDP_ITT.1~~	~~Basic internal transfer protection~~						~~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		
FDP_SDI.2	Stored data integrity monitoring and action (2)							X	X		
FIA_AFL.1	Authentication failure handling (1:TCL)			X	X				X		
FIA_AFL.1	Authentication failure handling (2:TCR)			X	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	

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Exchange	O.Software_Update
FIA_UAU.3	Unforgeable authentication				X						
FIA_UAU.5	Multiple authentication mechanisms				X						
FIA_UAU.6	Re-authenticating				X					X	
FIA_UID.2	User *identification* ~~*authentication*~~ before any action	X	X	X	X					X	
FMT_MSA.1	Management of security attributes	X								X	
FMT_MSA.3	Static attribute initialization (1:FIL)	X									
FMT_MSA.3	Static attribute initialization (2:FUN)	X						X	X	X	
FMT_MSA.3	Static attribute initialization (3:DAT)	X									
FMT_MSA.3	Static attribute initialization (4:UDE)	X									
FMT_MSA.3	Static attribute initialization (5:IS)	X						X	X		
FMT_MOF.1	Management of security functions behaviour (1)	X				X	X	X	X		
FMT_MOF.1	Management of security functions behaviour (2)	X							X		
FMT_MOF.1	Management of security functions behaviour (3)	X			X						
FMT_MOF.1	Management of security functions behaviour (4)	X			X						
FMT_MOF.1	Management of security functions behaviour (5)	X			X						
FMT_MTD.1	Management of TSF data	X			X	X		X	X		
FMT_SMF.1	Specification of management functions	X								X	
FMT_SMR.1	Security management roles	X								X	
FPT_FLS.1	Failure with preservation of secure state								X		
FPT_PHP.2	Notification of physical attack						X		X		
FPT_PHP.3	Resistance to physical attack						X	X	X		
FPT_STM.1	Reliable time stamps		X	X				X	X		
FPT_TST.1	TSF testing			X					X		
FTP_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 operation (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	Timing of authentication (1:TC)				X					X	

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Exchange	O.Software_Update
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		
FTP_ITC.1	Inter-TSF trusted channel (4:TC)									X	

Table 15 - Coverage of security objectives for the SE5000 by SFRs

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

Security Objective	SFR	Rationale
O.Access	FDP_ACC.1(1:FIL) FDP_ACF.1(1:FIL)	The File Structure SFP defines the policy for restricting modification or deletion of the application and data files structure and access conditions.
	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(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 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_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource.
	FIA_UID.2	Connected devices have to be successfully *identified* ~~*authenticated*~~ before allowing any other action.

Security Objective	SFR	Rationale
	FMT_MSA.1	Supports the Function SFP by restricting the ability to change defaults for the security attributes User Group, User ID to nobody.
	FMT_MSA.3(1:FIL)	Supports the File Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3(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_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.
	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. Also Restricts the ability to read remote early detection communication facility data to control cards.
	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_MOF.1(1)	Restricts the ability to enable the *manufacture* test functions ~~*as 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 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.
	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	Protects the stored audit records from unauthorised deletion.

Security Objective	SFR	Rationale
	FAU_STG.4	Prevents loss of audit data loss (overwrites 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.
	FAU_STG.1	Protects the stored audit records from unauthorised deletion.
	FAU_STG.4	Prevents loss of audit data loss (overwrites the oldest stored audit records and behaves correctly if the audit trail is full).
	FDP_SDI.2(1)	Monitors stored user data 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 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 traceability of audited 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.*~~
	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.
	FIA_UAU.3	Provides unforgeable authentication.
	FIA_UAU.5	Multiple authentication methods are required for use of workshop cards.
	FIA_UAU.6	Periodically re-authenticates tachograph cards.
	FIA_UID.2	Connected devices are successfully *identified* ~~*authenticated*~~ before allowing any other action.

Security Objective	SFR	Rationale
	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 processs.
	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.
	~~*FIA_UAU.2(2:EGF)*~~	~~*An external GNSS facility has to be successfully authenticated before allowing any action.*~~
O.Integrity	FAU_STG.1	Protects the stored audit records from unauthorised deletion.
	FDP_ETC.2	Provides export of user data with security attributes using the User Data Export SFP.
	FDP_SDI.2(1)	Monitors stored user data for integrity errors.
	FMT_MOF.1(1)	Prevents access to commands used in manufacturing that may be used to affect integrity.
	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 SFP User Data Export. Data downloaded is protected by signature against undetected modification.
	~~FDP_ITT.1~~	~~Provides protection for user data during transfer to the printer and display.~~
	FDP_SDI.2(1)	Monitors stored user data for integrity errors.
	FMT_MOF.1(1)	Prevents access to commands used in manufacturing that may be used to affect outputs.
	FPT_PHP.2 FPT_PHP.3	Requires resistance to physical attack to the TOE software in the field, and detection of attempted attacks on the TOE, after the TOE activation.
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).

Security Objective	SFR	Rationale
	FDP_ACC.1(5:IS) FDP_ACF.1(5:IS)	The Input Sources SFP defines 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_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_ITT.1~~	~~Where the TOE is implemented as physically separated components this provides integrity protection of transferred data.~~
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource.
	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_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.
	FDP_SDI.2(2)	Requires consistency between motion sensor data and GNSS data.
	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 to support processing.
	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.
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_ACC.1(5:IS) FDP_ACF.1(5:IS)	The Input Sources SFP defines 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_SDI.2(1 & 2)	Requires consistency between motion sensor data and GNSS data.
	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.

Security Objective	SFR	Rationale
	~~FDP_ITT.1~~	~~Where the TOE is implemented as physically separated components this provides integrity protection of transferred data.~~
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource.
	FDP_SDI.2(1&2)	Monitors stored user data for integrity errors.
	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.*~~
	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_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_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 specified 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 to support processing.
	FPT_TST.1	Detects integrity failure events for security data and stored executable code.
	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.
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).
	FDP_ACC.1(4:UDE) FDP_ACF.1(4:UDE)	Restricts the ability to read remote early detection communication facility data to control cards.

Security Objective	SFR	Rationale
	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.
	FIA_UAU.6	Periodically reauthenticates Tachograph cards.
	FIA_UID.2	Connected devices are successfully *identified* ~~*authenticated*~~ 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 functions.
	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 used 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 tachograph cards.
	FCS_CKM.1(2)	Key generation used to support authentication for the exchange.
	FCS_CKM.2(2)	Key distribution used to support authentication for the exchange.
	FCS_CKM.4(2)	Specifies the requirements for key destruction.

Security Objective	SFR	Rationale
	FCS_COP.1(4:TDES)	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 16 - Suitability of the SFRs

9.3.3. Security assurance requirements rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [5] 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 predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 4 – Subjects and external entities, entry ‘Attacker’). This decision represents a part of the conscious security policy for the recording equipment required by the Regulation [5] and reflected by this 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 17 - SARs' dependencies (additional to EAL4 only)

9.3.4. Security requirements – internal consistency

This part of the security requirements rationale shows that the set of security requirements for the SE5000 consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

a) SFRs

The dependency analysis in chapter 9.3.1 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 chapter 9.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items. The current ST accurately reflects the requirements of Commission Implementing Regulation 2016/799 implementing Regulation 165/799 of the European Parliament and of the Council, Annex 1C [5], which is assumed to be internally consistent.

b) SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the assurance components in chapter 9.3.3 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 chapters 9.3.1 and 9.3.3. Furthermore, as also discussed in chapter 9.3.3, the chosen assurance components are adequate for the functionality of the SE5000. So, there are no inconsistencies between the goals of these two groups of security requirements.

10. SE5000 TOE SUMMARY SPECIFICATION (ASE_TSS)

The following sub-chapters shows how each SFR from chapter 9.1 is met by one or several TSF's.

10.1. TSF.ACTIVITIES

TSF.ACTIVITIES keeps control of all activity done by the user and ensures that user data is written to VU and card. It also enables/disables functionality depending on user (driver, workshop, control and company). It detects event related to user behaviour.

(1) Detects *Card conflict*, *Time overlap*, *Driving without an appropriate card*, or *Card insertion while driving and* reports an event to TSF.ERRORMGR.
- [FAU_GEN.1.1]

(2) Enforces the [Function SFP] on company locks management permitted only in company mode, monitoring of control activities only permitted in control mode, release of tachograph cards only permitted after all relevant data has been stored on the Card.
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN), FMT_MOF.1.1(3), FMT_MOF.1.1(4), FMT_SMF.1.1]

(3) Enforces the [User Data Export SFP] to store user data relevant to the period while the card is inserted and relevant to the cardholder on valid Driver-, Workshop-, and Control Cards.
- [FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.2(4:UDE)]

(4) Supports accessibility to calibration function only permitted in calibration mode.
- [FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN), FMT_SMF.1.1]

(5) Restrict functionality at start-up and allow nobody to override the initial values
- FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN)]

10.2. TSF.BIST

TSF.BIST runs test to ensure that tampering of memory is detected. It also run test to ensure correctness of Composite TOE.

(1) Detects code and data integrity violations and reports *Recording equipment fault[VU internal fault]* event to TSF.ERRORMGR. Any user authorized to display/print/download events and faults can verify the integrity of code and data through the absence of *Recording equipment fault[VU internal fault]* and *Security breach attempt[Stored data integrity error]* audit records.
- [FAU_GEN.1.1, FPT_TST.1.2, FPT_TST.1.3]

(2) Protects cryptographic keys and certificates installed by the manufacturer against modification.
- [FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(3) Protects VU identification data against unauthorised modification.
- [FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(4) Protects TSF software against physical tampering attacks.
- [FPT_PHP.3.1]

(5) Runs a suite of self tests during start up and periodically during normal operation. This includes verification of the integrity of TSF data memory, TSF software, and TOE Platform built-in tests.
- [FPT_TST.1.1]

10.3. TSF.CARD

TSF.CARD controls all secure communication with tachograph card. Ensures that a secure communication channel exists and is used for communication. Detect Card related events. Control start-up /shutdown of card. Ensure that temporary stored cryptographic keys (used for card communication) is removed when not needed.

