Security Target EFAS-4.10

Name of project:	EFAS-4.10
Document number	1250-100-SEC-EN
Version:	10
Rendered by/at:	Valery Toda / 2019.01.29
Last edited by/at:	Bernd Hoeppener / 2019.08.29
Status:	APPR

	Name:	Date:	Signature:
Reviewed by:	Valery Toda	2019.08.29	
Approved by:	Dr. Johannes Neudecker	2019.08.29	

Release notes:

version	date	section	changes, notes	modified by
00	2019.02.06	All	Initial Version	Valery Toda
01	2019.02.19	All	TOE Reference, Abbreviations, References, SFRs, CC-References, Figures, Table 20, Table 23, Table 25, Table 26	Valery Toda
02	2019.02.27	1.2, 6.*, 7.1, 7.2, 13	TOE Overview updated, Rationale updated, SFR updated, Annex C added, References updated	Valery Toda
03	2019.03.05	All	TOE Summary Specification updated, TOE statement of compatibility updated, Assurance measures updated	Valery Toda
04	2019.03.05	8.1.3	Confidentiality of data exchange updated	Valery Toda
05	2019.03.06	9.2.1	"Security Functional Requirements of the Security Controller" corrected.	Valery Toda
06	2019.03.06	8.3.1	Table 16 corrected, Repair (M) Statement corrected	Valery Toda
07	2019.06.26	1.3.2 9.1	TOE Configuration and Statement of compatibility corrected	Valery Toda
08	2019.07.01	1.1	Library reference corrected.	Bernd Hoeppener
08	2019.07.01	9.2.1	"FCS_COP.1(2:SHA-2)" added to SFRs. "FCS_COP.1/SHA" marked as "not relevant, because not used, no conflict". "FCS_COP_1(2:SHA-2) removed from table.	Bernd Hoeppener
09	2019.08.26	11	Table 2*- references related to generation methods corrected. Table 21 – key Symbol of first entry added	Valery Toda
10	2019.08.29	11 8.1.13	Key symbols updated in table 26 and "SF.UPDATE VU".	Bernd Hoeppener
10	2019.08.29	8.1.13 8.1.4	SHA-256 used for integrity check of SC SW.	Bernd Hoeppener
10	2019.08.29	11	"PP" replaced by "ST".	Bernd Hoeppener

Table of Contents

Table of Figures

Table of Tables

1 ST Introduction

1.1 ST Reference

This document is the Security Target (ST) of the EFAS-4.10 provided by intellic Germany GmbH for a Common Criteria evaluation.

Document Title:	Security Target - EFAS-4.10
Document Date:	2019.08.29
Document Version:	10
Editor:	Valery Toda
Publisher:	intellic Germany GmbH
CC-Version:	3.1 (Revision 5)
Assurance Level:	The minimum assurance level for this ST is EAL4 augmented.
General Status:	APPR
TOE:	EFAS-4.10
TOE Developer:	intellic Germany GmbH
TOE Sponsor:	Intellic GmbH (Austria)
Certification ID:	BSI-DSZ-CC-1117
IT Evaluation Scheme:	German CC Evaluation Scheme
Evaluation Body:	SRC Security Research & Consulting GmbH (SRC)

1.2 TOE Reference

The target of evaluation (TOE) is the product “EFAS-4.10 digital tachograph with SW Version 05.00 as developed by intellic Germany GmbH, based on INFINEON M7892 G12” (EFAS-4.10 V05.00).

The Target of Evaluation (TOE) is a Vehicle Unit in the sense of Annex 1C of the Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 [EU]. It is intended to be installed in road transport vehicles and will be used within the Tachograph System to store, display, print and output data related to driver activities in accordance with the requirements of [EU].

Der Evaluationsgegenstand (EVG) ist eine Fahrzeugeinheit (Abk.: FE) im Sinne von Anhang 1 C der VERORDNUNG (EU) 2016/799 DER KOMMISSION vom 18 März 2016 [EU]. Sie wird in ein Fahrzeug eingebaut und dient im Tachograph-System dazu, die Daten der Fahreraktivitäten aufzuzeichnen und zu speichern, am Display anzuzeigen, auszudrucken bzw. auf ein externes Gerät herunterzuladen entsprechend den Anforderungen aus [EU].

The INFINEON SC is used with the following configuration (Sales name SLE78CFX4000P):

- M7892 Design Step G12 with FW-Identifier 78.015.18
- and following SW - libraries:

  Asymmetric CryptoLibrary CL70 version 2.07.003 (including ECC, RSA, Toolbox) and belonging User Guidance documentation.
  Symmetric CryptoLibrary SCL78-SCP-v3 version 2.02.010 and belonging User Guidance documentation.

1.3 TOE Overview

1.3.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) addressed by this Security Target is a second-generation vehicle unit (VU) in the sense of [EU] 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 display, printer and external devices.
The TOE 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. The GNSS receiver allows recording of the position of the vehicle at certain points during the daily working period, and providing a second source of vehicle motion information. This device is embedded in the VU and contains currently an embedded antenna. (A connection to a suitable external antenna is planned for the future.) Because the GNSS receiver is within the same physical boundary as the VU, its protection is addressed by this ST. Furthermore, the TOE is connected to an external remote early detection facility (DSRC communication module), to allow remote early detection equipment to detect possible manipulation or misuse of the VU. The VU cannot yet communicate via Bluetooth with external devices involved in Intelligent Transport Systems. (The communication through this optional wireless interface is planned for the future.) Human users identify themselves to the TOE using tachograph cards.
The physical scope of the TOE is a device to be installed in a vehicle. The TOE consists of:

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

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

a. motion sensor (MS);
b. two Tachograph smart cards;
c. a power supply;
d. a remote early detection communication reader;
e. other devices used for calibration, software update and diagnostics;
f. intelligent dedicated equipment for data download.

The TOE 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 TOE has four modes of operation:

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

The TOE switches to the appropriate mode of operation according to the valid tachograph cards inserted into the card interface devices, as shown in Table 1. The modes of operation are significant in that certain operations can be carried out only whilst in certain modes of operation (see [EU] 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: Modes of operation

1.3.2 TOE configuration

TOE is configured in accordance to Configuration 2 in [PPT]. The GNSS receiver is internal (with an internal antenna) and the remote early detection is external. It should be noted that although the printer mechanism is part of the TOE, the paper documents that it produces are not.

1.3.3 TOE major security features for operational use

The TOE security features aim to:

- protect the data memory in such a way as to prevent unauthorized 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, confidentiality of data exchanged between the vehicle unit and the tachograph cards,
- protect the confidentiality, integrity and authenticity of data output through the remote early detection communication facility 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 below.

1.3.3.1 Identification and authentication

The TOE identifies and authenticates tachograph cards and motion sensors.

1.3.3.2 Access control to functions and stored data

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

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

1.3.3.3 Accountability of users

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

1.3.3.4 Audit of events and faults

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

1.3.3.5 Residual information protection for secret data

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

1.3.3.6 Integrity and authenticity of exported data

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

1.3.3.7 Stored data accuracy

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

1.3.3.8 Reliability of services

The TOE provides features that aim to assure the reliability of its services. These features include self-testing, physical protection, control of executable code, resource management, and secure handling of events.

1.3.3.9 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 [EU] Annex 1C, Appendix 11.

1.3.4 TOE Type

The TOE type is the second-generation digital tachograph vehicle unit EFAS-4.10, a vehicle unit in the sense of Annex 1C [EU]. (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 TOE contains an internal GNSS facility and is connected to an external remote early detection communication facility. Currently, it is not yet equipped with Bluetooth.

The life cycle of the EFAS-4.10 is based on the principles described in [EU], Appendix 10, and chapter 3.2, as shown in Figure 1. Grey blocks indicate the developing and manufacturing steps before delivery.

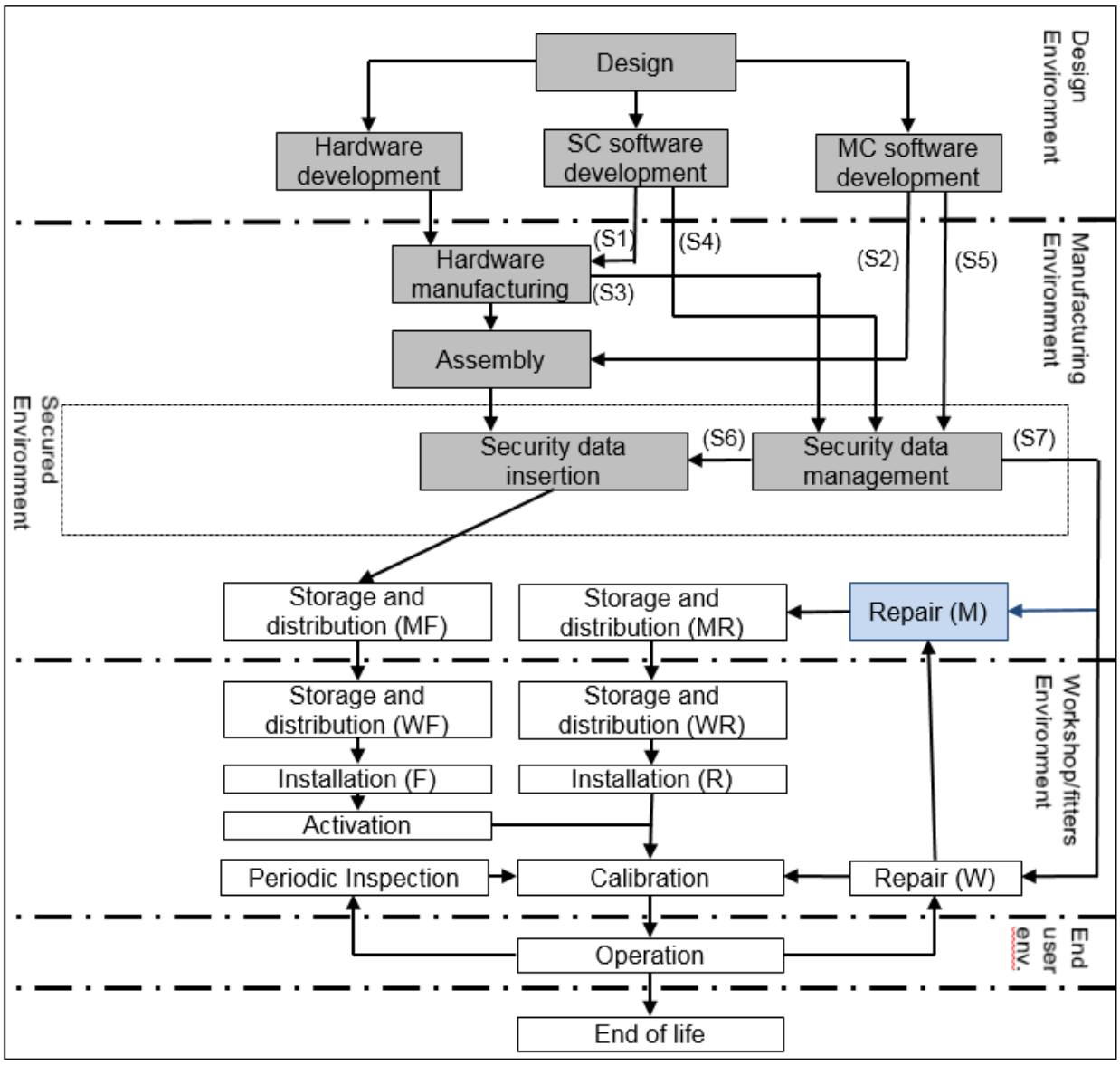

Figure 1: EFAS-4.10 Life-Cycle
(M=Manufacturer, W=Workshop, R=Repaired, F=Fabricated)

The security functionality defined by this Security Target focuses on the operational phase in the end user environment. However, some single properties of the calibration phase, being significant for the security of the TOE in its operational phase, are also considered by [PPT]. The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [EU]: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU.

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

A software or MC-SW-parameter update can be executed by a workshop on the basis of encrypted update data prepared by the Security Server in the manufacturing environment. The VU enables a software update of defined parts of the software or a MC-SW-parameter update, if the corresponding authentication was successful.