(1) Detects *Insertion of non-valid card*, *Last card session not correctly closed*, *Card fault*, and *Security breach attempt* (on Tachograph Card authentication failure, hardware sabotage, or Tachograph Card data input integrity error) and reports event to TSF.ERRORMGR.
- [FAU_GEN.1.1]

(2) Ensures that no TSF-mediated action is performed before the claimed identity of a Tachograph Card has been authenticated. TSF.CARD allows reading out of audit records from an expired Tachograph Card, which cannot become authenticated.
- [FIA_UAU.1.1(1:TC), FIA_UAU.1.1(2:TC)]

(3) When a 2nd generation Tachograph Card is inserted, TSF.CARD uses TSF.CRYPTO and in compliance with the procedures of [Annex_1C] Appendix 11 chapter 10:
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS), FDP_RIP.1.1, FIA_ATD.1.1(1:TC), FIA_UAU.3.1, FIA_UAU.3.2, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_SMR.1.1, FMT_SMR.1.2, FIA_UAU.1.2(1:TC)]

(3.1) Identifies the Tachograph Card (represented by the security attributes *User group* and *User ID*) and verifies its identity by verifying its certificate chain.
(3.2) When the Tachograph Card is a Workshop Card, the user is requested to enter a PIN for verification by the Workshop Card. Authentication proceeds only if the PIN is verified to be correct. If the PIN is incorrect, the PIN is requested until the Workshop Card reports that it is locked, then *Insertion of non-valid card* is reported to TSF.ERRORMGR, the Workshop Card is declared non-valid and the user as unknown. The PIN is stored at most until end of calibration mode and the Tachograph Card is ejected, when it is wiped and made unavailable.
(3.3) Authenticates the Tachograph Card
(3.4) Generates cryptographic session keys and performs key agreement with the Card.
(3.5) Ensures that the security attributes *User group* and *User ID* cannot be changed while the Tachograph Card is inserted.

(4) When a 1st generation tachograph Card is inserted, TSF.CARD uses TSF.CRYPTO and in compliance with the procedures of [Annex_1C] Appendix 11 chapter 4:
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS), FIA_ATD.1.1(1:TC), FIA_UAU.3.1, FIA_UAU.3.2, FIA_UID.2.1, FMT_SMR.1.1, FMT_SMR.1.2, FIA_UAU.1.2(2:TC)]

(4.1) Checks that the ability to authenticate 1st generation Tachograph Cards is still enabled. When the ability is disabled, the inserted Tachograph Card is rejected and declared invalid.
(4.2) When the ability is enabled, identifies the Card (represented by the security attributes *User group* and *User ID*) and verifies its identity by verifying its certificate chain.
(4.3) When the ability is enabled, authenticates the Card
(4.4) When the ability is enabled, generates cryptographic session keys and performs key agreement with the Card.
(4.5) When the Card is a Workshop Card, it is never authenticated, but declared non-valid and ejected immediately.

(5) When 5 consecutive unsuccessful authentication attempts of a local Card have been detected *Insertion of non-valid card* is reported to TSF.ERRORMGR, the Card is declared invalid and the user is set to Unknown.
- [FIA_AFL.1.1(1:TCL), FIA_AFL.1.2(1:TCL)]

(6) When 1 consecutive unsuccessful authentication attempts of a Company Card at a remotely connected company has been detected, the remotely connected company is warned.
- [FIA_AFL.1.1(2:TCR), FIA_AFL.1.2(2:TCR)]

(7) Re-authenticates all inserted Tachograph Cards:
- [FIA_UAU.6.1]

(7.1) After a power supply interruption
(7.2) When the secure messaging session has been aborted
(7.3) After any other reset than power supply interruption
(7.4) When any of the session keys are about to expire
(7.5) Once every 12 hours

(8) While a Tachograph Card is authenticated, TSF.CARD uses the inter-TSF trusted channel for communication with that Card:
- [FAU_GEN.1.1, FDP_ETC.2.1, FDP_ETC.2.2, FDP_ETC.2.3, FDP_ETC.2.4, FDP_ITC.2.1, FDP_ITC.2.2, FDP_ITC.2.3, FDP_ITC.2.4, FDP_ITC.2.5, FPT_TDC.1.1(1), FPT_TDC.1.2(1), FTP_ITC.1.1(2:TC), FTP_ITC.1.2(2:TC), FTP_ITC.1.3(2:TC), FPT_TDC.1.1(2), FPT_TDC.1.2(2), FTP_ITC.1.1(4:TC), FTP_ITC.1.2(4:TC), FTP_ITC.1.3(4:TC)]

(8.1) Initiates actions [SELECT (Selection by name and Selection of an Elementary File using its File Identifier), READ BINARY, UPDATE BINARY].
(8.2) Enforces the [User Data Export SFP] on data exported to Tachograph Cards.
(8.2.1) All communication associates security attributes with data exported to Cards to enable the Card to verify the data's integrity and authenticity in compliance with [Annex_1C] Appendix 11 Section 10.5.
(8.2.2) TSF.CARD maintains a Send Sequence Counter for each authenticated Tachograph Card and the session keys agreed with the Tachograph Card during authentication.

(8.2.3) TSF.CARD maintains information on the storage capacity on each elementary file on an inserted Tachograph Card and uses this information to ensure that most recent replaces the oldest data when all storage capacity is in use.

(8.3) TSF.CARD enforces [Input Sources SFP] through all communication verifies integrity and data imported from the Card using the security attributes associated with the Card and its data, in compliance with [Annex_1C] Appendix 11 Section 10.5. Data is only accepted for use if its integrity and authenticity has been verified, otherwise it is ignored and discarded.

(8.4) TSF.CARD maintains a logical trusted channel for each authenticated Card.

(8.5) The secure messaging session is aborted:

(8.5.1) When a message is received without security attributes.

(8.5.2) When and integrity or authenticity error of data imported from the Card is detected. Reports a *Security breach attempt* to TSF.ERRORMGR.

(8.5.3) When aborted by the Card.

(9) Requires input from TSF.MMI to release a Tachograph Card and rejects any request to eject a Tachograph Card while the vehicle is moving and, if the vehicle is stopped, ensures that all relevant data has been written to the Card before ejecting the Card.

- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN)]

(10)Temporarily stored cryptographic keys:

- [FDP_RIP.1.1]

(10.1) When the secure messaging session against any Tachograph Card is aborted or ends, the related session keys are made unavailable, and

(10.2) When the secure messaging session against a Workshop Card is aborted, the related Motion Sensor keys used during pairing are made unavailable.

(11)TSF.CARD only uses TSF.CRYPTO interfaces intended for use by TSF.CARD.

- [FDP_ACF.1.4(2:FUN)]

(12)Uses TSF.PSI to ensure that a secure state is maintained in case of a power supply interruption or any other reset condition, as a power supply interruption may cause a transaction to be stopped before completion. User data and audit records are kept in non-volatile memory until they have been completely written to Tachograph Cards.

- [FPT_FLS.1.1]

(13)TSF.CARD implicitly tests the communication link to the tachograph card by performing secure messaging/(re)authentication over the link while a card is inserted.

- [FPT_TST.1.1]

(14)Restrict functionality at start-up and allow nobody to override the initial values

- [FMT_MSA.1.1, FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_MSA.3.1(4:UDE), FMT_MSA.3.2(4:UDE), FMT_MSA.3.1(5:IS), FMT_MSA.3.2(5:IS)]

10.4. TSF.CASING

TSF.CASING consists of a physical box that gives protection from tampering and dust/water according to IP class. The enclosure of the VU is made in such way that it is not possible to open once sealed. It is considered as a closed box. The case ensures that the VU will not be physically modified without detection

(1) The TSF.CASING provides a mechanical protection of the TOE. Any breach attempt will be evident to a visual inspection.

- [FPT_PHP.2.1, FPT_PHP.2.2]

(1.1) The VU is enclosed in a Stoneridge unique case. It is realized in mechanics and inherits no basic components. At end of final assembly of manufacturing the VU, the VU is permanently closed using heat stakes that force the box and the front of the case together.

(1.2) The card slots are covered by a plastic tamper protection construction on the card readers.

(1.3) A security seal (called Tamper label) is mounted over the split line between the box and the front will reveal any attempt to reach electronic details through the hole for the printer paper magazine of the VU.

(2) This ensures that:

- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ITC.1.1, FDP_ITC.1.2, FDP_ITC.1.3]

(2.1) The TOE only process data from the right input sources:

(2.1.1) Human input via buttons

(2.1.2) RTC

(2.1.3) GNSS receiver

(2.2) Physical tampering is detected.

10.5. TSF.CONFIG

TSF.CONFIG enforces calibration function modifying parameters.

(1) TSF.CONFIG handles the access to the calibration and road side calibration function.
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FMT_MOF.1.1(2), FMT_MTD.1.1, FMT_SMF.1.1, FMT_MOF.1.1(4)]

(1.1) When the TOE is non-activated, the calibration function is always accessible
(1.2) When the TOE is activated the calibration function is only accessible in Calibration Mode.
(1.3) When the TOE is activated, manually changing the clock is restricted to Calibration Mode.
(1.4) Roadside calibration functions are restricted to control mode.

(2) Ensures that calibration parameters can only be input in calibration mode from the right input sources.
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS), FDP_ITC.1.1, FDP_ITC.1.2, FDP_ITC.1.3]

(3) Handles the driver consent, which determines whether personal data can leave the vehicle network (exported through external interfaces).
- [FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.3(4:UDE)]

(4) Warns the remotely connected company if the card authentication has failed.
- [FIA_AFL.1.2(2:TCR)]

(5) Restrict functionality at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_MSA.3.1(4:UDE), FMT_MSA.3.2(4:UDE), FMT_MSA.3.1(5:IS), FMT_MSA.3.2(5:IS)]

10.6. TSF.CRYPTO

TSF.CRYPTO uses the TOE Platform's hardware co-processors for basic DES, AES, RSA, and ECC operations and the TOE Platform's True Random Number Generator for generation of random numbers. Access to RSA and ECC operations uses a TOE Platform Crypto Library.