1.3.5 TOE connectivity

The following TOE-external components are

a) mandatory for a proper TOE operation:
   - power supply (e.g. from the vehicle in which the TOE is installed)
   - motion sensor
   - access to GNSS signals (provided within the TOE (see [EU] Annex 1C, Appendix 12))
   - DSRC connection to a remote early detection communication reader (provided through an external remote early detection communication facility (see [EU] Annex 1C, Appendix 14));
b) functionally necessary for an Annex 1C compliant operation:
   - calibration device (calibration phase only)
   - tachograph cards (four different types)
   - printer paper
   - external storage media for data download;
c) helpful for a convenient TOE operation, but not required:
   - connection to the vehicle network (e.g. CAN-connection, see [ISO16844-4])

Application note 1: The TOE will verify whether the connected motion sensor and tachograph cards possess appropriate credentials showing that they belong to the digital tachograph system. A security certification according to [EU], Annex 1C, Appendix 10 is a prerequisite for the type approval of a motion sensor and 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 [EU], Annex 1C, the TOE is operated and used not only with 2nd generation tachograph cards, but also with 1st generation tachograph cards (i.e. using the security mechanisms and card interface protocol specified in [EU] 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 TOE with 2nd generation motion sensors. The capability of the TOE to be used with 1st generation tachograph cards may be suppressed once and forever by workshops, so that 1st generation tachograph cards can no longer be accepted by the TOE. This may only be done after the European Commission has launched a procedure aiming to request workshops to do so, for example during the periodic inspection of recording equipment. Such procedure may be needed according to the results of a digital tachograph system threat assessment. The TOE therefore contains both 1st generation and 2nd generation security elements, and is able to execute both 1st generation and 2nd generation security mechanisms, according to the generation of the

cards that are inserted in the TOE. Full details of inter-generational operability requirements are in [EU], Annex 1C, Appendix 15.

In order to avoid redundancy and to minimize the evaluation efforts, the evaluation of the TOE will be conducted as a composite evaluation and will make use of the evaluation results of the CC evaluation of the security controller "M7892 G12 (sales name SLE78CFX4000P)" provided by INFINEON. The IC is evaluated according to Common Criteria EAL 6 augmented by ALC_FLR.1 and is listed under the Certification ID BSI-DSZ-CC-0891-V3. The evaluation of the IC is based on Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014.

1.4 Architecture Overview

The Target of Evaluation (TOE) is the Digital Tachograph EFAS-4.10 It is designed in accordance with the Tachograph Specification [EU].

Figure 2 shows security relevant physical interfaces and internal components of the EFAS-4.10 digital tachograph.

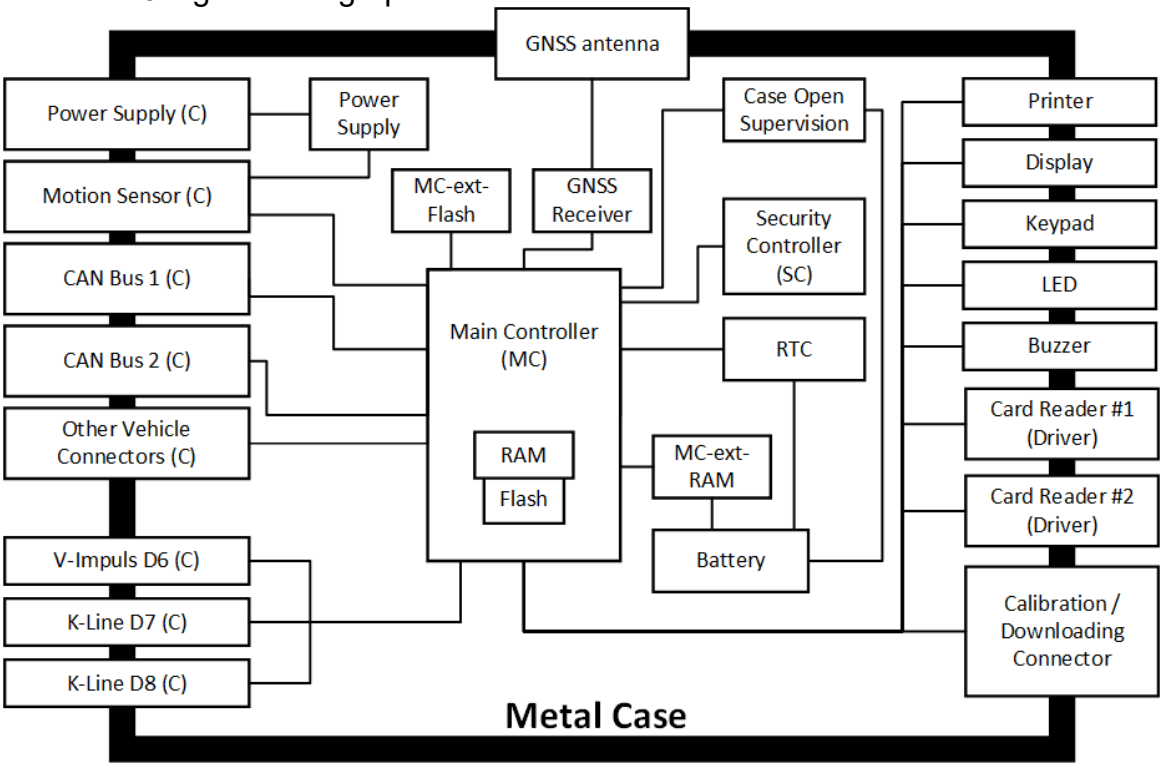

Figure 2: EFAS-4.10 with Interfaces

(C): Connector

1.5 TOE Hardware

The hardware components are:

Security Controller (SC)
The security controller is a micro controller that consists of a central processing unit, a cryptographic coprocessor and embedded RAM, EEPROM and optionally ROM memory.

The SC implements most of the security functions of the TOE:
- Storage of sensitive data (certificates, identities, audit records, …)
- Cryptographic operations.
- Supervision of time/date and motion data.
- Supervision of user data stored in the MC flash.

Main Controller (MC)
The main controller controls all external interfaces. It has exclusive access to the VU onboard flash and RAM.

MC-ext Flash
The MC-ext-flash contains the software for the MC which does not fit into the MC-internal flash as well as configuration and user data.

MC-ext RAM
The MC-ext-RAM stores temporary data.

Real Time Clock (RTC)
The RTC provides the EFAS-4.10 with a reliable time.

Case Open Supervision
The case open supervision circuit detects any case opening while the external supply voltage is connected or not. The circuit is triggered when either the housing is opened or the VU battery is empty.

Battery
The internal battery ensures the proper operation of the RTC, the case open supervision circuit and the MC RAM while the VU is disconnected from the vehicle power supply.

Card Reader #1 and #2
The card readers provide the interface to the Tachograph Cards.

Printer
The printer is able to output the data in printed form.

Keypad
With help of the keypad it is possible to input control information.

Display, LED and Buzzer

The VU informs the user via the build-in display, buzzer and LED about the relevant values (road speed, driving times) and events (e.g. errors or speed limit violations).

Power Supply
The Power Supply hardware provides all components with necessary voltage.

Metal Case
The rigid metal case is secured by a sealed screw and the case opening switch, which triggers the case open supervision circuit when released.

Internal GNSS Receiver
The GNSS Receiver provides NMEA sentences to the Vehicle Unit.

1.6 TOE Software

The TOE software consists of three parts:

SC Software
The SC software provides data access functions, tachograph card access functions and motion sensor communication functions for use by the MC application software. Furthermore, the SC software provides functions for secure communication between the VU and the Security Server as well as between the VU and a remote company server (with connection to a Company Card). In addition, the SC software supervises the other parts of the VU, especially the time/date handling as well as the code and user data storage in the MC flash.

MC Application Software
The MC application software implements all functions necessary for the operation of a digital tachograph, as the control of external and internal interfaces, the memory access, and the supply voltage supervision. For security operations, the MC application software makes use of the services of the SC.

MC Boot Software
The MC boot software starts the MC application software and executes parts of the software or MC-SW-parameter update.

1.7 Details of Security Mechanisms

EFAS-4.10 provides all security mechanisms required in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT]), in particular the following:

EFAS-4.10 monitors the case opening, the values of the power supply, the RTC, the flash memory contents and the communication with the motion sensor. The TOE runs self-tests during initial start-up, and during normal operation to verify its correct operation. For events impairing the security, EFAS-4.10 generates audit records with associated data. The EFAS-4.10 preserves a secure state independently from the values of the power supply, including cut-off, and prevents a misuse of security relevant data involved in its operations.

1.8 TOE Product Scope

This Security Target applies to the following components of the TOE respectively:

- The vehicle unit EFAS-4.10, Hardware/Software
- Operating Manual EFAS-4.10 document in paper form (on request) / electronic pdf-form (for all kinds of users)
- Service and Installation Manual EFAS-4.10, document in paper form (on request) / electronic pdf-form (for workshop personnel)

The TOE is able to operate in the environment of vehicles with 24 V and 12 V power supply from different vehicle manufacturers. The TOE is able to be adapted via parameter settings to cover the vehicle variety (e.g. optional interfaces: the first and second CAN bus, the K-Line and the info interface).

1.9 TOE Environment

1.9.1 Development Environment

The EFAS-4.10 developers ensure that the assignment of responsibilities during development is done in a manner which maintains IT security. The TOE is developed in a well-structured environment with well-defined responsibilities. The specification, implementation and tests in the development departments are organized based on formal methods. Suitable measures enforce the usage of guidelines. The complete development of the TOE is well documented. The confidentiality and integrity of development results is protected (usage of file servers with dedicated access rights, version controls, backup strategies, usage of e-mail encryption for communication and firewall protection). The used measures are always documented.

1.9.2 Manufacturing Environment

In the manufacturing environment, responsibilities are assigned in a manner which maintains IT security and the EFAS-4.10 is protected from physical attacks which might compromise IT security. The manufacturing environment is well documented, supported by procedures based on ISO 9001:2000 (see [ISO9001]). Measures are defined to protect security data like cryptographic keys against disclosure and manipulation. Systems which implement security data generation algorithms are accessible to authorized and trusted persons only. Security data are generated, transported, and inserted into the EFAS-4.10, in such a way as to preserve its appropriate confidentiality and integrity.

When leaving the manufacturing environment, the TOE is complete and ready to be delivered to the customer.

1.9.3 Fitters and Workshop Environment

The EFAS-4.10 fitters and workshop environment is as described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT]).

1.9.4 End User Environment

The EFAS-4.10 end user environment is as described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT]).

2 Conformance Claims

2.1 CC Conformance Claims

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [CC1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [CC2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [CC3]

as follows:

- Part 2 extended,
- Part 3 conformant (EAL4 augmented by ATE_DPT.2 and AVA_VAN.5).

2.2 PP Claim

This Security Target claims strict conformance to the Protection Profile ‘Digital Tachograph – Vehicle Unit (VU PP)’, BSI-CC-PP-0094-2017 [PPT], as sponsored by Joint Research Centre, European Commission, editors Julian Straw, David Bakker, Jacques Kunegel and Luigi Sportiello, Version 1.0 as of 19th May 2017.

2.3 Package Claim

This Security Target claims conformance to the assurance package defined in [5] Annex 1C, Appendix 10.

2.4 Conformance Rationale

Since this Security Target claims strict conformance to the Protection Profile BSI-CC-PP-0094-2017 [PPT] referenced in 2.2 “PP Claim”, no rationale is necessary here.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

The primary and secondary assets to be secured are as introduced in BSI-CC-PP-0094-2017 (see [PPT] section 3.1).

The **primary assets** to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap. 10.1 for the term definitions)

Object No.	Asset	Definition
1	user data (recorded by or stored in the TOE)	Any data, other than security data (see Annex A) recorded or stored by the VU, as required by of [EU], Annex 1C, Section 3.12.
2	user data transferred between the TOE and an external connected device	All user data being transferred from or to the TOE. A TOE communication partner can be: - a motion sensor, - a tachograph card - a remote early detection communication facility, and - 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 TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	Asset	Definition
3	TOE design and software code	Design information and source code (uncompiled or reverse engineered) for the TOE that could facilitate an attack.
4	TOE hardware	Hardware used to implement and support TOE functions.
5	TOE immanent secret security	Secret security elements (i.e. symmetric and private keys) used by the TOE in

Object No.	Asset	Definition
	data	order to enforce its security functionality (see Annex A). • SW update keys
6	TOE immanent non-secret security data	Non-secret security elements (i.e. certificates and public keys) used by the TOE in order to enforce its security functionality (see Annex A). • Serial Number
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.
9	TOE security relevant software components (security patch)	Updateable security relevant software components of the TOE (inclusive update credentials), in particular SC software (except the update mechanism).
10	TOE non-security relevant software components (patch)	Updateable non-security relevant software components of the TOE (inclusive update credentials), such as MC software
11	TOE non-security relevant SW Parameters	Updateable non-security relevant MC-SW-Parameters (inclusive update credentials)

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 the TSF and TSF-data in the sense of the CC.