(1) TSF.CRYPTO uses the Platform TSF SF.CS to provide a physical random generation compliant with functional class PTG.2. It is also used for generation of cryptographic keys.
- [FCS_CKM.1.1(1), FCS_RNG.1.1, FCS_RNG.1.2]

(2) TSF.CRYPTO contains a database that handles all cryptographic keys (except ephemeral keys used in key generation-, distribution-, and agreement of 2nd generation Tachograph Card session keys). The key database ensures that private and secret keys are stored in secure memory areas and provides functionality to delete and make key unavailable. TSF.CRYPTO also stores identification data for the currently paired Motion Sensor. The identification is stored during the pairing process and is only accessible through read-only interfaces to external modules.
- [FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT), FDP_ACF.1.4(3:DAT), , FCS_CKM.4.1(1), FIA_ATD.1.1(2:MS), FCS_CKM4.1(2)]

(3) TSF.CRYPTO provides functionality for AES in ECB-, CBC, and CMAC modes of operation using key sizes 128-, 192, and 256 bits. It uses the TOE Platform SF.CS to implement AES.
- [FCS_COP.1.1(1:AES)]

(4) SHA-2 algorithm is provided through a direct software implementation. Computes SHA-256, SHA-384, and SHA-512 hash digests.
- [FCS_COP.1.1(2:SHA-2)]

(5) TSF.CRYPTO provides functionality for ECC for perform ECDH and ECDSA operations Brainpool curves with sizes 256-, 384-, and 512 bits and NITS curves with sizes 256-, 384-, and 521 bits. It uses the TOE Platform SF.CS to implement ECC.
- [FCO_NRO.1.2, FCS_CKM.1.1(1), FCS_CKM.2.1(1), FCS_COP.1.1(3:ECC)]

(6) TSF.CRYPTO provides functionality for two-key TDES in ECB-, CBC, and RetailMAC modes of operation using key size 112 bits. It uses the TOE Platform SF.CS to implement TDES.
- [FCS_COP.1.1(4TDES)]

(7) TSF.CRYPTO provides functionality RSA operations using 1024 bits keys. It uses the TOE Platform SF.CS to implement RSA.
- [FCS_COP.1.1(5:RSA]

(8) SHA-1 algorithm is provided through a direct software implementation. Computes SHA-160 hash digest.
- [FCS_COP.1.1(6:SHA-1)]

(9) TSF.CRYPTO detects and prevents use of forged or copied authentication data when employing cryptographic functions for key derivation-, generation-, distribution-, and agreement for Motion Sensor pairing and Tachograph Card authentication.
- [FIA_UAU.3.1, FIA_UAU.3.2]

(10) TSF.CRYPTO performs all operations for generation of cryptographic keys and implements the algorithms for key distribution and agreement. It is used for mutual authentication of 1st generation Tachograph Cards, 2nd generation Tachograph Cards, and for pairing and authentication of 2nd generation Motion Sensors.
- [FCS_CKM.1.1(1), FCS_CKM.1.1(2), FCS_CKM.2.1(1), FCS_CKM.2.1(2),]

(11) TSF.CRYPTO ensures that all private- and secret keys, and certificates are correctly installed during the manufacturing process. When the personalization phase has completed successfully, cryptographic checksum protecting these assets are created, and all commands, actions and test points that are available during the manufacturing process are forever made inaccessible.
- [FMT_MOF.1.1(1)]

(12) Restrict default values at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(3:DAT), FMT_MSA.3.2(3:DAT)]

(13) Ensures the ephemeral ECC private key used for key generation is made unavailable immediately after use.
- [FDP_RIP.1.1]

(14) Erases faulty output data. Implements fault injection detection and, when a possible fault injection is detected, performs a security reset to main a secure state.
- [FPT_FLS.1.1, FDT_PHP.3.1]

(15) TSF.CRYPTO ensures that no TSF mediated action, i.e. Motion Sensor secure messaging, can occur before the Motion Sensor has been authenticated.
- [FIA_UAU.2.2(1:MS)]

10.7. TSF.DSRC

TSF.DSRC controls all communication and creates messages to be sent to a REDCR

(1) Detects *Remote Communication Facility communication fault* and reports event to TSF.ERRORMGR.
- [FAU_GEN.1.1]

(2) Uses TSF.CRYPTO to encrypt and authenticate data:
- [FCO_NRO.1.1, FCO_NRO.1.3, FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.2(4:UDE)]
- Constructs the Encrypted Tachograph Payload, appends Security Data and computes the MAC.
- Verification of the MAC provides evidence of origin of the data
- Ensures only a controller can read remote early communication facility data.

(3) Provides self test through correct function and correct communication between the TOE and the remote communication facility.
- [FPT_TST.1.1]

(4) Restrict data and allow to nobody to override the initial values.
- [FMT_MSA.3.1(4:UDE), FMT_MSA.3.2(4:UDE)]

10.8. TSF.DOWNLOAD

TSF.DOWNLOAD provides services for download of data with corresponding signatures. When data is downloaded a validation is also done to ensure correctness of data within the download.

(1) Detects user data integrity errors and reports *Security breach attempt[Stored user data integrity error]* event to TSF.ERRORMGR. Any user authorized to display/print/download events and faults can verify the integrity of stored user data through the absence of *Security breach attempt[Stored user data integrity error]* audit records.
- [FAU_GEN.1.1, FDP_SDI.2.2(1), FPT_TST.1.2]

(2) Enforces [Data SFP] so unauthorised modification of stored audit records and user data is detected during download.
- [FAU_STG.1.2, FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT), FDP_SDI.2.1(1)]

(3) Provides functionality for authorised users, i.e. users not subject to the constraints in (4) below, to download audit records, stored by the VU. Stored audit records include audit records imported from the Motion Sensor.
- [FAU_SAR.1.1, FAU_SAR.1.2]

(4) The following constraints are applied to enforce [User Data Export SFP]:
- [FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.4(4:UDE), FMT_SMF.1.1]
- Restricts downloading from the VU to *Control Card*, *Workshop Card*, and *Company Card*.

(4.1) By restricting downloads to control-, company-, and calibration mode, personal identification and card number are only output when the inserted card is a Driver Card.

(4.2) In company mode driver related data are only output for periods where no lock exists or no other company holds a lock.

(5) Uses TSF.CRYPTO to create a hash (SHA-2 algorithm) over downloaded data and uses the hash to generate a digital signature (ECDSA):
- [FCO_NRO.1.1, FCO_NRO.1.3, FDP_ETC.2.1, FDP_ETC.2.2, FDP_ETC.2.3, FDP_ETC.2.4]

(5.1) Uses VU_Sign.SK belonging to the VU to sign the SHA-2 hash computed over the downloaded data.

(6) Provides self test through correct function and correct communication over the download link.
- [FPT_TST.1.1]

(7) Enforces that VU download functionality is accessible only in right mode of operation.
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN)]

(8) Restrict functionality at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_FMA.3.1(4:UDE), FMT_MSA.3.2(4:UDE)]

10.9. TSF.ERRORMGR

TSF.ERRORMGR ensures that reported Event/faults are stored in a correct way.

(1) Generates an audit record when any TSF reports an event or fault based on the event- or fault ID and the reported status. TSF.ERRORMGR stamps audit records with correct data and time. Audit records are sent TSF.STORAGE for storage in VU or, where related an inserted Tachograph Card or its user, to the Tachograph Card. Uses TSF.MMI to display a visual warning.
TSF.ERRORMGR uses TSF.TAM for information regarding a Tachograph Card's insertion and withdrawal times, which are used to determine whether data is relevant to store on the Tachograph Card.
TSF.ERRORMGR uses TSF.TIME to provide correct time to an audit record.
- [FAU_GEN.1.1, FAU_GEN.1.2, FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.2(4:UDE), FIA_AFL.1.2(1:TCL), FIA_AFL.1.2(3:MS), FPT_PHP.2.3]

(2) Ensures that the start-up tests are execute, and runtime tests in BIST are executed once per 24 hours. Generates an audit record and a security reset if the tests fail to execute, or if any test reports an error.
- [FPT_TST.1.1]

10.10. TSF.FRAMEWORK

TSF.FRAMEWORK handle start-up of the TOE in a controlled way.

(1) Ensures that the bootloader is deactivated at first start, and does not continue beyond this point until the bootloader is deactivated. This effectively removes all commands, action or test points that are specific to the testing need during the manufacturing phase.
- [FMT_MOF.1.1(1)]

(2) Provides interface to generate security reset.
- [FPT_FLS.1.1]

(3) Ensures that operational mode is not entered until power is sufficient to detect a power supply interruption and report the event.
- [FPT_FLS.1.1]

(4) Tachograph application and data files structure is created during the manufacturing process and then locked against any future modification or deletion, no functionality exist inside VU to change application or data file structure
- [FDP_ACC.1.1(1:FIL), FDP_ACF.1.1(1:FIL), FDP_ACF.1.2(1:FIL), FDP_ACF.1.3(1:FIL), FDP_ACF.1.4(1:FIL), FMT_MSA.3.1(1:FIL), FMT_MSA.3.2(1:FIL)]

(5) Audit functions are always on after power on therefore no detection or reports of start up and shut down of audit functions are possible

- [FAU_GEN.1.1]

10.11. TSF.GNSS

TSF.GNSS controls all communication received from GNSS satellites including supervision of signal loss

(1) Reports *Absence of position information from GNSS* and *Recording equipment fault - Internal GNSS Receiver* to TSF.ERRORMGR. Since external GNSS is not supported by the TOE faults related to "*Communication error with the external GNSS facility*" can never occur
- [FAU_GEN.1.1]

10.12. TSF.IPC

TSF.IPC is the communication channel between MCU and SAM. It acts as a gateway and only forwards messages approved

(1) TSF.IPC acts as a firewall that only accepts signals that are permitted to be sent to the TOE. Thus, data from external input sources will not be accepted as executable code.
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.4(5:IS), FDP_ITC.2.5]

(2) Restrict functionality at start-up and allow nobody to override the initial values.
- [FMT_MSA.3.1(5:IS), FMT_MSA.3.2(5:IS)]

10.13. TSF.MMI

TSF.MMI controls input and output of user by using buttons, display and a printer

(1) Provides Display Output to visually warn the user. Detects "Recording equipment", printer fault and display fault.
- [FAU_GEN.1.1, FIA_AFL.1.2(3:MS), FIA_AFL.1.2(1:TCL), FPT_PHP.2.3]

(2) Provides capability to review audit records through display or printer
- [FAU_SAR.1.1, FAU_SAR.1.2]

(3) Release of tachograph cards shall function only when the vehicle is stopped and require positive action by the human user
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN)]

(4) In operational mode do not output to display or printer or any personal identification or card number 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.
- [FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.4(4:UDE),]

(5) Restrict the ability to enable the printout functions (to display or printer) in calibration to workshops
- [FMT_MOF.1.1(2)]

(6) Restrict the ability to enable the printout functions (to display or printer) in performing control activities to controller
- [FMT_MOF.1.1(4)]

(7) Restrict functionality at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_MSA.3.1(4:UDE), FMT_MSA.3.2(4:UDE)]

10.14. TSF.MMU

TSF.MMU keeps control of memory allocation/deallocation used to ensure that no external interfaces are available at the same time as the secret keys

(1) Prevents unauthorised modification of private- and secret keys through its Secure Access Domain by disabling access to external interface code before enabling access to private- and secret keys (when entering Secure Access Domain) and disabling access to private- and secret keys before enabling access to external interface code (when exiting Secure Access Domain).
- [FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(2) Resists physical tampering attacks (fault injection) of the private- and secret keys by responding automatically with security reset.

- [FPT_PHP.3.1]

(3) Ensures a secure initialisation state of the MMU
(4) Restrict default values at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(3:DAT), FMT_MSA.3.2(3:DAT)]

10.15. TSF.PSI

TSF.PSI is the supervisor for external power to TOE. It also ensure that there is time enough to store relevant data in case of a power loss

(1) When a power supply interruption is detected, TSF.PSI: Reports a Power supply interruption event to TSF.ERRORMGR and preserves a secure state.
- [FAU_GEN.1.1, FPT_FLS.1.1, FPT_PHP.2.3, FPT_PHP.3.1]

(1.1) Stores an indication that the event has occurred.
(1.2) Notifies other TSFs that a power supply interruption is ongoing.
(1.3) Prevents normal operation until a power-on reset has occurred, the event has been stored and power is valid.

(2) Power supply interruption is:
(2.1) The power goes below a defined threshold for 200 milliseconds or more.
(2.2) Approximately 300 consecutive (i.e. less than 4 seconds between each pulse) pulses where the interruption is shorter than 200 milliseconds occurs.

(3) Ensure that operational mode is not entered until power is sufficient to detect a power supply interruption and report the event.
- [FTP_FLS.1.1]

10.16. TSF.STORAGE

TSF.STORAGE is a supporting all TSF:s in storing data and keep control of replacement of oldest data

(1) Sets the subject identity on audit records and stores audit records, user data, and audit records imported from the Motion Sensor.
- [FAU_GEN.1.1, FAU_GEN.1.2, FAU_STG.1.1, FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(2) Implements the storage rules for audit records, user data, and audit records imported from Motion Sensor stated in [Annex_1C] chapters 3.12.
- [FAU_STG.4.1, FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(3) Computes and stores cryptographic checksums that are used by TSF.DOWNLOAD to detect unauthorised deletions or modifications to audit records, user data, and audit records imported from the Motion Sensor.
- [FAU_STG.1.1, FAU_STG.1.2, FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT)]

(4) TSF.STORAGE ensures that data stored on valid Driver-, Workshop-, and Control Cards are updated with necessary data relevant to the card holder and for the period the Card is inserted and that manually entered driver and activity data, corresponding to last card withdrawal time to current insertion time will be stored to valid Driver- and Workshop Cards.
- [FDP_ACC.1.1(3:DAT), FDP_ACF.1.1(3:DAT), FDP_ACF.1.2(3:DAT), FDP_ACF.1.3(3:DAT), FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.2(4:UDE)]

(5) TSF.STORAGE ensures that release of a Tachograph Card cannot happen before all relevant data has been written to the Tachograph Card.
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN)]

(6) TSF.STORAGE ensures that a transaction is either completely written. If a transaction is stopped before completion, TSF.STORAGE ensures that it is repeated until is complete. The completeness criteria includes the cryptographic checksum protecting the data from unauthorised deletion and modification.
- [FPT_FLS.1.1]

(7) TSF.STORAGE stores the security attributes for Tachograph Card *User ID* for inserted Tachograph Cards.
- [FIA_ATD.1.1(1:TC)]

(8) Restrict functionality and data at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_MSA.3.1(3:DAT), FMT_MSA.3.2(3:DAT)]

10.17. TSF.SPEED

TSF.SPEED controls all secure communication with motion sensor. Ensures that a secure communication channel exists and is used for communication. Detect Motion sensor related events. Control initialization of motion sensor communication. Ensure that events/faults reported by motion sensor is stored within VU.

(1) Reports events and faults to TSF.ERRORMGR:
- [FAU_GEN.1.1]

(1.1) *Vehicle motion conflict*
(1.2) *Motion data error*
(1.3) *Security breach attempt* due to [*Unauthorised change of motion sensor*, *Motion sensor authentication failure*, *Motion sensor stored data integrity error*, and *Sensor no further details*]
(1.4) *Recording equipment fault* due to [*Sensor fault*]

(2) Handles pairing, authentication, and re-authentication of the Motion Sensor using TSF.CRYPTO for all cryptographic operations. Detects when 3 consecutive unsuccessful authentication attempts have occurred, report the authentication failure to TSF.ERRORMGR and continues to use the motion data sent by the Motion Sensor (ignoring any security attributes).
TSF.SPEED relies on TSF.CRYPTO to detect and prevent use of forged or copied authentication data.
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS), FIA_AFL.1.1(3:MS), FIA_AFL.1.2(3:MS), FIA_UAU.3.1, FIA_UAU.3.2, FIA_UAU.2.1(1:MS)]

(3) TSF.SPEED identifies the Motion Sensor through its *serial number*, *approval number* and the *pairing date* from the pairing data.These security attributes are established during pairing/authentication and are maintained and used for secure messaging with the Motion Sensor.
- [FMT_SMR.1.1, FMT_SMR.1.2, FIA_ATD.1.1(2:MS)]

(4) Handles secure messaging in normal operation with the Motion Sensor, using TSF.CRYPTO for all cryptographic operations. The secure messaging is only available after a successful pairing and authentication of a Motion Sensor and secure messaging is only available to the last paired Motion Sensor. When a motion data integrity or authenticity error is detected, reports the event to TSF.ERRORMGR and continues to use the motion data sent by the Motion Sensor (ignoring any security attributes).
- [FDP_ITC.2.1, FDP_ITC.2.2, FDP_ITC.2.3, FDP_ITC2.4, FDP_ITC.2.5, FIA_UAU.2.1(1:MS), FPT_TDC.1.1(1), FPT_TDC.1.2(1)]

(5) All communication requires TSF.SPEED to initiate the communication according to 0. TSF.SPEED provides the logical channel for communication with the Motion Sensor and uses TSF.CRYPTO to handle confidentiality, integrity, and authenticity of all data transferred over that channel.
- [FTP_ITC.1.1(1:MS), FTP_ITC.1.2(1:MS), FTP_ITC.1.3(1:MS)]

(6) Monitors motion data to enforce the [Input Sources SFP] by comparing motion data input without security attributes against motion data imported with security attributes from the Motion Sensor. Motion data is further validated against GNSS data based on vehicle speed. If any inconsistency is detected, *Motion data integrity error* is reported to TSF.ERRORMGR.
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS), FDP_SDI.2.1(2), FDP_SDI2.2(2), FDP_ITC.2.1, FDP_ITC.2.2, FDP_ITC.2.3, FDP_ITC2.4, FDP_ITC.2.5]

(7) TSF.SPEED implicitly tests the communication link to the Motion Sensor by continuously performing secure messaging over the link starting when it is first activated.
- [FPT_TST.1.1]

(8) Restrict functionality at start-up and allow nobody to override the initial values.
- [FMT_MSA.3.1(5:IS), FMT_MSA.3.2(5:IS)]

10.18. TSF.TAM

TSF.TAM synchronise the system and keep control of mode of operation to ensure that all relevant data are stored and functions are enabled/disabled

(1) Detects *Recording equipment fault* [*Download fault*] and reports the event to TSF.ERRORMGR.
- [FAU_GEN.1.1]

(2) Controls mode of operation based on inserted Tachograph Cards and provides this information to other TSFs. The information is used to ensure access to functions and data.
- [FDP_ACC.1.1(2:FUN), FDP_ACF.1.1(2:FUN), FDP_ACF.1.2(2:FUN), FDP_ACF.1.3(2:FUN), FMT_MOF.1.1(2), FMT_MOF.1.1(3), FMT_MOF.1.1(4), FMT_MOF.1.1(5)]

(3) Initiates Motion Sensor pairing in calibration mode when there is no currently paired Motion Sensor, or when a Motion Sensor different from the currently paired Motion Sensor is detected.

- [FDP_ACC.1.1(5:IS) FDP_ACF.1.1(5:IS) FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS)]

(4) Initiates re-authentication of Tachograph Cards after power supply interruptions and other resets.
- [FIA_UAU.6.1]

(5) Controlls data export to printer and download so no personal identification45 or card number46 are outputted unless they correspond to an inserted tachograph card. When no card is inserted driver related data shall be output relating only to the current and previous 8 calendar days
- [FDP_ACC.1.1(4:UDE), FDP_ACF.1.1(4:UDE), FDP_ACF.1.4(4:UDE)]

(6) Restrict functionality and data at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(2:FUN), FMT_MSA.3.2(2:FUN), FMT_MSA.3.1(4:UDE), FMT_MSA.3.2(4:UDE)]

10.19. TSF.TIME

TSF.TIME provides the VU with a correct time.

(1) Detects *Time conflict* event (too large deviation between internal clock and time supplied by the GNSS receiver) and reports the event to TSF.ERRORMGR.
- [FAU_GEN.1.1]

(2) Provides a reliable time source for current time, as UTC date and time. The current time is automatically adjusted once every 12 hours based on time received from the GNSS receiver, or triggered in calibration mode.
- [FPT_STM.1.1]

(3) Monitors RTC data to enforce the [Input Sources SFP] by comparing internal RTC data against GNSS time. If any inconsistency is detected, *Time conflict* event is reported to TSF.ERRORMGR.
- [FDP_ACC.1.1(5:IS), FDP_ACF.1.1(5:IS), FDP_ACF.1.2(5:IS), FDP_ACF.1.3(5:IS)]

(4) Restrict functionality at start-up and allow nobody to override the initial values
- [FMT_MSA.3.1(5:IS), FMT_MSA.3.2(5:IS)]

10.20. SFR Coverage

SFR	Covered by TSS location	
Class FAU Security audit		
FAU_GEN.1.1	TSF.ACTIVITIES	(1)
	TSF.BIST	(1)
	TSF.CARD	(1), (8)
	TSF.DSRC	(1)
	TSF.DOWNLOAD	(1)
	TSF.ERRORMGR	(1)
	TSF.FRAMEWORK	(5)
	TSF.GNSS	(1)
	TSF.MMI	(1)
	TSF.PSI	(1)
	TSF.STORAGE	(1)
	TSF.SPEED	(1)
	TSF.TAM	(1)
	TSF.TIME	(1)
FAU_GEN.1.2	TSF.ERRORMGR	(1)
	TSF.STORAGE	(1)
FAU_SAR.1.1	TSF.DOWNLOAD	(3)
	TSF.MMI	(2)
FAU_SAR.1.2	TSF.DOWNLOAD	(3)
	TSF.MMI	(2)
FAU_STG.1.1	TSF.STORAGE	(1), (3)

[45] Personal identification (surname and first name) shall be blanked.
[46] Card number shall be partially blanked (every odd character).