3.1.2 Subjects and external entities

The subjects and external entities considered by this Security Target are listed in the following table:

No.	Role	Definition
1	Human user	Human users are to be understood as legitimate human user of the TOE. 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).[1]
5	Remote early detection communication reader	The equipment used to perform targeted roadside checks.
6	Unknown equipment	A technical device not possessing valid credentials for its authentication, or for which validity of its credentials is not verifiable.
7	Attacker	An attacker is a threat agent (a person or a

[1] See Annex A for definitions of European level (EUR) keys and certificates.

No.	Role	Definition
		process acting on his behalf) trying to undermine the security policy defined by the current SP, 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 recognized by the TOE.

Table 4: Subjects and external entities

Table 4 defines the subjects in the sense of the CC that can be recognized by the TOE independent of their nature (human or connected entity). Where a successful appropriate identification and authentication process takes place, the TOE creates – for each of those respective external entities – an 'image' inside, and 'works' then with this TOE internal image (also called subject in the CC). From this point of view, the TOE 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 recognized by the TOE.

3.2 Threats

This section describes the threats as described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT] sec. 3.2) to be averted by the TOE independently or in collaboration with its IT environment. These threats arise from the assets protected by the TOE and the method of TOE's use in the operational environment.
The threats are defined in the following tables.

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

Table 5: Threats addressed solely by the TOE.

Label	Threat
T.Access	Attackers (e.g. human users) could try to access functions not allowed to them (e.g. drivers gaining access to calibration function), to modify or delete user data.

T.Calibration_Parameters	Human users could try to use a miscalibrated TOE (through calibration data [2] modification, or through organisational weaknesses) to misrepresent driver activities (user data).
T.Clock	Attackers could try to modify the internal clock of the TOE, and interfere with the correct operation of the TOE.
T.Design	Attackers could try to gain illicit knowledge of the TOE design and software code, either from manufacturer's material (e.g. through theft or bribery) or from reverse engineering, interfere with the correct operation of the TOE.
T.Environment	Attackers could use environmental attacks (thermal, electromagnetic, optical, chemical or mechanical) to interfere with processing of user data.
T.Fake_Devices	Attackers could try to connect unknown equipment (fake motion sensor, tachograph card or external GNSS facility) to the TOE to misrepresent driver activities (user data at rest or being transferred between the TOE and an external connected device).
T.Hardware	Attackers could try to modify TOE hardware, and interfere with the correct operation of the TOE.
T.Identification	Human users could try to use several 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.Power_Supply	Attackers could try to interfere with the recording or transmission of user data by modifying (cutting, reducing, increasing) the TOE's power supply to interfere with its correct operation.
T.Security_Data	Attackers could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment, and attempt to misrepresent driver activities (user data).
T.Software	Attackers could try to modify TOE software on the VU or during the updates (modification of patches for updates) in order to interfere with the correct operation of the TOE. Users could try to modify MC-SW-parameters during the updates
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 TOE and its operational environment

[2]Part of user data. For definition of calibration data see [EU] Annex 1C, Chapter 3.12.10.

3.3 Assumptions

This section describes the assumptions as described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT] sec. 3.3) that are made about the operational environment in order to be able to provide the security functionality. If the TOE is placed in an operational environment 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 TOE after its installation at the latest before the vehicle is used in scope of Regulation (EC) N° 561/2006.
A.Approved_Workshops	The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.
A.Card_Availability	Tachograph cards are available to the TOE human users and delivered by Member State authorities to authorized 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 standardized and secure methods (see [EU] Annex 1C, Chapter 3).
A.Controls	Law enforcement controls of the TOE will be performed regularly and randomly, and must include security audits (as well as visual inspection of the TOE).
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 TOE will only be operated together with a motion sensor that is type approved according to [EU] Annex 1C.[3]

Table 7: Assumptions

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

3.4 Organizational Security Policies

This section shows the organizational security policies as described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT] sec. 3.4) that are to be enforced by the TOE, its operational environment, or a combination of the two.
The organizational security policies are provided in the following table.

Short name	Organizational Security Policy
P.Crypto	The cryptographic algorithms described in [EU] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

Table 8: Organizational Security Policies

4 Security Objectives

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

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

4.1 Security Objectives for the TOE

The TOE security objectives (as also described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT] sec. 4.1)) address the protection to be provided by the TOE, independent of the TOE environment, and are listed in the table below.

Short name	Security objective for the TOE
O.Access	The TOE must control user access to functions and data on the basis of user type and identity.
O.Authentication	The TOE must authenticate users and connected entities (when a trusted path or trusted channel[4] needs to be established towards these users).
O.Accountability	The TOE must collect accurate accountability data.
O.Audit	The TOE must audit attempts to undermine system security and trace them to associated users.
O.Integrity	The TOE must maintain stored data integrity.

[4] Trusted channel is referred to in [EU], Annex 1C, Appendix 11 as a secure messaging session.

O.Output	The TOE must ensure that data output accurately reflects data measured or stored.
O.Processing	The TOE must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The TOE must provide a reliable service.
O.Secure_Exchange	The TOE must secure data exchanges with the motion sensor, with tachograph cards and with the remote early detection communication reader.
O.Software_Update	The TOE must check the authenticity and integrity before installing or update of the TOE software.

Table 9: Security objectives for the TOE

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment (as also described in the Protection Profile BSI-CC-PP-0094-2017 (see [PPT] sec. 4.2)) address the protection that must be provided by the TOE environment, independent of the TOE itself, and are listed in the table below.

Specific phase	Short name	Security objective for the environment
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 TOE, 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 TOE 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 TOE. The software parts for updates have to be secured during the generation and transport to the VU. MC-SW-Parameter updates have to be secured during the generation and transport to the VU.
	OE.Data_Strong	Security data inserted into the TOE for compatibility with 2nd generation tachograph cards, motion sensors and remote early detection communication readers must be as cryptographically strong as required by [EU] Annex 1C, Appendix 11 Part B. Security data inserted into the TOE for compatibility with 1st generation tachograph cards and motion sensors must be as cryptographically strong as required by [EU] 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 TOE 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 TOE human users and delivered by Member State Authorities to authorised persons only.
	OE.Card_Traceability	Card delivery shall be traceable (white lists, black lists), and black lists must be used during security audits.
	OE.Controls	Law enforcement controls 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[5]	The Motion Sensor of the recording equipment connected to the TOE must be type approved according to [EU] Annex 1C.
	OE.EOL	When no longer in service the TOE 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 TOE (see section 1.9.4). 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 TOE 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 TOE.

5 Extended Components Definition

This ST uses a component that is defined as an extension to CC Part 2.

The extended component is FCS_RNG.1 Random number generation. This component is fully defined and justified in [FCRNG] Section 3. [PPT] defines a restricted set of ways in which the extended component can be used in a Security Target. These are set out in Annex B, and further information is provided in [FCRNG].

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

5.1 Rationale for extended component

CC Part 2 [CC2] defines two components FIA_SOS.2 and FCS_CKM.1 that are similar to FCS_RNG.1. However, FCS_RNG.1 allows the specification of requirements for the generation of random numbers in a manner that includes necessary information for intended use, as is required here. These details describe the quality of the generated data that other security services rely upon. Thus by using FCS_RNG the ST author is able to express a coherent set of SFRs that include the generation of random numbers as a security service.

5.2 Extended component definition

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

5.2.1 FCS_RNG Generation of random numbers

Family behavior

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

Component levelling

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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Generation of random numbers

Hierarchical to: -

Dependencies: -

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

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

6 TOE Security Requirements

This Security Target clarifies and adapts the security requirements as given in the Protection Profile BSI-CC-PP-0094-2017 ([PPT] sec. 6).

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

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [CC1] of the CC. These operations are used in the Protection Profile BSI-CC-PP-0094-2017 [PPT] and in this ST, respectively.

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 as well as by the ST author are denoted by underlined text and appear in square brackets.

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 as well as by the ST author are denoted by underlined text and appear in square brackets.

The **iteration** operation is used when a component is repeated with varying operations. Iterations taken from the PP are denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator. Iterations that have been made by the ST author are denoted by showing a slash “/”, and the iteration indicator after the component identifier. (In order to trace elements belonging to a component, the same slash “/” with iteration indicator is used behind the elements of a component.)

Whenever an element in [PPT] contains an operation that the PP author left uncompleted, the ST author completed that operation (as described above) and the operation within the ST is shown with yellow background. In case the ST author added a SFR this is also shown with yellow background.

6.1 Security Functional Requirements for the TOE

This section is subdivided to show security functional requirements as derived in the Protection Profile BSI-CC-PP-0094-2017 ([PPT] sec. 6.1) that relate to the TOE itself, and those that relate to external communications. This is to facilitate comparison of the communication requirements between this ST and others in the PP family. Section 6.1.1 addresses requirements for the VU in general. Section 0 addresses the communication requirements for 2nd generation tachograph cards to be used with the TOE. Section 6.1.3 addresses the communication requirements for 1st generation tachograph cards to be used with the TOE.

Because the TOE is designed with an internal GNSS receiver, whole SFRs or parts of operations within several SFRs regarding an EGF (External GNSS Facility) will be omitted or crossed out within this ST compared to [PPT]. At the end of this section an overview is given within Table 11 which shows all omitted SFRs or parts of SFRs including a rationale.

6.1.1 Security functional requirements for the VU

6.1.1.1 Class FAU Security Audit

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 [EU] 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 the event, type of event, subject identity, and the outcome (success or failure) of the event[6]; 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 [EU] Annex 1C, sections 3.12.8 and 3.12.9].

FAU_SAR.1 Audit review

Hierarchical to: -

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

Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [anyone, subject to the requirements of [EU] 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.

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 unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [detect[7]] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to:	FAU_STG.3
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [overwrite the oldest stored audit records] and [the data memory shall be able to hold events data as required by [EU] Annex 1C, section 3.12.8 without overwriting], if the audit trail is full.
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 TOE.*

6.1.1.2 Class FCO Communication

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[8]] **in accordance with [EU], Annex 1C, Appendix 11, Chapters 14 and 13, respectively**.

[7] Audit records are “events/faults” defined in [EU] 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”.

[8] The originator is the vehicle unit.

FCO_NRO.1.2 The TSF shall be able to relate the [identity (VU private key (VU_Sign.SK) and VU DSRC key (VUDSRC_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 [EU], Annex 1C, Appendix 11, Chapters 14 and 13].

6.1.1.3 Class FDP User Data Protection

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[9]] on [subject: any user of the TOE, objects: application and data files structure as defined in Application note 6, operations: read, write, modify].

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.*

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

Hierarchical to: -

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

FDP_ACF.1.1(1:FIL) The TSF shall enforce the [File Structure SFP] to objects based on the following: [none].

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

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

deletion].

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[10]] on [see [EU], Annex 1C, Chapter 2.3, Chapter 3.21, Chapter 3.23, Chapter 3.6, Chapter 3.1].
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.*

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1(2:FUN)	The TSF shall enforce the [Function SFP] to objects based on the following: [mode of operation and life cycle state].
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 [EU], 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

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

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].

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[11]] on [see [EU], Annex 1C, REQ 94, 97, 101, 119].
Application note 8:	*The assignment in this iteration relates to control over access to VU identification data, MS identification data, calibration mode data, security data and MS audit records[12].*

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

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1(3:DAT)	The TSF shall enforce the [Data SFP] to objects based on the following: [see [EU], Annex 1C, REQ 94, 97, 101, 119].
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 unauthorized modification of the serial number, approval number pairing date related to the 20 most recent pairings of motion sensors[13];
- ~~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)[14];~~
- the vehicle unit is able to record and store in its data memory, and prevent unauthorized 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 unauthorized modification of data relevant to the most recent time adjustment and the five largest time adjustments outside the frame of a regular calibration;

[12] 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.

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

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

- the vehicle unit is able to store, and prevent unauthorized modification of the keys and certificates identified in Annex A, managed by the manufacturer;
- the vehicle unit is able to store in its data memory, and prevent unauthorized 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 unauthorized 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].

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[15]] on [subjects: any user of the TOE, objects: data exported to a tachograph card as defined in Application note 9, operation: access].

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.

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

Hierarchical to: -

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

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

FDP_ACF.1.1(4:UDE)	The TSF shall enforce the [User Data Export SFP] to objects based on the following: [subjects: any user of the TOE, objects: data exported to a tachograph card as defined in Application note 9, operation: access].
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[16]; - 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~~ none].
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 [17] or card number [18] 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

[16] See [EU] Annex 1C, Chapter 3.14.1 and 3.14.2.

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

[18] Card number shall be partially blanked (everey odd character).