SFR	Covered by TSS location	
FAU_STG.1.2	TSF.DOWNLOAD TSF.STORAGE	(2) (3)
FAU_STG.4.1	TSF.STORAGE	(2)
Class FCO Communication		
FCO_NRO.1.1	TSF.DSRC TSF.DOWNLOAD	(2) (5)
FCO_NRO.1.2	TSF.CRYPTO	(5)
FCO_NRO.1.3	TSF.DSRC TSF.DOWNLOAD	(2) (5)
Class FDP User protection		
FDP_ACC.1.1(1:FIL)	TSF.FRAMEWORK	(4)
FDP_ACF.1.1(1:FIL)	TSF. FRAMEWORK	(4)
FDP_ACF.1.2(1:FIL)	TSF. FRAMEWORK	(4)
FDP_ACF.1.3(1:FIL)	TSF. FRAMEWORK	(4)
FDP_ACF.1.4(1:FIL)	TSF. FRAMEWORK	(4)
FDP_ACC.1.1(2:FUN)	TSF.ACTIVITIES TSF.CARD TSF.CONFIG TSF.DOWNLOAD TSF.MMI TSF.STORAGE TSF.TAM	(2) (9) (1) (7) (3) (5) (2)
FDP_ACF.1.1(2:FUN)	TSF.ACTIVITIES TSF.CARD TSF.CONFIG TSF.DOWNLOAD TSF.MMI TSF.STORAGE TSF.TAM	(2) (9) (1) (7) (3) (5) (2)
FDP_ACF.1.2(2:FUN)	TSF.ACTIVITIES TSF.CARD TSF.CONFIG TSF.DOWNLOAD TSF.MMI TSF.STORAGE TSF.TAM	(2), (4) (9) (1) (7) (3) (5) (2)
FDP_ACF.1.3(2:FUN)	TSF.ACTIVITIES TSF.CARD TSF.CONFIG TSF.MMI TSF.STORAGE TSF.TAM	(2), (4) (9) (1) (3) (5) (2)
FDP_ACF.1.4(2:FUN)	TSF.CARD	(11)
FDP_ACC.1.1(3:DAT)	TSF.BIST TSF.CRYPTO TSF.DOWNLOAD TSF.MMU TSF.STORAGE	(2), (3) (2) (2) (1) (1), (2), (3), (4)
FDP_ACF.1.1(3:DAT)	TSF.BIST TSF.CRYPTO TSF.DOWNLOAD TSF.MMU TSF.STORAGE	(2), (3) (2) (2) (1) (1), (2), (3), (4)

SFR	Covered by TSS location	
FDP_ACF.1.2(3:DAT)	TSF.BIST	(2), (3)
	TSF.CRYPTO	(2)
	TSF.DOWNLOAD	(2)
	TSF.MMU	(1)
	TSF.STORAGE	(1), (2), (3), (4)
FDP_ACF.1.3(3:DAT)	TSF.BIST	(2), (3)
	TSF.CRYPTO	(2)
	TSF.DOWNLOAD	(2)
	TSF.MMU	(1)
	TSF.STORAGE	(1), (2), (3), (4)
FDP_ACF.1.4(3:DAT)	TSF.CRYPTO	(2)
FDP_ACC.1.1(4:UDE)	TSF.ACTIVITIES	(3)
	TSF.CONFIG	(3)
	TSF.DSRC	(2)
	TSF.DOWNLOAD	(4)
	TSF.ERRORMGR	(1)
	TSF.MMI	(4)
	TSF.STORAGE	(4)
	TSF.TAM	(5)
FDP_ACF.1.1(4:UDE)	TSF.ACTIVITIES	(3)
	TSF.CONFIG	(3)
	TSF.DSRC	(2),
	TSF.DOWNLOAD	(4)
	TSF.ERRORMGR	(1)
	TSF.MMI	(4)
	TSF.STORAGE	(4)
	TSF.TAM	(5)
FDP_ACF.1.2(4:UDE)	TSF.ACTIVITIES	(3)
	TSF.DSRC	(2)
	TSF.ERRORMGR	(1)
	TSF.STORAGE	(4)
FDP_ACF.1.3(4:UDE)	TSF.CONFIG	(3)
FDP_ACF.1.4(4:UDE)	TSF.DOWNLOAD	(4)
	TSF.MMI	(4)
	TSF.TAM	(5)
FDP_ACC.1.1(5:IS)	TSF.CARD	(3), (4)
	TSF.CASING	(2)
	TSF.CONFIG	(2)
	TSF.IPC	(1)
	TSF.SPEED	(2), (6)
	TSF.TAM	(3)
	TSF.TIME	(3)
FDP_ACF.1.1(5:IS)	TSF.CARD	(3), (4)
	TSF.CASING	(2)
	TSF.CONFIG	(2)
	TSF.IPC	(1)
	TSF.SPEED	(2), (6)
	TSF.TAM	(3)
	TSF.TIME	(3)
FDP_ACF.1.2(5:IS)	TSF.CARD	(3), (4)
	TSF.CASING	(2)
	TSF.CONFIG	(2)
	TSF.SPEED	(2), (6)
	TSF.TAM	(3)
	TSF.TIME	(3)

SFR	Covered by TSS location	
FDP_ACF.1.3(5:IS)	TSF.CARD TSF.CASING TSF.CONFIG TSF.SPEED TSF.TAM TSF.TIME	(3), (4) (2) (2) (2), (6) (3) (3)
FDP_ACF.1.4(5:IS)	TSF.IPC	(1)
FDP_ETC.2.1	TSF.CARD TSF.DOWNLOAD	(8) (5)
FDP_ETC.2.2	TSF.CARD TSF.DOWNLOAD	(8) (5)
FDP_ETC.2.3	TSF.CARD TSF.DOWNLOAD	(8) (5)
FDP_ETC.2.4	TSF.CARD TSF.DOWNLOAD	(8) (5)
FDP_ITC.1.1	TSF.CASING TSF.CONFIG	(2) (2)
FDP_ITC.1.2	TSF.CASING TSF.CONFIG	(2) (2)
FDP_ITC.1.3	TSF.CASING TSF.CONFIG	(2) (2)
FDP_ITC.2.1	TSF.CARD TSF.SPEED	(8) (4), (6)
FDP_ITC.2.2	TSF.CARD TSF.SPEED	(8) (4), (6)
FDP_ITC.2.3	TSF.CARD TSF.SPEED	(8) (4), (6)
FDP_ITC.2.4	TSF.CARD TSF.SPEED	(8) (4), (6)
FDP_ITC.2.5	TSF.CARD TSF.IPC TSF.SPEED	(8) (1) (4), (6)
~~FDP_ITT.1.1~~		
FDP_RIP.1.1	TSF.CARD TSF.CRYPTO	(3), (10) (13)
FDP_SDI.2.1(1)	TSF.DOWNLOAD	(2)
FDP_SDI.2.2(1)	TSF.DOWNLOAD	(1)
FDP_SDI.2.1(2)	TSF.SPEED	(6)
FDP_SDI.2.2(2)	TSF.SPEED	(6)
Class FIA Identification and authentication		
FIA_AFL.1.1(1:TCL)	TSF.CARD	(5)
FIA_AFL.1.2(1:TCL)	TSF.CARD TSF.ERRORMGR TSF:MMI	(5) (1) (1)
FIA_AFL.1.1(2:TCR)	TSF.CARD	(6)
FIA_AFL.1.2(2:TCR)	TSF.CARD TSF.CONFIG	(6) (4)
FIA_AFL.1.1(3:MS)	TSF.SPEED	(2)
FIA_AFL.1.2(3:MS)	TSF.ERRORMGR TSF.MMI TSF.SPEED	(1) (1) (2)
FIA_ATD.1.1(1:TC)	TSF.CARD TSF.STORAGE	(3), (4) (7)

SFR	Covered by TSS location	
FIA_UAU.3.1	TSF.CARD TSF.CRYPTO TSF.SPEED	(3), (4) (9) (2)
FIA_UAU.3.2	TSF.CARD TSF.CRYPTO TSF.SPEED	(3), (4) (9) (2)
FIA_UAU.5.1	TSF.CARD	(3)
FIA_UAU.5.2	TSF.CARD	(3)
FIA_UAU.6.1	TSF.CARD TSF.TAM	(7) (4)
FIA_UID.2.1	TSF.CARD	(3), (4)
Class FMT Security management		
FMT_MSA.1.1	TSF.CARD	(14)
FMT_MSA.3.1(1:FIL)	TSF.FRAMEWORK	(4)
FMT_MSA.3.2(1:FIL)	TSF.FRAMEWORK	(4)
FMT_MSA.3.1(2:FUN)	TSF_ACTIVITIES TSF.CARD TSF.CONFIG TSF.DOWNLOAD TSF.MMI TSF.STORAGE TSF.TAM	(5) (14) (5) (8) (7) (8) (6)
FMT_MSA.3.2(2:FUN)	TSF_ACTIVITIES TSF.CARD TSF.CONFIG TSF.DOWNLOAD TSF.MMI TSF.STORAGE TSF.TAM	(5) (14) (5) (8) (7) (8) (6)
FMT_MSA.3.1(3:DAT)	TSF.CRYPTO TSF.MMU TSF.STORAGE	(12) (4) (8)
FMT_MSA.3.2(3:DAT)	TSF.CRYPTO TSF.MMU TSF.STORAGE	(12) (4) (8)
FMT_MSA.3.1(4:UDE)	TSF.CARD TSF.CONFIG TSF.DSRC TSF.DOWNLOAD TSF.MMI TSF.TAM	(14) (5) (4) (8) (7) (6)
FMT_MSA.3.2(4:UDE)	TSF.CARD TSF.CONFIG TSF.DSRC TSF.DOWNLOAD TSF.MMI TSF.TAM	(14) (5) (4) (8) (7) (6)
FMT_MSA.3.1(5:IS)	TSF.CARD TSF.CONFIG TSF.IPC TSF.SPEED TSF.TIME	(14) (5) (2) (8) (4)

SFR	Covered by TSS location	
FMT_MSA.3.2(5:IS)	TSF.CARD TSF.CONFIG TSF.IPC TSF.SPEED TSF.TIME	(14) (5) (2) (8) (4)
FMT_MOF.1.1(1)	TSF.CRYPTO TSF.FRAMEWORK	(11) (1)
FMT_MOF.1.1(2)	TSF.CONFIG TSF.MMI TSF.TAM	(1) (5) (2)
FMT_MOF.1.1(3)	TSF.ACTIVITIES TSF.TAM	(2) (2)
FMT_MOF.1.1(4)	TSF.ACTIVITIES TSF.CONFIG TSF.MMI TSF.TAM	(2) (1) (6) (2)
FMT_MOF.1.1(5)	TSF.TAM	(2)
FMT_MTD.1.1	TSF.CONFIG	(1)
FMT_SMF.1.1	TSF.ACTIVITIES TSF.CONFIG TSF.DOWNLOAD	(2), (4) (1) (4)
FMT_SMR.1.1	TSF.CARD TSF.SPEED	(3), (4) (3)
FMT_SMR.1.2	TSF.CARD TSF.SPEED	(3), (4) (3)
Class FPT Protection of the TSF		
FPT_FLS.1.1	TSF.CARD TSF.CRYPTO TSF.FRAMEWORK TSF.PSI TSF.STORAGE	(12) (14) (2), (3) (1), (3) (6)
FPT_PHP.2.1	TSF.CASING	(1)
FPT_PHP.2.2	TSF.CASING	(1)
FPT_PHP.2.3	TSF.ERRORMGR TSF:MMI TSF.PSI	(1) (1) (1)
FPT_PHP.3.1	TSF.BIST TSF.CRYPTO TSF.MMU TSF.PSI	(4) (14) (2) (1)
FPT_STM.1.1	TSF.TIME	(1)
FPT_TST.1.1	TSF.BIST TSF.CARD TSF.DSRC TSF.DOWNLOAD TSF.ERRORMGR TSF.SPEED	(5) (13) (3) (6) (2) (7)
FPT_TST.1.2	TSF.BIST TSF.DOWNLOAD	(1) (1)
FPT_TST.1.3	TSF.BIST	(1)
Class FTP Trusted path/channels		
FTP_ITC.1.1(1:MS)	TSF.SPEED	(5)
FTP_ITC.1.2(1:MS)	TSF.SPEED	(5)

SFR	Covered by TSS location	
FTP_ITC.1.3(1:MS)	TSF.SPEED	(5)
Class FCS Cryptographic support (2nd generation Tachograph Cards/Motion Sensor)		
FCS_CKM.1.1(1)	TSF.CRYPTO	(1), (5), (10)
FCS_CKM.2.1(1)	TSF.CRYPTO	(5), (10)
FCS_CKM.4.1(1)	TSF.CRYPTO	(2)
FCS_COP.1.1(1:AES)	TSF.CRYPTO	(3)
FCS_COP.1.1(2:SHA2)	TSF.CRYPTO	(4)
FCS_COP.1.1(3:ECC)	TSF.CRYPTO	(5)
FCS_RNG.1.1	TSF.CRYPTO	(1)
FCS_RNG.1.2	TSF.CRYPTO	(1)
Class FIA Identification and authentication (2nd generation Tachograph Cards/Motion Sensor)		
FIA_ATD.1.1(2:MS)	TSF.CRYPTO TSF.SPEED	(2) (3)
FIA_UAU.1.1(1:TC)	TSF.CARD	(2)
FIA_UAU.1.2(1:TC)	TSF.CARD	(3)
FIA_UAU.2.1(1:MS)	TSF.CRYPTO TSF.SPEED	(15) (2), (4)
Class FPT Protection of the TSF (2nd generation Tachograph Cards/Motion Sensor)		
FPT_TDC.1.1(1)	TSF.CARD TSF.SPEED	(8) (4)
FPT_TDC.1.2(1)	TSF.CARD TSF.SPEED	(8) (4)
Class FDP FTP (2nd generation Tachograph Cards)		
FTP_ITC.1.1(2:TC)	TSF.CARD	(8)
FTP_ITC.1.2(2:TC)	TSF.CARD	(8)
FTP_ITC.1.3(2:TC)	TSF.CARD	(8)
Class FCS Cryptographic support (1st generation Tachograph Cards)		
FCS_CKM.1.1(2)	TSF.CRYPTO	(10)
FCS_CKM.2.1(2)	TSF.CRYPTO	(10)
FCS_CKM.4.1(2)	TSF.CRYPTO	(2)
FCS_COP.1.1(4:TDES)	TSF.CRYPTO	(6)
FCS_COP.1.1(5:RSA)	TSF.CRYPTO	(7)
FCS_COP.1.1(6:SHA-1)	TSF.CRYPTO	(8)
Class FIA Identification and authentication (1st generation Tachograph Cards)		
FIA_UAU.1.1(2:TC)	TSF.CARD	(2)
FIA_UAU.1.2(2:TC)	TSF.CARD	(4)
Class FPT Protection of the TSF (1st generation Tachograph Cards)		
FPT_TDC.1.1(2)	TSF.CARD	(8)
FPT_TDC.1.2(2)	TSF.CARD	(8)
Class FTP Trusted path/channels (1st generation tachograph Cards)		
FTP_ITC.1.1(4:TC)	TSF.CARD	(8)
FTP_ITC.1.2(4:TC)	TSF.CARD	(8)
FTP_ITC.1.3(4:TC)	TSF.CARD	(8)

11. COMPOSITE TOE

The SE5000 is a composite TOE as it utilizes the platform *"Infineon Security Controller M7893 B11 with RSA2048/4096 v2.03.008, EC v2.03.008 and with specific IC dedicated software (firmware)"* to fulfil its obligations.

11.1. Statement of Compatibility between Composite ST and Platform ST

11.1.1. Compatibility of Security Assurance Measures

- The assurance level for the platform is, according to reference [19], EAL 6 augmented with ALC_FLR.1.
- The assurance level for the composite TOE is EAL 4 augmented with ATE_DPT.2 and AVA_VAN.5.

The assurance level of the platform covers the assurance level of the composite TOE.

11.1.2. Relevant Platform TSFs

The table below shows that all platform TSFs stated in reference [16] are relevant for the composite TOE.

Platform TSF	Platform SFR	Composite TOE utilization of platform TSF	Composite TOE SFR
SF_DPM :Device Phase management	FAU_SAS.1 FMT_LIM.1 FMT_LIM.2 FDP_ACC.1 FDP_ACF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FPT_PHP.3 ~~FDP_ITT.1~~ FPT_ITT.1	- Protection against re-activation of test points etc. needed and used during manufacturing. - Execution of self-tests at initial start-up and during normal operation.	FMT_MOF.1(1) FPT_TST.1
SF_PS :Protection against Snooping	FPT_PHP.3 FDP_IFC.1 FPT_ITT.1 ~~FDP_ITT.1~~ FPT_FLS.1	- Protection against SW debug or analysis after VU activation. - Protection against entrance of executable code from external sources.	FPT_PHP.3 FDP_ACC.1(5:IS) FDP_ACF.1(5:IS)
SF_PMA :Protection against Modifying Attacks	FPT_PHP.3 FDP_IFC.1 FPT_ITT.1 ~~FDP_ITT.1~~ FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FDP_ACC.1 FDP_ACF.1 FRU_FLT.2 FPT_TST.2 FDP_SDI.1 FDP_SDI.2 FPT_FLS.1	- Execution of self-tests at initial start-up and during normal operation. - Generation of audit records. - Preservation of secure state at failure. - Notification of physical attack. - Resistance to physical attack.	FPT_TST.1 FAU_GEN.1 FPT_FLS.1 FPT_PHP.2 FPT_PHP.3

Platform TSF	Platform SFR	Composite TOE utilization of platform TSF	Composite TOE SFR
SF_PLA :Protection against Logical Attacks	FDP_ACC.1 FDP_ACF.1 FMT_MSA.1 FMT_MSA.3 FPT_PHP.3 ~~FDP_ITT.1~~ FDP_IFC.1 FPT_FLS.1 FMT_SMF.1	- Execution of self-tests at initial start-up and during normal operation. - Generation of audit records. - Preservation of secure state at failure. - Notification of physical attack. - Resistance to physical attack.	FPT_TST.1 FAU_GEN.1 FPT_FLS.1 FPT_PHP.2 FPT_PHP.3
SF_CS :Cryptographic Support	FCS_COP.1/DES FSC_COP.1/AES FCS_COP.1/RSA FCS_CKM.1/RSA FCS_COP.1/ECDSA FCS_CKM.1/EC FCS_COP.1/ECDH FCS_COP.1/SHA-SW FCS_COP.1/SHA-2-HW FPT_PHP.3 ~~FDP_ITT.1~~ FPT_ITT.1 FPT_TST.2 FPT_FLS.1 FCS_RNG.1	- Execution of standard cryptographic operations according to AES, ECC, SHA-2, RSA and TDES. - Random number generation. - Generation of cryptographic keys.	FCS_CKM.1(1) FCS_RNG.1 FCS_COP.1(1:AES) FCS_COP.1(2:SHA-2) FCS_COP.1(3:ECC) FCS_CKM.1(2) FCS_COP.1(4:TDES) FCS_COP.1(5:RSA)

11.1.3. Compatibility of Security Functional Requirements

The following table lists the SFRs stated in the Public ST for the Infineon Security Controller M7893 B11 (ref. [16]). The table shows whether a platform requirement is relevant or irrelevant for the composite TOE, i.e. whether the functionality implemented by a platform SFR is actually used or not by the composite TOE. Also, the table provides links between the relevant platform SFRs and the composite TOE SFRs when existing.