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 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 [19]] on [subjects: TOE, objects: any data defined in Application note 10, operations: use of data only from valid source, prevention of external inputs being accepted as executable code].
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.*

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1(5:IS)	The TSF shall enforce the [Input Sources SFP] to objects based on the following: [subjects: TOE, objects: any data defined in Application note 10].
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

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

executable code].

FDP_ACC.1/SW-Upgrade Subset access control

Hierarchical to:	-
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SW-Upgrade	The TSF shall enforce the [SFP SW_Upgrade] on [updateable software components and User with identity WORKSHOP for updates of MC software components and MC-SW-parameters and SC software components].

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/SW-Upgrade	The TSF shall enforce [SFP SW_Upgrade] to objects based on the following: [updateable software components and SW parameters may be exchanged if the integrity and the authenticity of the patch data is confirmed with help of the update credentials].
FDP_ACF.1.2/SW-Upgrade	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[- update of software components and SW parameters is only possible after workshop card authentication, - update of software components and SW parameters is only possible if the integrity and the authenticity of the patch data were confirmed with help of the update credentials].
FDP_ACF.1.3/SW-Upgrade	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4/SW-Upgrade	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

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].

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 initialization

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

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

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

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: -

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

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

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

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

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

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE: [

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

FDP_ITC.2/SW-Upgrade Import of user data[20] with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Import of user data without security attributes, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/SW-Upgrade	The TSF shall enforce the [SFP_SW_Upgrade] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/SW-Upgrade	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/SW-Upgrade	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/SW-Upgrade	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/SW-Upgrade	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [update of the indicated software components and SW parameters only if the integrity and the authenticity of the patch data is confirmed with help of the update credentials].

FDP_ITT.1 Basic internal transfer protection

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control
FDP_ITT.1.1	The TSF shall enforce the [Data_SFP] to prevent [modification] of user data when it is transmitted between physically-separated parts of the TOE.

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 [allocation of the resource to] the following objects: [- Temporarily stored cryptographic keys that are listed in Table 20, Table 21, Table 23, Table 24;

[20] User data means here patch data as well as credentials material needed for software updates

- 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);
- no further objects].

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 Annex A – Key & Certificate Tables that are marked as having to be made unavailable at decommissioning the TOE is a matter of the related organizational 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.*

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].

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, no other motion data integrity errors] 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].

6.1.1.4 Class FIA Identification and Authentication

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] unsuccessful authentication attempts occur related to [local tachograph card authentication].
FIA_AFL.1.2(1:TCL)	When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [a) Generate an audit record of the event, b) Warn the human user, c) Assume the human user to be an Unknown User and the card to be non-valid].
Application note 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.*

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 [5] unsuccessful authentication attempts occur related to [remote tachograph company card authentication].
FIA_AFL.1.2(2:TCR)	When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [warn the remotely connected company].
Application note 15:	*FIA_AFL.1(2:TCR) is only applicable if the TOE provides a remote download facility (see [EU] Annex 1C paragraph 193.*

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 [20] unsuccessful authentication attempts occur related to [motion sensor authentication].
FIA_AFL.1.2(3:MS)	When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [a) Generate an audit record of the event, b) Warn the user,

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

Application note 16 *The positive integer number expected in FIA_AFL.1.1(3:MS) shall be ≤ 20 during a calibration. Outside of a calibration any authentication failure shall generate the actions in FIA_AFL.1.2(3:MS).*

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 [EU] Annex 1C, section 3.12.13 and Appendix 1 2.73 and 2.74.*

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.*

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: -

Dependencies:	-
FIA_UAU.5.1	The TSF shall provide [authentication using the methods described in [EU], Annex 1C, Appendix 11, Chapter 10 (certificate chain authentication and PIN)] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [rule: if the card is a workshop card then authentication using both certificate chain authentication and a PIN of at least 4 digits is required].
Application note 19:	*FIA_UAU.5 applies only to authentication using a workshop card, where a PIN is required.*

FIA_UAU.6 Re-authenticating

Hierarchical to:	-
Dependencies:	-
FIA_UAU.6.1	The TSF shall re-authenticate the ~~user~~ **tachograph card** under the conditions [at power supply recovery, when the secure messaging session is aborted as described in [EU] Annex 1C, Appendix 11 and more frequently than once per day].

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	-
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.1.5 Class FMT Security Management

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].

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.

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.

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.

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.

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.

FMT_MOF.1 Management of security functions behavior (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].

FMT_MOF.1 Management of security functions behavior (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.*

FMT_MOF.1 Management of security functions behavior (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].

FMT_MOF.1 Management of security functions behavior (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].

FMT_MOF.1 Management of security functions behavior (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)].

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)].

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)].

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.

6.1.1.6 Class FPT Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -
Dependencies: -
FPT_FLS.1.1 The TSF shall preserve a secure state[21] 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].

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 behavior
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*

[21] 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.

months in type approval conditions.

Application note 22: *The TOE is designed so that it can be opened. The TOE detects any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the TOE generates an audit record (The audit record is generated and stored after power supply reconnection). After its activation, the TOE detects hardware sabotage related to card readers, security controller and internal clock.*

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.

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 [EU] Annex 1C, Chapter 2, Sections 3.3 and 3.23.*

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

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

Hierarchical to:	-
Dependencies:	-
FPT_TDC.1.1/SW-Upgrade	The TSF shall provide the capability to consistently interprete [SW upgrade patch data and update credentials and MC-SW- parameter update data and update credentials] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/SW-Upgrade	The TSF shall use [the credentials which belong to software component or MC-SW- parameter update data and particular VU] when interpreting the TSF data from another trusted IT product.

6.1.1.7 Class FTP Trusted path/channels

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[22]].
Application note 26:	*Details of the communication channel can be found in [EU] Appendix 11, Chapter 12.*

6.1.1.8 Class FCS Cryptographic Support

FCS_COP.1/SW-Upgrade Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4

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

FCS_COP.1.1/SW-Upgrade	The TSF shall perform [the cryptographic operations decryption and data integrity protection] in accordance with a specified cryptographic algorithm [AES in CBC and COUNTER mode and CMAC] and cryptographic key size [128 bits] that meet the following: [[FIPS 197] (AES), [NIST SP800-38A] (AES CBC mode) and [NIST SP800-38B] (AES CMAC), [NIST SP800-38D] (COUNTER)].

FCS_CKM.4/SW-Upgrade Cryptographic key destruction

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/SW-Upgrade	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting with random values] that meets the following [- Requirements in Table 26; - 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[23]].

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

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

6.1.2.1 Class FCS Cryptographic Support

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

[23]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.

key generation algorithm [AES, ECC].and specified cryptographic key sizes [for the keys indicated in Table 23 and Table 24 as being generated by the TOE the key sizes required by [EU] Annex 1C, Appendix 11, Part B for those keys] that meet the following: [Reference [FCRNG] predefined RNG class [PTG.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.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 [EU] Annex 1C, Appendix 11, Part B] that meets the following [[EU] 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 the tachograph cards.*

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 [overwriting with random values] that meets the following [- Requirements in Table 23 and Table 24; - 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[24]; - no further standards].

FCS_COP.1 Cryptographic operation (1:AES)

[24]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.

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(1:AES)	The TSF shall perform [the following: a) pairing of a vehicle unit and a motion sensor; b) mutual authentication between a vehicle unit and a motion sensor; c) ensuring confidentiality, authenticity and integrity of data exchanged between a vehicle unit and a motion sensor; d) ensuring authenticity and integrity of data exchanged between a vehicle unit and a tachograph card; e) ensuring confidentiality of data exchanged between a vehicle unit and a tachograph card; f) ~~ensuring authenticity and integrity of data exchanged between a vehicle unit and an external GNSS facility~~] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128, 192, 256 bits] that meet the following: [FIPS PUB 197: Advanced Encryption Standard and [EU] Appendix 11, Part B].

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

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(2:SHA-2)	The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication (FIPS) PUB 180-4: Secure Hash Standard (SHS)].

FCS_COP.1 Cryptographic operation (3:ECC)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security

attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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

a) digital signature generation;

b) digital signature verification;

c) cryptographic key agreement;

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

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

~~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 [[EU] Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [EU] Appendix 11, Part B] that meet the following: [[EU] Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters in Table 11

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	512	secp521r1

Table 11 - 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 shall be of (roughly) equal strength. Table 12 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 12 - Cipher suites

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.2.3].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [AIS-31 (strength of mechanism: high)].

6.1.2.2 Class FIA Identification and authentication

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 [EU] Annex 1C, section 3.1.12.2, and Appendix 1 2.140 and 2.144.*

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

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

6.1.2.3 Class FPT Protection of the TSF

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 [EU] 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 [EU] 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.*

6.1.2.4 Class FTP Trusted path/channels

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 [EU] Appendix 11, Chapter 10.*

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

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

6.1.3.1 Class FCS Cryptographic support

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 [EU] Annex 1C, Appendix 11 Part A, Chapter 3].

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.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 [EU] Annex 1C, Appendix 11

Part A] that meets the following [[EU] Annex 1C, Appendix 11 Part A, Chapter 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 [overwriting with random values] that meets the following [- Requirements in Table 20 and Table 21; - 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[25]; - no further standards]

FCS_COP.1 Cryptographic operation (4:TDES)

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(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: [[EU] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_COP.1 Cryptographic operation (5:RSA)

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

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

	FCS_CKM.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: [[EU] Annex 1C, Appendix 11 Part A, Chapter 3].

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

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(6:SHA-1)	The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication (FIPS) PUB 180-4: Secure Hash Standard (SHS)].

6.1.3.2 Class FIA Identification and authentication

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

6.1.3.3 Class FPT Protection of the TSF

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 [EU] 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 [EU] 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.*

6.1.3.4 Class FTP Trusted path/channels

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 [ISO16844-3] Appendix 2].

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

The following Table 11 shows SFRs or parts of SFRs which are omitted resp. crossed out within this ST compared to [PPT] including a note of the ST author which give reasons and justification for omitting them.

SFR	Omitted parts	Note
FDP_ACC.1(3:DAT)	Application note 8 of [PPT]: External GNSS Facility identification data	Because the TOE is designed with an internal GNSS receiver, this can be omitted within the ST.
FDP_ACF.1(3:DAT)	Parts of SFR: the vehicle unit is able to record and store in its data memory, and prevent unauthorized modification of the serial number, approval number and coupling date related to the 20	Because the TOE is designed with an internal GNSS receiver and these items of the SFR are only applicable for an external GNSS receiver, they are crosses out within the ST.

	most recent coupled external GNSS facilities (if applicable) the vehicle unit is able to record and store in its data memory, and prevent unauthorized modification of audit records generated by the external GNSS facility (if applicable)	
FDP_ACF.1(4:UDE)	Parts of SFR: 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	The TOE is not equipped with an ITS interface. This item can be crossed out within the ST
FDP_ITC.1	Parts of SFR: and GNSS data	Because the TOE is designed with an internal GNSS receiver and this item of the SFR is only applicable for an external GNSS receiver, it can be crossed out within the ST.
FDP_ITC.2	Parts of SFR: and external GNSS facility (if applicable) 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;	Because the TOE is designed with an internal GNSS receiver and these items of the SFR are only applicable for an external GNSS receiver, they can be crossed out within the ST.
FMT_SMR.1	Parts of SFR: g) External GNSS facility (if applicable)	Because the TOE is designed with an internal GNSS receiver and this item of the SFR is only applicable for an external GNSS receiver, it can be crossed out within the ST.

FPT_TST.1	Parts of SFR: link to external GNSS facility (if applicable)	Because the TOE is designed with an internal GNSS receiver and this item of the SFR is only applicable for an external GNSS receiver, it can be crossed out within the ST.
FCS_COP.1(1:AES)	Parts of SFR: f) ensuring authenticity and integrity of data exchanged between a vehicle unit and an external GNSS facility	Because the TOE is designed with an internal GNSS receiver, this item of the SFR can be crossed out within the ST.
FCS_COP.1(3:ECC)	Parts of SFR: e) coupling of a vehicle unit and an external GNSS facility; f) mutual authentication between a vehicle unit and an external GNSS facility;	According to Footnote 30 in [PPT] items e) and f) are only applicable when the TOE supports connection to an EGF. Because the TOE has an internal GNSS receiver these items can be crossed out within the ST.
FIA_AFL.1.1(4:EGF)	Whole SFR	Because the TOE is designed with an internal GNSS receiver, the whole SFRs can be omitted within the ST.
FIA_ATD.1(3:EGF)	Whole SFR	
FIA_UAU.2(2:EGF)	Whole SFR	
FTP_ITC.1(3:EGF)	Whole SFR	

Table 11: SFRs in ST compared to [PPT]

6.2 Security assurance requirements for the TOE

The security assurance requirements are as derived in BSI-CC-PP-0094 (see [PPT], section 6.2).
The assurance level for this Security Target is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [CC3]. These security assurance requirements are derived from [EU] Annex 1C, Appendix 10 (SEC_006).

7 Rationale

7.1 Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats (see 3.2) and OSPs (see Table 8) are addressed by the security objectives. It also shows that all assumptions (see Table 7) are addressed by the security objectives for the TOE environment.

	T.Card_Data_Exchange	T. Remote_Detect_Data	T.Output_Data	T.Access	T.Calibration_Parameters	T.Clock	T.Design	T.Environment	T.Fake_Devices	T.Hardware	T.Identification	T.Identification	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	P.Crypto
O.Access				x	x	x			x					x		x													x
O.Authentication				x	x	x			x		x	x																	x
O.Accountability											x																		
O.Audit	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
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									x																			x	

_MS																											
OE.EOL							x						x														

Table 12: Security objectives rationale

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

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

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

T.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.

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

T.Identification is addressed by O.Authentication to ensure the identification of the user, O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address this threat by storing all activity carried (even without an identification) with the VU. The OE.Driver_Card_Unique, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.
T.Design is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Reliability. OE.EOL helps to safeguard access to the TOE design through secure disposal of equipment at end of life.

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

T.Clock is addressed by O.Access to ensure that the full time adjustment function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive time adjustment data is accurate. Workshops are approved by Member States authorities and are therefore trusted to properly set the clock

(OE.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.

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 which have to be performed regularly and randomly.

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

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

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.

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.

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.

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.

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.Software_Upgrade is included such that software revisions shall be security certified before they can be implemented in the TOE to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU helping to address the threat.

T.Tests is addressed by O.Reliability, OE.Manufacturing and OE.Test_Points. If the TOE provides a reliable service as required by O.Reliability, and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the TOE can neither enter any invalidated test mode nor have any back door. OE_Test_Points requires removal of commands, actions and test points before the end of the manufacturing phase, ensuring that they cannot be used to attack the TOE during the operational phase. Hence, the related threat will be mitigated.

A.Activation is upheld by OE.Activation.

A.Approv_Workshops is upheld by OE.Approv_Workshops.

A.Card_Availability is upheld by OE.Card_Availability.

A.Card_Traceability is upheld by OE.Card_Traceability.

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

A.Controls is upheld by OE.Controls.

A.Driver_Card_Unique is upheld by OE.Driver_Card_Unique.

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

A.Compliant_Drivers is upheld by OE.Compliant_Drivers.

A.Inspections is upheld by OE.Regular_Inspection.

A.Type_Approved_Dev is upheld by OE.Type_Aprroval_MS.

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.

7.2 Security requirements rationale

7.2.1 Rationale for SFRs' dependencies

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

SFR	Dependencies	Rationale
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_ACC.1/SW-Upgrade	FDP_ACF.1	Satisfied by FDP_ACF.1/SW-Upgrade
FDP_ACF.1/SW-Upgrade	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1/SW-Upgrade FMT_MSA.3 is not fulfilled but justified: For a SW update and a SW parameter update, the patch data are accepted only together with the corresponding credentials, which contain all information needed for verification. So, it is not necessary to initialize any static attributes.
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, FTP_ITC.1 or FTP_TRP.1, FPT_TDC.1	Satisfied by FDP_ACC.1(5:IS), FTP_ITC.1(1:MS, 2:TC & 4:TC) and FPT_TDC.1(1&2)
FDP_ITC.2/SW-Upgrade	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1	Satisfied by FDP_ACC.1/SW-Upgrade

	FPT_TDC.1	FTP_ITC.1 or FTP_TRP.1 is not fulfilled, but justified: For a SW update and SW parameter update, the patch data are accepted only together with the corresponding credentials, which contain all information needed for verification. So, it is not necessary to establish trusted channel or trusted path. Satisfied by FPT_TDC.1/SW-Upgrade
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(1:MS)
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
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/SW-Upgrade	-	-
FPT_TST.1	-	-
FTP_ITC.1(1:MS)	-	-
FCS_COP.1/SW-Upgrade	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied by FDP_ITC.2/SW-Upgrade Satisfied by FCS_CKM.4/SW-Upgrade
FCS_CKM.4/SW-Upgrade	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.2/SW-Upgrade

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, 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, FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_RNG.1	-	-
FIA_ATD.1(2:MS)	-	-
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
FPT_TDC.1(1)	-	-
FTP_ITC.1(2:TC)	-	-

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, 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)	-	-

7.2.2 Security functional requirements rationale

The SFR rationale is taken from BSI-CC-PP-0094-2017 ([PPT] section 7.2.2).

		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	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(1:FIL)	Subset access control	x									
FDP_ACF.1(1:FIL)	Security attribute based access control	x									
FDP_ACC.1(2:FUN)	Subset access control	x						x	x	x	
FDP_ACF.1(2:FUN)	Security attribute based access control	x						x	x	x	
FDP_ACC.1(3:DAT)	Subset access control	x									
FDP_ACF.1(3:DAT)	Security attribute based access control	x									
FDP_ACC.1(4:UDE)	Subset access control	x			x					x	
FDP_ACF.1(4:UDE)	Security attribute based access control	x			x					x	
FDP_ACC.1(5:IS)	Subset access control	x						x	x		
FDP_ACF.1(5:IS)	Security attribute based access control	x						x	x		
FDP_ACC.1/SW-Upgrade	Subset access control	x									
FDP_ACF.1/SW-Upgrade	Security attribute based access control	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_ITC.2/SW-Upgrade	Import of user data with security attributes										x
FDP_ITT.1	Basic internal transfer protection						x	x	x		
FDP_RIP.1	Subset residual information protection	x						x	x		
FDP_SDI.2(1)	Stored data integrity monitoring and action			x		x	x		x		
FDP_SDI.2(2)	Stored data integrity monitoring and action							x	x		
FIA_AFL.1(1:TCL)	Authentication failure handling			x	x				x		
FIA_AFL.1(2:TCR)	Authentication failure handling			x	x				x		
FIA_AFL.1(3:MS)	Authentication failure handling			x	x				x		
FIA_ATD.1(1:TC)	User attribute definition			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 before any action	x	x	x	x					x	
FMT_MSA.1	Management of security attributes	x								x	
FMT_MSA.3(1:FIL)	Static attribute initialization	x									
FMT_MSA.3(2:FUN)	Static attribute initialization	x						x	x	x	
FMT_MSA.3(3:DAT)	Static attribute initialization	x									
FMT_MSA.3(4:UDE)	Static attribute initialization	x									
FMT_MSA.3(5:IS)	Static attribute initialization	x						x	x		
FMT_MOF.1(1)	Management of security functions	x				x	x	x	x		
FMT_MOF.1(2)	Management of security functions	x							x		
FMT_MOF.1(3)	Management of security functions	x			x						
FMT_MOF.1(4)	Management of security functions	x			x						
FMT_MOF.1(5)	Management of security functions	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		
FPT_TDC.1/SW-Upgrade	Inter-TSF basic TSF data consistency										x
FTP_ITC.1(1:MS)	Inter-TSF trusted channel									x	
FCS_COP.1/SW-Upgrade	Cryptographic operation										x
FCS_CKM.4/SW-Upgrade	Cryptographic key destruction										x
FCS_CKM.1(1)	Cryptographic key generation				x					x	
FCS_CKM.2(1)	Cryptographic key distribution				x					x	
FCS_CKM.4(1)	Cryptographic key destruction				x					x	
FCS_COP.1(1:AES)	Cryptographic operation				x					x	
FCS_COP.1(2:SHA-2)	Cryptographic operation				x					x	
FCS_COP.1(3:ECC)	Cryptographic operation				x					x	
FCS_RNG.1	Random number generation				x					x	
FIA_ATD.1(2:MS)	User attribute definition				x					x	
FIA_UAU.1(1:TC)	Timing of authentication				x					x	
FIA_UAU.2(1:MS)	User authentication before any action				x					x	

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Exchange	O.Software_Update
FPT_TDC.1(1)	Inter-TSF basic TSF data consistency							x	x		
FDP_ITC.1(2:TC)	Inter-TSF trusted channel									x	
FCS_CKM.1(2)	Cryptographic key generation									x	
FCS_CKM.2(2)	Cryptographic key distribution									x	
FCS_CKM.4(2)	Cryptographic key destruction									x	
FCS_COP.1(4:TDES)	Cryptographic operation									x	
FCS_COP.1(5:RSA)	Cryptographic operation									x	
FCS_COP.1(6:SHA-1)	Cryptographic operation									x	
FIA_UAU.1(2:TC)	Timing of authentication				x						
FPT_TDC.1 (2)	Inter-TSF basic TSF data consistency							x	x		
FTP_ITC.1	Inter-TSF trusted channel									x	

Table 13: Coverage of Security Objectives for the TOE by SFR

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

Security 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 unauthorized code).

	FDP_ACC.1/SW-Upgrade FDP_ACF.1/SW-Upgarde	Provides authentication for software updates.
	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 authenticated before allowing any other action.
	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 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 unauthorized 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_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 unauthorized 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 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 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_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_ATD.1(2:MS)	These attributes identify the motion sensor 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 authenticated before allowing any other action.
	FMT_MOF.1(3)	Restricts the ability to carry out company locks management to company cards.
	FMT_MOF.1(4)	Restricts the ability to monitor control activities to control cards.
	FMT_MOF.1(5)	Restricts access to the download functions.
	FMT_MTD.1	Restricts the ability to carry out manual time setting to workshop cards.
	FCS_CKM.1(1)	Key generation to support the authentication process.
	FCS_CKM.2(1)	Key distribution to support the authentication process.
	FCS_CKM.4(1)	Key destruction when temporary keys are no longer required.

	FCS_COP.1(1:AES)	Cryptographic algorithm used to support authentication.
	FCS_COP.1(2:SHA-2)	Cryptographic algorithm used to support authentication.
	FCS_COP.1(3:ECC)	Cryptographic algorithm used to support authentication.
	FCS_RNG.1	Random numbers are generated in support of cryptographic key generation for authentication.
	FIA_UAU.1(1:TC & 2:TC)	A tachograph card has to be successfully authenticated.
	FIA_UAU.2(1:MS)	A motion sensor has to be successfully authenticated before allowing any action.
O.Integrity	FAU_STG.1	Protects the stored audit records from unauthorized deletion.
	FDP_ETC.2	Provides export of user data with security attributes using the User_Data_Export SFP.
	FDP_SDI.2(1)	Monitors user data stored 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 user data stored 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).

	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 unauthorized 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.
	FDP_MSA.3(2:FUN)	Supports the Function SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FDP_MSA.3(5:IS)	Supports the Input Sources SFP 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 unauthorized 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.
	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 user data stored 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.
	FDP_MSA.3(2:FUN)	Supports the Function SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FDP_MSA.3(5:IS)	Supports the Input Sources SFP 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).
	DP_ACC.1(4:UDE) FDP_ACF.1(4:UDE)	Restricts the ability to read remote early detection communication facility data to control cards.
	FDP_ETC.2	Provides export of user data with security attributes using the User_Data_Export SFP.
	FDP_ITC.2	Handles integrity and authenticity errors in data imported with security attributes.
	FIA_ATD.1(1:TC)	Defines user attributes for tachograph cards.
	FIA_ATD.1(2:MS)	These attributes identify the motion sensor connected to the vehicle unit.
	FIA_UAU.6	Periodically reauthenticates Tachograph cards.
	FIA_UID.2	Connected devices are successfully 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.
	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(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.
	FCS_COP.1(4:DES)	Cryptographic algorithm used to support authentication.

	FCS_COP.1(5:RSA)	Cryptographic algorithm used to support authentication.
	FCS_COP.1(6:SHA-1)	Cryptographic algorithm used to support authentication.
	FIA_UAU.1(2:TC)	Tachograph card has to be successfully authenticated.
O.Software_Update	FDP_ITC.2	Provides verification of imported software updates.
	FDP_ITC.2/SW-Upgrade	Provides import of software update data from outside of the TOE, using the defined conditions for the software update acceptance.
	FPT_TDC.1/SW-Upgrade	Capability to ensure the consistency of data for the update.
	FCS_COP.1/SW-Upgrade	Cryptographic algorithm used to support software updates.
	FCS_CKM.4/SW-Upgrade	Specifies the requirements for key destruction.