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FRU_FLT.2	**Limited fault tolerance** The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).*	SF_PMA	X		FPT_TST.1
FPT_FLS.1	**Failure with preservation of secure state** The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur*.	SF_PS SF_PMA SF_PLA SF_CS	X		FPT_FLS.1
FMT_LIM.1	**Limited capabilities** The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with *"Limited availability (FMT_LIM.2)"* the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*	SF_DPM	X		None
FMT_LIM.2	**Limited availability** The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with *"Limited capabilities (FMT_LIM.1)"* the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*	SF_DPM	X		FMT_MOF.1(1)
FAU_SAS.1	**Audit Storage** The TSF shall provide the test process *before TOE Delivery* with the capability to store *the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software* in the *not changeable configuration page area and non-volatile memory.*	SF_DPM	X		None

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FPT_PHP.3	**Resistance to physical attack** The TSF shall resist *physical manipulation and physical probing* to the *TSF* by responding automatically such that the SFRs are always enforced.	SF_DPM SF_PS SF_PMA SF_PLA SF_CS	X		FPT_PHP.3
~~FDP_ITT.1~~	~~Basic internal transfer protection~~ ~~The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.~~	~~SF_DPM~~ ~~SF_PS~~ ~~SF_PMA~~ ~~SF_PLA~~ ~~SF_CS~~	~~X~~		~~FPT_PHP.3~~
FPT_ITT.1	**Basic internal TSF data transfer protection** The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.	SF_DPM SF_PS SF_PMA SF_CS	X		FPT_PHP.3
FDP_IFC.1	**Subset information flow control** The TSF shall enforce the *Data Processing Policy* on *all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.*	SF_PS SF_PMA SF_PLA	X		FPT_PHP.3
FPT_TST.2	**Subset TOE testing** The TSF shall run a suite of self tests *at the request of the authorized user* to demonstrate the correct operation of the *alarm lines and/or following environmental sensor mechanisms:* - *The information is given in the confidential Security Target.*	SF_PMA SF_CS	X		FPT_TST.1
FDP_ACC.1	**Subset access control** The TSF shall enforce the *Memory Access Control Policy on all subjects (software running at the defined and assigned privilege levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. privilege levels.*	SF_DPM SF_PMA SF_PLA	X		None

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FDP_ACF.1	**Security attribute based access control** The TSF shall enforce the Memory Access Control Policy to objects based on the following: Subject: - software running at the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines. - software running at the privilege levels containing the application software Object: - data including code stored in memories Attributes: - the memory area where the access is performed to and/or the operation to be performed. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information of the relevant memory range before, during or after the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation.* The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.* The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*	SF_DPM SF_PMA SF_PLA	X		None
FMT_MSA.1	**Management of security attributes** The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *change default, modify or delete* the security attributes *permission control information to the software running on the privilege levels.*	SF_DPM SF_PMA SF_PLA	X		None
FMT_MSA.3	**Static attribute initialisation** The TSF shall enforce the *Memory Access Control Policy* to provide *well defined* default values for security attributes that are used to enforce the SFP. The TSF shall allow *any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed,* to specify alternative initial values to override the default values when an object or information is created.	SF_DPM SF_PMA SF_PLA	X		None

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FMT_SMF.1	**Specification of management functions** The TSF shall be capable of performing the following security management functions: *access the configuration registers of the MMU.*	SF_DPM SF_PMA SF_PLA	X		None
FCS_COP.1/ DES	**Cryptographic operation** The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)* with cryptographic key sizes *of 2 x 56 bit or 3 x 56 bit,* that meet the following *standards:* *National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*	SF_CS	X		FCS_COP.1(4:TDES)
FCS_COP.1/ AES	**Cryptographic operation** The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* and cryptographic key sizes *of 128 bit or 192 bit or 256 bit* that meet the following *standards:* *U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197*	SF_CS	X		FCS_COP.1(1:AES)

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FCS_COP.1/ RSA	**Cryptographic operation** The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes *1976 - 4096 bits* that meet the following *standards* *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 < 2^{2048}* *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 < 2^{2048}* *Signature Verification:* *According to section 5.2.2 RSAVP1 in PKCS v2.1 RFC3447, without 5.2.2.1.*	SF_CS	X		FCS_COP.1(5:RSA)[47]

[47] TBD – Reference showing that platform SFR and composite TOE SFR are compatible.

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FCS_COP.1/ ECDSA	**Cryptographic operation** The TSF shall perform *signature generation and signature verification* in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* *Signature Generation:* *1. According to section 7.3 in ANSI X9.62 - 2005 Not implemented is step d) and e) thereof. The output of step e) has to be provided as input to our function by the caller. Deviation of step c) and f): The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.* *2. According to sections 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002 Not implemented is section 6.2.1: The output of 5.4.2 has to be provided by the caller as input to the function.* *Signature Verification:* *1. According to section 7.4.1 in ANSI X9.62–2005 Not implemented is step b) and c) thereof. The output of step c) has to be provided as input to our function by the caller. Deviation of step d): Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.* *2. According to sections 6.4 (6.4.1. + 6.4.3 + 6.4.4) in ISO/IEC 15946-2:2002 Not implemented is section 6.4.2: The output of 5.4.2 has to be provided by the caller as input to the function.*	SF_CS	X		FCS_COP.1(3:ECC)
FCS_COP.1/ ECDH	**Cryptographic operation** The TSF shall perform *elliptic curve Diffie-Hellman key agreement* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* *1. According to section 5.4.1 in ANSI X9.63 -2001: Unlike section 5.4.1.3 our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and y-coordinate.* *2. According to sections 8.4.2.1, 8.4.2.2, 8.4.2.3, and 8.4.2.4 in ISO/IEC 15946-3:2002:* *The function enables the operations described in the four sections.*	SF_CS	X		FCS_COP.1(3:ECC)

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FCS_COP.1/ SHA-SW	**Cryptographic operation** The TSF shall perform *hash-value calculation of user chosen data* in accordance with a specified cryptographic algorithm *SHA-2* and with cryptographic key sizes *of none* that meet the following *standards:* *U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256 and section 6.4 SHA-512.*	SF_CS	X		FCS_COP.1(2:SHA-2)
FCS_COP.1/ SHA-2-HW	**Cryptographic operation** The TSF shall perform *hash-value calculation of user chosen data* in accordance with a specified cryptographic algorithm *SHA-2* and with cryptographic key sizes *of none* that meet the following *standards:* *U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256.*	SF_CS		X	
FCS_CKM.1/ RSA	**Cryptographic key generation** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *rsagen1 (PKCS v2.1 RFC3447)* and specified cryptographic key sizes *of 1976 – 4096 bits* that meet the following *standard:* *According to section 3.2(2) in PKCS v2.1 RFC3447, for u=2, i.e., without any (r_i, d_i, t_i), i > 2. For p x q < 2^{2048} additionally according to section 3.2(1).*	SF_CS		X	
FCS_CKM.1/ EC	**Cryptographic key generation** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002* and specified cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* *ECDSA Key Generation:* *1. According to the appendix A4.3 in ANSI X9.62-2005 the cofactor h is not supported.* *2. According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002*	SF_CS	X		FCS_CKM.1(1)

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FDP_SDI.1	**Stored data integrity monitoring** The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC values for certain memories.*	SF_PMA	X		FDP_SDI.2(1)
FDP_SDI.2	**Stored data integrity monitoring and action** The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one- and/or more-bit-errors* on all objects, based on the following attributes: *corresponding EDC value for the memories and error correction for the SOLID FLASH™ NVM.* Upon detection of a data integrity error, the TSF shall correct 1 bit errors in the SOLID FLASH™ NVM automatically and inform the user about more bit errors.	SF_PMA	X		None

Platform SFR ID	Platform SFR	Platform TSF	Relevant	Irrelevant	Composite TOE SFRs
FCS_RNG.1	**Random Number Generation** 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 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.* *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 continuously. 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.* The TSF shall provide *numbers in the format 8- or 16-bit* that meet *PTG.2.6* *Test procedure A, as defined in [7] 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.*	SF_CS	X		FCS_RNG.1

11.1.4. Compatibility of Security Objectives

The security objectives for the platform TOE are stated in ref. [16] and summarized in the following list:

- O.Phys-Manipulation Protection against Physical Manipulation
- O.Phys-Probing Protection against Physical Probing
- O.Malfunction Protection against Malfunction
- O.Leak-Inherent Protection against Inherent Information Leakage
- O.Leak-Forced Protection against Forced Information Leakage
- O.Abuse-Func Protection against Abuse of Functionality
- O.Identification TOE Identification
- O.RND Random Numbers
- O.Add-Functions Additional specific security functionality
- O.Mem-Access Area based Memory Access Control

These objectives focus on self-protection of the platform, protection of stored data, protection of processed data and on support functions, e.g. cryptography and random number generation. The security objectives for the composite TOE, see chapter 7.1, are defined at an entirely different level, i.e. the smart tachograph application.

All the security objectives for the platform do contribute to the smart tachograph security objectives and do harden the smart tachograph security functionality in the end. Hence the security objectives for the platform and the security objectives for the composite TOE are in no contradiction.

11.1.5. Compatibility of Threats

The threats for the platform TOE are stated in ref. [16] and summarized in the following list:

- T.Phys-Manipulation Physical Manipulation
- T.Phys-Probing Physical Probing
- T.Malfunction Malfunction due to Environmental Stress
- T.Leak-Inherent Inherent Information Leakage
- T.Leak-Forced Forced Information Leakage
- T.Abuse-Func Abuse of Functionality
- T.RND Deficiency of Random Numbers
- T.Mem-Access Memory Access Violation

These threats are all related to attacks addressing the platform physically, to make some processing in the platform fail, or to abuse specific functionality of the platform. The threats and OSPs for the composite TOE, see chapters 6.2 and 6.4, are defined at an entirely different level, i.e. the smart tachograph application.

All threats for the platform are somehow sub-aspects of the smart tachograph threats. Furthermore, the threats for the platform address the fact that security functionality of the composite TOE could be modified or deactivated by attacking the platform using physical means. Hence the threats for the platform and the threats and OSPs for the composite TOE are in no contradiction.

11.1.6. Compatibility of Organisational Security Policies

The OSPs defined for the platform TOE are stated in ref. [16] and summarized in the following list:

- P.Process-TOE Protection during TOE Development and Production
- P.Add-Functions Additional Specific Security Functionality

P.Process-TOE is met by a security objective or the development and production environment for the platform and cannot contradict to any OSP or threat for the composite TOE.

The OSP P.Add-Functions requires the platform TOE to implement specific cryptographic functions as service functionality to the embedded software of the composite TOE, which actually uses several of the required cryptographic algorithms in its own smart tachograph functionality. Hence the OSPs for the platform are in no contradiction to the threats and OSPs of the composite TOE.

11.1.7. Compatibility of Assumptions

The assumptions about the operational environment of the platform TOE are stated in ref. [16]. This chapter shows the relevance of these assumptions for the composite TOE.

A.Process-Sec-IC Protection during Packaging, Finishing and Personalization

Categorisation: *The assumption is automatically fulfilled*

This assumption is relevant for the composite ST. It will automatically be fulfilled by application of the security assurance requirements concerning development security and delivery procedure.

Though there is no dedicated security objective for the composite TOE to which this assumption can be mapped, application of the security assurance requirements concerning development security and delivery procedure integrally contributes to the achievement of all composite TOE security objectives.

A.Plat-Appl Usage of Hardware Platform

Categorisation: *The assumption is automatically fulfilled*

This assumption is relevant for the Composite-ST. It has to be respected by the SW developer of the composite TOE. It will automatically be fulfilled by application of the security assurance requirements concerning TOE construction (detailed design and implementation).

Though there is no dedicated security objective for the composite TOE to which this assumption can be mapped, application of the security assurance requirements concerning TOE construction (detailed design and implementation) integrally contributes to the achievement of all composite TOE security objectives.