7.2.3 Security Assurance Requirements Rationale

The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [EU] Annex 1 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: entry ‘Attacker’). This decision represents a part of the conscious security policy for the recording equipment required by the Regulation [EU] and reflected by the current ST.

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

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package.

Component	Dependencies required by CC Part 3	Dependency fulfilled 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 14: SARs' dependencies (additional to EAL4 only)

7.2.4 Security Requirements – Internal Consistency

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

a) SFRs

The dependency analysis in section 7.2.1 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately explained.
All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior 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 [EU], 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 section 7.2.3 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been

shown not to arise in sections 7.2.1 and 7.2.3. Furthermore, as also discussed in section 7.2.3, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

8 TOE Summary Specification

In addition to the requirements of CC [CC1], the current ST defines not only the TOE Security Functionality (TSF) but also Security Functions (SF.xxx) whose combination constitutes the TOE Security Functionality.

8.1 TOE Security Functions

For the definition of the Security Functions (SF_xxx) related to the SC, it is referred to the Security Target [SCST], sec. 7. Security Functions of the SC are relevant for the EFAS-4.10. The following sections provide a survey of the Security Functions of the TOE under consideration of the requirements in the protection profile [PPT] including all extensions and operations made in sec. 6.1.

8.1.1 SF.ACS Security Attribute Based Access Control

SF.ACS controls the access to the data and functions and enforces the File_Structure SFP, Function SFP, Data SFP, User_Data_Export SFP, Input Sources SFP as required by FDP_ACC.1(*), FDP_ACF.1(*) and FDP_ITC.1, FDP_ITC.2 and FMT_MSA.3(*).

SF.ACS implements the File_Structure SFP for tachograph application and data files structure (FDP_ACC.1(1:FIL), FDP_ACF.1(1:FIL)) and enforces the Function SFP, Data SFP, User_Data_Export SFP on subjects, objects, and operations as described in 6.1.1.3 (FDP_ACC.1(2:FUN), FDP_ACF.1(2:FUN), FDP_ACC.1(3:DAT), FDP_ACF.1(3:DAT), FDP_ACC.1(4:UDE), FDP_ACF.1(4:UDE)).

SF.ACS ensures that cards cannot be released before relevant data have been stored to them:

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

SF.ACS ensures that user data may only be processed from the right input sources:

- vehicle motion data, as required by FPT_TDC.1(1), FPT_TDC.1(2) for 2nd resp. 1st generation
- VU's real time clock, as required in FPT_STM.1
- recording equipment calibration parameters, as required in FDP_ITC.1
- tachograph cards, as required by FPT_TDC.1(1), FPT_TDC.1(2) for 2nd resp. 1st generation, supported by
- users' inputs

in accordance with the requirements FDP_ACC.1(5:IS), FDP_ACF.1(5:IS), FPT_STM.1, FDP_ITC.1,FDP_ITC.2, FPT_TDC.1(1), FPT_TDC.1(2) for 2nd resp. 1st generation.

SF.ACS ensures that user data (entered manually) may only be entered for the period last card withdrawal — current insertion in accordance with the requirements FDP_ACC.1(4:UDE), FDP_ACF.1(4:UDE).

SF.ACS controls the access to the data and functions of the TOE and prevents the possibility to analyze or debug TOE's software (inclusive the cryptographic keys) in the field after the EFAS-4.10 activation (ADV_ARC). This includes that SF.ACS allows the calibration functions only in calibration mode in accordance with FMT_SMF.1.

Inputs from external sources are not accepted as executable code (as required in FDP_ITC.2, FDP_ACC.1(5:IS), FDP_ACF.1(5:IS)).

Update of the security and non-security relevant software components is only possible after the corresponding authentication and verification with help of credentials as required in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade.

Nobody may change the public/private keys and the KM_{VU} after their insertion during the production process. Nobody may read the private keys and the KM_{VU} after their insertion during the production process in full compliance with FMT_MSA.1, FMT_MSA.3(*).

In doing so, SF.ACS directly supports FCS_COP.1(5:RSA) for 1st generation and FCS_COP.1(3:ECC) for 2nd generation.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.2 SF.SECAUDIT Audit

SF.SECAUDIT generates an audit record inter alia of the following auditable events: start-up and shutdown of the audit functions and all other events described below. The audit function will be started up as soon as the TOE has external power supply after activation and shut down, when the external power supply is interrupted. In this case SF.SECAUDIT records within each audit record at least the information date and time of begin and end of the event and the type of event.

SF.SECAUDIT, for events impairing the security of the EFAS-4.10, records those events with associated data as required in FAU_GEN.1.

Upon detection of a data integrity error, SF.SECAUDIT generates an audit record about it (FDP_SDI.2(1)) or FDP_SDI.2(2)

SF.SECAUDIT enforces audit records storage rules in a way as required in FDP_ETC.2. In particular, SF.SECAUDIT supports the enforcing the User Data Export SFP and provides the capability to read recorded information possibly secured with help of associated security attributes.

SF.SECAUDIT stores audit records generated by the motion sensor in its data memory as required by FAU_GEN.1. FAU_SAR.1 specifies the capability to read audit records.

SF.SECAUDIT shall enforce the following rules for monitoring audited events known to indicate a potential security violation:
Accumulation or combination of

- security breach attempts like

  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorized change of motion sensor,
  - card data input integrity error,
  - stored user data integrity error,
  - internal data transfer error,
  - unauthorized case opening,
  - hardware manipulation,
- last card session not correctly closed,
- motion data error event,
- power supply interruption event,
- communication error with the remote communication facility
- absence of position information from GNSS receiver
- time conflict
- VU internal fault.

in a way which covers FAU_GEN.1.

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

SF.SECAUDIT is also able to provide reliable **time stamps** based on the RTC time information (as required in FPT_STM.1) for its own use.

SF.SECAUDIT overwrites the oldest stored audit records if the audit trail is full as required in FAU_STG.4.

The SF is effective only with support of the Security Functions of the SC, see Statement of Compatibility.

8.1.3 SF.EX_CONF

Confidentiality of Data Exchange

SF.EX_CONF protects the confidentiality of secret data being exchanged between the TOE and the external subjects

- Tachograph cards,
- motion sensor,
- Security Server.

For this purpose, encryption based on symmetric AES cryptography is used.
The data transfer between the EFAS-4.10 and

- Tachograph cards are secured according to [EU] CSM_186 (AES in CBC mode) as required in FCS_COP.1(1:AES) using a trusted channel as required in FTP_ITC.1(2:TC). The confidentiality is applicable to elementary file Sensor_Installation_Data of DF Tachograph_G2 read from workshop card only. No confidentiality is required for other data. No confidentially is required for 1st generation tachograph cards because 1st generation workshop cards are rejected by the VU according to [EU] req. (18).
- The motion sensor is secured according to [EU] CSM_216 (AES in CBC mode) as required in FCS_COP.1(1:AES). using a trusted channel as required in FTP_ITC.1(1:MS).

The software update patch contains two files. The firmware image file is encrypted by the Security Server with AES keys $K_{Firmware}$-SC and $K_{Firmware}$-MC. The credentials file is encrypted with the unique keys of the associated VUs ($KENC_{UpdateVu}$).

The SW upgrade credentials are secured with AES-cryptographic mechanisms based on VU-specific keys according to the BSI recommendations in [TR-02102] - AES in CBC mode with key length 128 bits as required in FCS_COP.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade.

The SW-upgrade and parameter update image files are secured with AES-cryptographic mechanisms based on keys read from the decrypted credentials according to BSI recommendations in [TR-02102] - AES in COUNTER mode with key length 128 bits as required in FCS_COP.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade.

The cryptographic keys used for securing the data transfer as session keys are generated during the preceding mutual authentication process between the EFAS-4.10 and the external subject (see SF.IA_KEY and SF.GEN_SKEYS).

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.4 SF.EX_INT

Integrity and Authenticity of Data Exchange

SF.EX_INT protects the authenticity and integrity of data being exchanged between the TOE and the external subjects

- tachograph card,
- motion sensor,
- Security Server,
- external device and
- downloading equipment.

The data transfer between the EFAS-4.10 and

- tachograph cards is secured as required in FCS_COP.1(4:TDES), FCS_COP.1(1:AES). SF.EX_INT verifies the integrity and authenticity of data imported from tachograph cards using a trusted channel according to [EU] CSM_021 as required in FTP_ITC.1(4:TC) for communication with 1st generation tachograph cards and according to [EU] CSM_155 as required by FTP_ITC.1(2:TC) for communication with 2nd generation tachograph cards. Upon detection of card data integrity or authenticity error, SF.EX_INT generates an audit record compliant with FAU_GEN.1 and does not use the data as required in FDP_ITC.2. SF.EX_INT exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity as required in FDP_ETC.2.
- the motion sensor is secured according to ISO/DIS 16844-3 (see [ISO16844]) and as required in FCS_COP.1(1:AES) and after proper authentication as required in FIA_UAU.2(1:MS), FIA_UAU.6, FIA_UID.2. SF.EX_INT verifies the integrity and authenticity of motion data imported from the motion sensor using a trusted channel according to [EU] CSM_216 as required in FTP_ITC.1(1:MS). Upon detection of a motion data integrity or authenticity error, SF.EX_INT generates an audit record and continues to use imported data as required in FDP_ITC.2.
- downloading equipment are secured according to PKCS#1 V2.0 and with hash algorithm SHA-1 / SHA-2 as required in FCS_COP.1(5:RSA), FCS_COP.1(6:SHA-1), FCS_COP.1(3:ECC), FCS_COP.1(2:SHA-2). (Note: The source equipment (EFAS-4.10) identification and its security certification (Member state and equipment) are also downloaded. The verifier of the data must possess a trusted European public key to verify the certificate chain.)

SF.EX_INT is able to generate evidence of origin for transmitted data, to relate the VU identity and to provide a capability to verify the evidence of origin of information as required in FCO_NRO.1.

SF.EX_INT verifies the authenticity and integrity of received software upgrade data as required by FDP_ITC.2/SW-Upgrade.

The software update patch contains two files, one image file and one credential file.

The integrity of SW-upgrade credentials are secured with AES-cryptographic mechanisms based on VU-specific keys according to the BSI recommendations in [TR-02102], - AES in CBC mode with key length 128 bits (CMAC) as required in FCS_COP.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade.

The MC-firmware part of the image file or the MC-SW-parameter part of the image file is encrypted by the Security Server (see SF.EX_CONF above) and secured additionally with SHA-256 as required in FCS_COP.1(2:SHA-2).

The SC-firmware part of the image file is encrypted by the Security Server (see SF.EX_CONF above) and secured additionally with SHA-256 as required in FCS_COP.1(2:SHA-2). The credential file is encrypted (see SF.EX_CONF above) and

secured additionally (AES CMAC) with the unique key of the associated VUs ($KAUTH_{UpdateVu}$).

The cryptographic keys used for securing the data transfer for tachograph cards are session keys which are generated during the preceding mutual authentication process between the EFAS-4.10 and the tachograph card (see SF.IA_KEY and SF.GEN_SKEYS).

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.5 SF.GEN_SKEYS Generation of Session Keys

SF.GEN_SKEYS generates session keys for symmetric cryptography used for protecting the confidentiality, integrity and authenticity of data exchanged between the TOE and the external world

- tachograph card,
- motion sensor,
- external device.

SF.GEN_SKEYS enforces that the key material meets the following requirements:

- random numbers generated by the EFAS-4.10 and used in the key generation process have a high quality FCS_RNG.1 and
- symmetric keys generated by the TOE are checked by the TSF with regard to their cryptographic strength, and only cryptographically strong keys (with the required key length) will be accepted by the TSF.
- Calculation of a session key based on secrets stored in the TSF and in the external device and based on dynamic data portions provided by both components at connection time.

SF.GEN_SKEYS generates and managed session keys in accordance with the cryptographic key derivation algorithms as specified in [CSM] as required in FCS_CKM.1(*), FCS_CKM.2(*) and FCS_CKM.4(*). The deletion of keys takes place due value overwriting with random values.

Random numbers FCS_RNG.1 are generated by the random number generator of the SC. SF.GEN_SKEYS is directly connected with SF.IA_KEY which realizes the internal and external authentication process.