A.Resp-Appl Treatment of User Data

Categorisation: *The assumption is automatically fulfilled*

This assumption is relevant for the composite ST. It can be mapped to the following security objectives for the composite TOE:

- O.Access
- O.Output

Hence, the composite TOE will automatically fulfil this assumption.

A.Key-Function Usage of Key-dependent Functions

Categorisation: *The assumption is automatically fulfilled*

This assumption is relevant for the composite ST. It can be mapped to the following security objective for the composite TOE:

- O.Output

Hence, the composite TOE will automatically fulfil this assumption.

The above statements shows that none of the assumptions for the platform TOE stated in ref. [16] are significant for the operational phase of the composite TOE.

11.1.8. Compatibility of Security Objectives for the Operational Environment

The security objectives for the operational environment of the platform TOE are stated in ref. [16] and summarized in the following list:

- OE.Plat-Appl Usage of Hardware Platform
- OE.Resp-Appl Treatment of User Data
- OE.Process-Sec-IC Protection during composite product manufacturing

The security objectives for the operational environment OE.Plat-Appl and OE.Resp-Appl address different aspects of the development of the embedded software and will therefore be automatically regarded in the evaluation of the composite TOE.

The security objective for the operational environment OE.Process-Sec-IC is relevant for the composite ST. OE.Process-Sec-IC is covered by the following security objectives for the operational environment of the composite TOE:

- OE.Manufacturing
- OE.Data_Generation
- OE.Data_Transport
- OE.Delivery
- OE.Test_Points

12. APPENDIX A – CRYPTOGRAPHIC MECHANISMS

The cryptographic mechanisms and their purpose related to this ST and [5] are listed in Table 18, Table 19, Table 20, Table 21, and Table 22 below. Note that in these tables reference [5] actually refers to reference [5] Appendix 11.

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Integrity and authenticity in certificate chain verification TOE <-> Tachograph Card (1st generation)	RSA using SHA-1	1024	[FIPS_180-4] (SHA-1), [PKCS_1] (RSA), [ISO_9796-2] (signature, modified by [5] CSM_018, CSM_019),	[5]: CSM_020	FCS_CKM.2.1(2) FCS_COP.1.1(5:RSA)
Confidentiality and authenticity for mutual authentication and key agreement TOE <-> Tachograph Card (1st generation)	RSA using SHA-1	1024	[FIPS_180-4] (SHA-1), [PKCS_1] (RSA), [ISO_9796-2] (signature, modified by [5] CSM_018), [ISO_9798-3] (mutual authentication)	[5]: CSM_020	FCS_COP.1.1(5:RSA) FCS_COP.1.1(6:SHA-1)
Data integrity and authenticity in secure messaging TOE <-> Tachograph Card (1st generation)	Retail-MAC with DES in Single-DES and two-key Triple-DES modes	112	[ANSI_X9_19] (Retail-MAC), [NIST_SP_800-67] (Triple-DES)[48]	[5]: sec. 5.3	FCS_COP.1.1(4:TDES)
Data confidentiality in secure messaging TOE <-> Tachograph Card (1st generation)	Two-key Triple-DES in CBC mode	112	[NIST_SP_800-67] (Triple-DES)[48] [ISO_10116] (CBC)	[5]: sec. 5.4	FCS_COP.1.1(4:TDES)

Table 18 - Use of cryptographic functions for backwards compatibility with 1st generation tachograph cards related to this ST and to [5] Appendix 11 Part A.

According to [5] the algorithms are suitable for confidentiality, authenticity, integrity, authentication and key agreement. An explicit validity period is not given.

[48] [NIST_SP_800-67] has superseded [FIPS_46-3], which is referred to in [5]. No changes affecting TOE implementation.

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Integrity and authenticity in certificate chain verification TOE <-> Tachograph Card (2nd generation)	ECDSA with hashing algorithm SHA-2 (for selection of SHA-2 algorithm, see Table 13)	256 to 521, see Table 23	[FIPS_180-4] (SHA-2), [FIPS_186-4] (ECDSA), [BSI_TR-03111] (data formats), [RFC_5480] (NIST curves), [RFC_5639] (Brainpool curves)	[5]: sec. 10.2.1	FCS_COP.1.1(2:SHA-2) FCS_COP.1.1(3:ECC)
Generation of ephemeral key pair for mutual authentication and key agreement TOE <-> Tachograph Card (2nd generation)	ECDSA key generation	256 to 521, see Table 23	[FIPS_186-4] (ECDSA), [BSI_TR-03111] (data formats), [RFC_5480] (NIST curves), [RFC_5639] (Brainpool curves)	[5]: CSM_76 CSM_164	FCS_CKM.1.1(1) FCS_CKM.2.1(1) FCS_COP.1.1(3:ECC)
Integrity and authenticity for mutual authentication TOE <-> Tachograph Card (2nd generation)	ECDSA with hashing algorithm SHA-2 (for selection of SHA-2 algorithm, see Table 13)	256 to 521, see Table 23	[FIPS_180-4] (SHA-2), [FIPS_186-4] (ECDSA), [BSI_TR-03111] (data formats), [RFC_5480] (NIST curves), [RFC_5639] (Brainpool curves)	[5]: CSM_173	FCS_COP.1.1(2:SHA-2) FCS_COP.1.1(3:ECC)
Key derivation of shared secret for key agreement TOE <-> Tachograph Card (2nd generation)	ECDH	256 to 521, see Table 23	[BSI_TR-03111] (ECKA-EG), [RFC_5480] (NIST curves), [RFC_5639] (Brainpool curves)	[5]: CSM_176 to CSM_180	FCS_CKM.1.1(1) FCS_CKM.2.1(1) FCS_COP.1.1(3:ECC)
Session key derivation for key agreement TOE <-> Tachograph Card (2nd generation)	Hashing algorithm SHA-2 (for selection of SHA-2 algorithm, see Table 13) and AES in CMAC mode of operation.	128 192 256	[FIPS_180-4] (SHA-2), [FIPS_197] (AES), [BSI_TR-03111] (key derivation, with changes according to [5]: CSM_179), [NIST_SP_800-38B] (CMAC)	[5]: CSM_176 to CSM_180	FCS_CKM.1.1(1) FCS_CKM.2.1(1) FCS_COP.1.1(2:SHA-2) FCS_COP.1.1(1:AES)

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Data integrity and authenticity for secure messaging TOE <-> Tachograph Card (2nd generation)	AES in CMAC mode of operation	128 192 256	[FIPS_197] (AES), [NIST_SP_800-38B] (CMAC)	[5]: sec.10.5	FCS_COP.1.1(1:AES)
Data encryption for secure messaging TOE <-> Tachograph Card (2nd generation)	AES in CBC mode of operation	128 192 256	[FIPS_197] (AES), [ISO_10116] (CBC)	[5]: sec.10.5	FCS_COP.1.1(1:AES)

Table 19 – Use of cryptographic functions for trusted channel TOE <-> 2nd generation Tachograph Card (mutual authentication, key agreement according to ECKA-EG, and secure messaging) related to this ST and to [5] Appendix 11 Part B.

According to [5] the algorithms are suitable for confidentiality, authenticity, integrity, authentication and key agreement. An explicit validity period is not given.

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Data encryption TOE <-> External DSRC Facility	AES in CBC mode of operation	128 192 256	[FIPS_197] (AES), [ISO_10116] (CBC), [ISO_9797-1] (padding)	[5]: sec. 13.1, 13.2	FCS_COP.1.1(1:AES)
Data integrity and authenticity TOE <-> External DSRC Facility	AES in CMAC mode of operation	128 192 256	[FIPS_197] (AES), [NIST_SP_800-38B] (CMAC)	[5]: sec. 13.1, 13.2	FCS_COP.1.1(1:AES)

Table 20 – Use of cryptographic functions for trusted channel TOE <-> External DSRC Facility related to this ST and to [5] Appendix 11 Part B.

According to [5] the algorithms are suitable for confidentiality, authenticity, integrity and authentication. An explicit validity period is not given.

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Confidentiality, authenticity, and integrity of data for pairing of TOE and Motion Sensor	AES in ECB and CBC mode of operation	128 192 256	[FIPS_197] (AES), [ISO_10116] (ECB, CBC), [ISO_9797-1] (padding)	[ISO_16844-3] sec: 7.4 (with changes according to [5]: sec. 12.1, 12.2, 12.3)	FCS_COP.1.1(1:AES)
Confidentiality, authenticity, and integrity of data for mutual authentication TOE <-> Motion Sensor	AES in ECB and CBC mode of operation	128 192 256	[FIPS_197] (AES), [ISO_10116] (ECB, CBC), [ISO_9797-1] (padding)	[ISO_16844-3] sec: 7.4 (with changes according to [5]: sec. 12.1, 12.2, 12.3)	FCS_COP.1.1(1:AES)

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Confidentiality, authenticity, and integrity of data for secure messaging TOE <-> Motion Sensor	AES in ECB and CBC mode of operation	128 192 256	[FIPS_197] (AES), [ISO_10116] (ECB, CBC), [ISO_9797-1] (padding)	[ISO_16844-3] sec: 7.4 (with changes according to [5]: sec. 12.1, 12.3)	FCS_COP.1.1(1:AES)

Table 21 – Use of cryptographic functions for trusted channel TOE <-> Motion Sensor related to this ST and to [5] Appendix 11 Part B.

According to [5] and [ISO_16844-3] sec: 7.4 the algorithms are suitable for confidentiality, authenticity, integrity, authentication and key agreement. An explicit validity period is not given.

Purpose	Cryptographic Mechanism	Key size (bits)	Standard of Implementation	Standard of Application	Related SFR
Data integrity and authenticity for VU Download to external media	ECDSA with hashing algorithm SHA-2 (for selection of SHA-2 algorithm, see Table 13)	256 to 521, see Table 23	[FIPS_180-4] (SHA-2), [FIPS_186-4] (ECDSA), [BSI_TR-03111] (data formats), [RFC_5480] (NIST curves), [RFC_5639] (Brainpool curves)	[5]: CSM_233	FCS_COP.1.1(2:SHA2) FCS_COP.1.1(3:ECC)

Table 22 – Use of cryptographic functions for VU Download related to this ST and to [5] Appendix 11 Part B.

According to [5] the algorithms are suitable for integrity and authenticity. An explicit validity period is not given.

Elliptic Curve Name	Key size (bits)	Standard of Implementation
NIST P-256	256	[RFC_5480]
BrainpoolP256r1	256	[RFC_5639]
NIST P-384	384	[RFC_5480]
BrainpoolP384r1	384	[RFC_5639]
BrainpoolP512r1	512	[RFC_5639]
NIST P-521	521	[RFC_5480]

Table 23 – Elliptic curves used