SF.GEN_SKEYS destroys cryptographic keys in accordance with a specified cryptographic key destruction method as implemented in the SC (overwriting with random values) as required by FDP_RIP.1.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.6 SF.GEN_DIGSIG

Generation of Digital Signatures optionally with Encryption

SF.GEN_DIGSIG provides a digital signature generation functionality based on asymmetric cryptography, as required in FCS_COP.1(5:RSA) and FCS_COP.1(3:ECC). The digital signature function will be used for several purposes with different signature keys and different formats for the digital signature input:

- Explicit generation of digital signatures of data using the signature scheme with appendix (signature generation operation) according to the standard PKCS#1 V2.0 and with hash algorithm SHA-1 for 1st generation tachograph cards.
- Within authentication processes between the EFAS-4.10 and tachograph cards for the creation of authentication tokens using the signature scheme with message recovery (signature generation operation) according to the standard ISO 9796-2 (see [ISO9796]) and with hash algorithm SHA-1 for 1st generation tachograph cards.
- Explicit generation of digital signatures of data using algorithm ECDSA with hash algorithm SHA-2 according to [EU] CSM_233 for 2nd generation tachograph cards.
- Within authentication processes between EFAS-4.10 and tachograph cards for the creation of authentication tokens with hash algorithm SHA-2 according to [EU] CSM_155 for 2nd generation tachograph cards.

SF.GEN_DIGSIG is able to generate evidence of origin for transmitted data, to relate the VU identity and to provide a capability to verify the evidence of origin of information as required in FCO_NRO.1.

Random numbers FCS_RNG.1 necessary for the generation of digital signatures are generated by the SC.

SF.GEN_DIGSIG provides the functionality to encrypt and decrypt data based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024 or the ECC algorithm with a key length of 256-512 bits. The decryption function will be used for the following purpose:

- Within the authentication process between the EFAS-4.10 and the tachograph card for the generation of authentication tokens using the decryption primitive according to the standard PKCS#1 V2.0 or according to [EU] CSM_233.

Signatures are generated and verified in compliance with FCS_COP.1(5:RSA) and FCS_COP.1(3:ECC).

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.7 SF.VER_DIGSIG Verification of Digital Signatures optionally with Decryption

SF.VER_DIGSIG provides a functionality to verify digital signatures based on asymmetric cryptography, as required in FCS_COP.1(5:RSA), FCS_COP.1(3:ECC). The SF to verify a digital signature will be used for several purposes with different keys and different formats for the digital signature input:

- Explicit verification of digital signatures of data using the signature scheme with appendix (signature verification operation) according to the standard PKCS#1 V2.0 and with hash algorithm SHA-1 for 1st generation tachograph cards.
- Within authentication processes between EFAS-4.10 and tachograph cards for the verification of authentication tokens using the signature scheme with message recovery (signature verification operation) according to the standard ISO 9796-2 (see [ISO9796]) and with hash algorithm SHA-1 for 1st generation tachograph cards.
- Within the verification and unwrapping of imported certificates using the signature scheme with message recovery (signature verification operation) according to the standard ISO 9796-2 (see [ISO9796]) and with hash algorithm SHA-1 for 1st generation tachograph cards.
- Explicit verification of digital signatures of data using AES in CMAC mode according to [EU] CSM_187 for 2nd generation tachograph cards.
- Within authentication processes between EFAS-4.10 and tachograph cards for the verification of authentication tokens according to [EU] CSM_155 for 2nd generation tachograph cards.
- Within the verification and unwrapping of imported certificates according to [EU] CSM_150 for 2nd generation tachograph cards.

SF.VER_DIGSIG provides the functionality to encrypt data based on asymmetric cryptography. The encryption function will be used for the following purpose:

- Within the authentication processes between EFAS-4.10 and tachograph card for the verification of authentication tokens using the decryption primitive according to the standard PKCS#1 V2.0 or according to [EU] CSM_155.

Signatures are verified in compliance with FCS_COP.1(5:RSA) and FCS_COP.1(3:ECC)..

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.8 SF.DATA_INT Stored Data Integrity Monitoring and Action

SF.DATA_INT protects the integrity of user data. User data include cryptographic keys. User data is stored

- in the data memory of the SC,
- in the data memory of the main processor. SF.DATA_INT protects data by an AES CMAC before transmitting them from the SC to the MC flash memory as required by FDP_ITT.1. SF.DATA_INT protects data by an AES CMAC before transmitting them from the SC to the MC flash memory as required by FDP_ITT.1.

Monitoring

SF.DATA_INT includes hardware mechanisms of the SC which protect user data against manipulation. Such hardware mechanisms are features within the design and construction which make reverse-engineering and tamper attacks more difficult. These features comprise dedicated shielding techniques and different scrambling features for the memory blocks.

SF.DATA_INT protects the user data stored in the data memory of the MC by AES CMAC values which are calculated about the data and stored in the MC together with the data. The CMAC-key is stored in the SC, also CMAC-verification of stored data is done in the SC in accordance with data integrity protection as defined in FCS_COP.1/SW-Upgrade.

SF.DATA_INT protects the user data stored in the SC by checksums and/or double storage.

The integrity of the user data is checked regularly and before data download. SF.DATA_INT is implemented with ensuring the fulfilment of the SFRs FDP_SDI.2(*) and FAU_STG.1. Upon detection of a stored user data integrity error, SF.DATA_INT generates an audit record in accordance with FAU_GEN.1 and FAU_STG.1. SF.DATA_INT overwrites the oldest stored audit records, if the audit trail is full.

If a cryptographic key (public or private) is corrupted, then the cryptographic key is not used.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.9 SF.IA_KEY Key Based User / TOE Authentication

The following subjects can be identified and authenticated with regard to the TOE by means of a challenge response procedure using random numbers (external authentication).

a) **Initial motion sensor identification and authentication (pairing, calibration)**: The EFAS-4.10 authenticates the motion sensor it is connected to:

- at motion sensor connection,
- at each calibration of the recording equipment,
- at power supply recovery.

Authentication is mutual and triggered by the EFAS-4.10 before allowing any other TSF-mediated actions in accordance with FIA_UAU.2(1:MS) (the identification as required in FIA_UID.2 takes place too). I.e. the TOE itself is also authenticated towards the motion sensor by means of a challenge-response procedure. Hereby, SF.IA_KEY detects and prevents use of authentication data that has been forged by or copied from any other user of the TSF (FIA_UAU.3), maintains the list of security attributes belonging to individual users as required by FIA_ATD.1(2:MS) and supports enforcing the Function SFP and Input Sources SFP to avoid value changes of security attributes (FMT_MTD.1, FMT_MSA.1, FMT_MSA.3(2:FUN) and FMT_MSA.3(5:IS).

b) **User identification and authentication via tachograph card:** The EFAS-4.10 identifies and authenticates its users at card insertion before allowing any other TSF-mediated actions in accordance with FIA_UID.2, FIA_UAU.1(1:TC), FIA_UAU.1(2:TC) and FIA_UAU.5. The authentication is mutual and triggered by the EFAS-4.10. I.e. the TOE itself is also authenticated towards the tachograph card by means of a challenge-response procedure. Hereby, SF.IA_KEY detects and prevents use of authentication data that has been forged

by or copied from any other user of the TSF (FIA_UAU.3), maintains the list of security attributes belonging to individual users as required by FIA_ATD.1(1:TC) and supports enforcing the Function SFP to avoid value changes of security attributes (FMT_MSA.1). Authentication is performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. After this the EFAS-4.10 maintains the following roles DRIVER (driver card), CONTROLLER (control card), WORKSHOP (workshop card), COMPANY (company card) and UNKNOWN (no card inserted) as required by FMT_SMR.1.

Note: The external authentication of the EFAS-4.10 corresponds to the internal authentication of the tachograph card and vice versa.

c) **External device identification and authentication:**
Before allowing any further interaction, the EFAS-4.10 shall successfully authenticate the external device. Authentication shall be mutual. I.e. the TOE itself is also authenticated towards the external device by means of a challenge-response procedure.

Cryptography:
In the cases

a) SF.IA_KEY uses symmetric cryptography according to ISO/DIS 16844-3 (see [ISO16844]), using TDES in a way as required in FCS_COP.1(4:TDES), FCS_COP.1(1:AES).

b) SF.IA_KEY uses asymmetric cryptography according to ISO 9796-2 (see [ISO9796]) and with hash algorithm SHA-1 for digital signatures with partial recovery, using RSA in a way as required by FCS_COP.1(5:RSA), FCS_COP.1(3:ECC).

c) SF.IA_KEY makes use of symmetric cryptography for mutual authentication between the VU and the external device as well as for data integrity during data exchange between the EFAS-4.10 and the external device.

Cryptographic Protocol:
In the case a):
SF.IA_KEY applies the **initial identification and authentication** as described in chapter 7.4 of ISO/DIS 16844-3 (see [ISO16844]).
The extended serial-number N_S of the motion sensor is sent to the EFAS-4.10. The EFAS-4.10 encrypts the extended serial number N_S of the motion sensor, using the "identification key" K_{ID}. The motion sensor transmits a pairing key K_P which is encrypted with the "master key" K_M to the EFAS-4.10.

The "session key" K_S is transmitted from the EFAS-4.10 to the motion sensor encrypted with the "pairing key" K_P. Pairing information is transmitted from the EFAS-4.10 to the motion sensor encrypted with the "pairing key" in a way as required in FCS_CKM.2(*) and FDP_ETC.2.
The initial identification and authentication leads to the generation of a "session key" K_S which secures a challenge response mechanism for the following communication between the EFAS-4.10 and the motion sensor.

In the case b):

SF.IA_KEY operates as described in [EU], Appendix 11 (“Get Challenge Operation”, “Generation of a digital signature” and “Encryption” for the internal authentication, “Random generation of the EFAS-4.10”, “Decryption” and “Verification of a digital signature” for the external authentication.
The private key necessary on the EFAS-4.10´s side for authentication purposes is stored on the EFAS-4.10 and is implicitly connected with the corresponding commands. The access to the keys is controlled by the Function SFP, which is realized by SF.ACS.

The combination of a successful internal authentication process followed by a successful external authentication process leads to the generation of a new session key (with sequence counter sent) which will be used to secure the following data transfer. The generation of session keys is task of SF.GEN_SKEYS.
For the tachograph card type “Workshop Card” the mutual authentication process described above is only possible after a successful preceding PIN based user authentication between user and Workshop Card. Since EFAS-4.10 only transfers the PIN from the keypad to the Workshop Card this belongs not to the TSF of EFAS-4.10.
Case c):
SF.IA_KEY uses a challenge response protocol with TDES-cryptographic mechanisms for calculation of a session key based on secrets stored in the SC and in the external device and based on dynamic data portions provided by both components at connection time (mutual authentication mechanism). Correct calculation and usage of the session key – shown in further communication - serves as proof of authenticity. Without proper authentication, communications will be aborted.

Unsuccessful authentication:
Case a):
After consecutive unsuccessful authentication attempts (specified in the assurance class development by manufacturer and not more than 20) have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorized (i.e. while not during a calibration of the recording equipment), SF.IA_KEY

- generates an audit record of the event as required by FAU_GEN.1,
- warns the user,
- continues to accept and use non secured motion data sent by the motion sensor

as required by FIA_AFL.1(3:MS).

Case b):
After 5 consecutive unsuccessful authentication attempts have been detected, SF.IA_KEY:

- generates an audit record of the event as required by FAU_GEN.1,
- warns the user,
- assumes the user as UNKNOWN, and the card as non-valid as required by FIA_AFL.1(1:TCL).

Case c)
In case of unsuccessful authentication the user will be informed as required by FIA_AFL.1(2:TCR).

Re-authentication and re-identification:

Case a):
SF.IA_KEY periodically (period specified in the assurance class development by manufacturer and more frequently than once per hour) re-identifies and re-authenticates the connected motion sensor as required by FIA_UAU.6, and ensures that the motion sensor identified during the last calibration of the recording equipment has not been changed. Thereby the session key generated during the initial identification and authentication is used.
SF.IA_KEY is able to establish, for every interaction, the identity of the motion sensor to which it is connected as required by FIA_UID.2. The identity of the motion sensor consists of the sensor approval number and the sensor serial number.

Case b):
SF.IA_KEY re-authenticates the user using the cryptography described above at “cryptographic protocol” at power supply recovery, periodically or after occurrence of specific events (specified in the assurance class development by the manufacturers and more frequently than once per day) as required by FIA_UAU.6.
SF.IA_KEY permanently and selectively tracks the identity of two users, by monitoring the tachograph cards inserted in the driver slot and the co-driver slot of the equipment respectively.
Case c):
For every interaction with an external device, SF.IA_KEY is able to establish the device identity.

The Identity of the TOE and the corresponding public/private key material is brought-in during production; nobody may change these attributes of the TSF after leaving the production environment. The same applies to other not VU-specific static security attributes. SF.IA_KEY detects and prevents use of authentication data that has been forged by any user or copied from any other user.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.10 SF.INF_PROT
Residual Information Protection

SF.INF_PROT ensures that any previous information content of a resource used for operations in which security relevant material is involved in volatile memory in the SC of the EFAS-4.10, is explicitly erased (overwriting with random values) upon the allocation of a new resource as required in FDP_RIP.1. Furthermore temporarily active keys are destroyed in accordance with FCS_CKM.4 (*) as implemented by SF.GEN_SKEYS. The deletion of keys takes place due value overwriting with random values.

Other temporary storage objects can be re-used without implying inadmissible information flow.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.11 SF.FAIL_PROT Failure and Tampering Protection
SF.FAIL_PROT preserves a secure state when the following types of failures occur:

- Detection of specified values of the power supply, including cut-off.

In the case described above, SF.FAIL_PROT

- generates an audit record (except when in calibration mode) compliant with FAU_GEN.1,
- preserve the secure state of the EFAS-4.10,
- maintain the security functions, related to components or processes still operational,
- preserve the stored data integrity

in compliance with FPT_FLS.1.

In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, SF.FAIL_PROT resets the EFAS-4.10 clearly as required by FPT_PHP.2.

SF.FAIL_PROT provides the capability to determine whether **physical tampering** has occurred in compliance with FPT_PHP.3. The EFAS-4.10 is designed such that the case open supervision circuit detects any “regular” case opening while the external supply voltage is connected or not and a corresponding audit record is generated (the audit record is generated and stored after power supply reconnection as required by FAU_GEN.1). All other physical tampering attempts can be easily detected by visual inspection.

After its activation, the EFAS-4.10 detects specified hardware manipulation (specified in the assurance class development, e.g. manipulation of the real time clock generating time stamps). In the case of sabotage of the real time clock, SF.FAIL_PROT generates an audit record as required by FAU_GEN.1 and the EFAS-4.10 will be blocked (other cases are specified in the assurance class development).

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.12 SF.SELFTEST Self Test

SF.SELFTEST provides the capability of running self tests during initial start-up, and during normal operation to verify its correct operation (FPT_TST.1).
The EFAS-4.10 self tests include the verification of the integrity of security data and the verification of stored executable code.
Security data are stored

- in the data memory of the SC

Executable code is stored

- in the program memory of the SC
- in the program memory of the main processor.

The SC verifies the integrity of security data and executable code stored in the memory of the SC and of respective memory of the main processor. The SC additionally verifies the integrity of the executable code of the main processor as required by FPT_TST.1.

SF.SELFTEST ensures that only allowed tests are available (FMT_MOF.1(*)) and preserves a secure state in the case that failures take place (FPT_FLS.1).

Upon detection of an internal fault during self test, SF.SELFTEST analyses and classifies the faults.

Classification:

- Class 0: Fatal error, main processor, SC, ROM, Flash defect. EFAS-4.10 operation and data logging not possible.
- Class 1: Serious faults in non-essential components of the EFAS-4.10. Restricted EFAS-4.10 operation possible (data logging not possible or only possible in an un-secured way).
- Class 2: Warning. Single components of the EFAS-4.10 are (temporarily) not available. EFAS-4.10 operation is possible (with data logging).
- Class 3: No error.

An audit record is generated, if necessary in accordance with FAU_GEN.1.

On failures - as required by FPT_FLS.1 - the TOE preserves a secure state.

All commands, actions or test points, specific to the testing needs of the manufacturing phase of the EFAS-4.10 are disabled or removed before the EFAS-4.10 is activated in accordance with FMT_MOF.1(*). It is not possible to restore them for later use.
The SF is supported by SF.DATA_INT.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.1.13 SF.UPDATE VU Software Upgrade

SF.UPDATE performs updates of software components in a secure way. If software components or parameters have to be updated, an authentication with the workshop card is required to allow the update. If the needed authentication was not successful (FDP_ACC.1/SW-Upgrade) no further checks take place.

The software update and SW parameter update mechanisms which are implemented ensure that the update is performed only if the integrity and the authenticity of the patch data is confirmed by means of update credentials (FDP_ACF.1/SW-Upgrade, FPT_TDC.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade). SF.UPDATE decrypts the loaded software and parameter components (FCS_COP.1/SW-Upgrade) and exchanges the corresponding parts of the software.

In particular, the VU Software Upgrade takes place in the following manner:
The software update or parameter patches contains two files.
The firmware image or parameter image file contains an unencrypted compatibility header and an encrypted main part. The latter is encrypted (AES in COUNTER mode) with AES keys $K_{Firmware}$-MC and $K_{Firmware}$-SC for MC and SC software, respectively.

The so called compatibility header's integrity is secured with AES-CMAC (KCOMP) which is verified and which contains a list of compatible SW versions which is verified before further decryptions and verifications take place. If the check fails, the update data is rejected. This is primarily done for user convenience to stop unintended actions before more time consuming crypto operations are done.

The credentials file is encrypted with the unique key of the associated VUs ($KENC_{UpdateVu}$) using AES in CBC mode. Only one unique VU which contains this key is able to decrypt and to verify the credentials which contain among others the keys for further steps $K_{Firmware}$-SC and $K_{Firmware}$-MC and SHA-256 integrity hash values.
In the first step, after decryption of the credentials file ($KENC_{UpdateVu}$) the integrity and authenticity of the credentials ($KAUTH_{UpdateVu}$) are verified. If all checks are positive the firmware images are decrypted (for SC and MC separately with $K_{Firmware}$-SC and $K_{Firmware}$-MC (last one also for parameters) and the integrity (and the authenticity indirectly) of the firmware image parts (SC and (MC-SW or parameter)) with SHA-256 FCS_COP.1(2:SHA-2) is verified. Only if all checks are positive, the update will take place.

SF.UPDATE destroys temporary private and secret cryptographic keys in accordance with a specified cryptographic key destruction method as implemented in the SC (overwriting with random values) as required by FCS_CKM.4/SW-Upgrade.

The SF is effective only with support of the Security Functions of the SC, see 9.

8.2 Assurance Measures

To satisfy the security assurance requirements defined in section 7.2, suitable assurance measures are employed by the developer of the TOE. For the evaluation of the TOE, the developer provides suitable documents. The documents describe the measures and include further information supporting the verification of the conformance of these measures against the claimed assurance requirements.
The following table includes a mapping between the assurance requirements and the documents including the relevant information for the correspondent requirement. The developer of the TOE provides these documents. (Note: The placeholder “xx” stands for the respective version number of the document.)

Assurance Class	**Family**	**Documentation containing the relevant information**
ADV Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD Guidance Documents	AGD_OPE.1	Part of the Operating manual EFAS-4.10
	AGD_PRE.1	Operating manual EFAS-4.10 Service and installation manual EFAS-4.10
ALC Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures

Assurance Class	Family	Documentation containing the relevant information
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: basic design
	ATE_FUN.1	Functional testing: Test specification and test records
	ATE_IND.2	Independent testing - sample: Samples of the TOE Source Code and Hardware
AVA Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis: Document Vulnerability Analysis

Table 15: Overview of Developers' TOE related Documentation

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Rationale

The SF is effective only with support of the Security Functions of the SC see 9.
The following section demonstrates that the set and combination of the defined TOE Security Functions is suitable to satisfy the identified TOE security functional requirements (SFRs). Furthermore, this section shows that each of the Security Functions is related to at least one security functional requirement.

The SFRs for the TOE of section 6.1 are related to the Security Functions of the TOE defined in section 8.1. The mapping of the SFRs for the TOE to the relevant Security Functions is done in the following.

The table below gives an overview of which Security Functions of the TOE contribute to the satisfaction of the SFRs for the TOE and the protection profile [PPT].

PP and ST Security Functional Requirements (SFR)	TOE Security Functionality (TSF)
FAU_GEN.1	SF.ACS, SF.IA_KEY, SF.SECAUDIT, SF.DATA_INT, SF.SELFTEST, SF.FAIL_PROT, SF.EX_INT
FAU_SAR.1	SF.SECAUDIT
FAU_STG.1	SF.ACS, SF.DATA_INT
FAU_STG.4	SF.SECAUDIT
FCO_NRO.1	SF.GEN_DIGSIG, SF.EX_INT
FCS_CKM.1(*)	SF.GEN_SKEYS
FCS_CKM.2(*)	SF.IA_KEY, SF.GEN_SKEYS
FCS_CKM.4(*)	SF.INF_PROT, SF.GEN_SKEYS
FCS_CKM.4/SW-Upgrade	SF.UPDATE
FCS_COP.1(1:AES)	SF.DATA_INT, SF.EX_INT, SF.EX_CONF, SF.IA_KEY
FCS_COP.1(2:SHA-2)	SF.EX_INT, SF.GEN_DIGSIG, SF.VER_DIGSIG, SF.UPDATE
FCS_COP.1(3:ECC)	SF.ACS, SF.EX_INT, SF.GEN_DIGSIG, SF.VER_DIGSIG, SF.IA_KEY
FCS_COP.1(4:TDES)	SF.EX_INT, SF.IA_KEY
FCS_COP.1(5:RSA)	SF.ACS, SF.EX_INT, SF.GEN_DIGSIG, SF.VER_DIGSIG, SF.IA_KEY
FCS_COP.1(6:SHA-1)	SF.EX_INT, SF.GEN_DIGSIG, SF.VER_DIGSIG
FCS_RNG.1	SF.GEN_SKEYS, SF.GEN_DIGSIG
FCS_COP.1/SW-Upgrade	SF.EX_CONF, SF.EX_INT, SF.DATA_INT, SF.UPDATE
FDP_ACC.1(*)	SF.ACS
FDP_ACC.1/SW-Upgrade	SF.ACS, SF.UPDATE
FDP_ACF.1(*)	SF.ACS
FDP_ACF.1/SW-Upgrade	SF.ACS, SF.UPDATE
FDP_ETC.2	SF.IA_KEY, SF.EX_INT, SF.SECAUDIT
FDP_ITC.1	SF.ACS
FDP_ITC.2	SF.ACS, SF.EX_INT
FDP_ITT.1	SF.DATA_INT
FDP_ITC.2/SW-Upgrade	SF.EX_INT, SF.EX_CONF, SF.UPDATE
FDP_RIP.1	SF.INF_PROT, SF.GEN_SKEYS
FDP_SDI.2(*)	SF.SECAUDIT, SF.DATA_INT
FIA_AFL.1(*)	SF.IA_KEY
FIA_ATD.1(*)	SF.IA_KEY
FIA_UAU.1(*)	SF.IA_KEY
FIA_UAU.2(1:MS)	SF.IA_KEY, SF.EX_INT
FIA_UAU.3	SF.IA_KEY
FIA_UAU.5	SF.IA_KEY
FIA_UAU.6	SF.IA_KEY, SF.EX_INT
FIA_UID.2	SF.IA_KEY, SF.EX_INT
FMT_MSA.1	SF.ACS, SF.IA_KEY
FMT_MSA.3(1:FIL)	SF.ACS
FMT_MSA.3(2:FUN)	SF.IA_KEY, SF.ACS

PP and ST Security Functional Requirements (SFR)	TOE Security Functionality (TSF)
FMT_MSA.3(3:DAT)	SF.ACS
FMT_MSA.3(4:UDE)	SF.ACS
FMT_MSA.3(5:IS)	SF.IA_KEY, SF.ACS
FMT_MOF.1(*)	SF.SELFTEST
FMT_MTD.1	SF.IA_KEY
FMT_SMF.1	SF.ACS
FMT_SMR.1	SF.IA_KEY
FPT_FLS.1	SF.SELFTEST, SF.FAIL_PROT
FPT_PHP.2	SF.FAIL_PROT
FPT_PHP.3	SF.FAIL_PROT
FPT_STM.1	SF.ACS, SF.SECAUDIT
FPT_TDC.1(*)	SF.ACS
FPT_TDC.1/SW-Upgrade	SF.UPDATE
FPT_TST.1	SF.SELFTEST
FTP_ITC.1(1:MS)	SF.EX_CONF, SF.EX_INT
FTP_ITC.1(2:TC)	SF.EX_CONF, SF.EX_INT
FTP_ITC.1(4:TC)	SF.EX_INT

Table 16: Coverage of Security Functional Requirements by TOE Security Functionality

8.3.2 Assurance Measures Rationale

The assurance measures of the developer as referred in sections 7.2 and 8.2 are suitable and sufficient to meet the CC assurance level EAL4 augmented by AVA_VAN.5 and ATE_DPT.2 as claimed in section 7.2. In particular, the deliverables listed in section 8.2 are suitable and sufficient to document that the assurance requirements are met.

9 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the INFINEON Security Controller M7892 G12 [SCST].
It is made in strict accordance with [AIS36].

9.1 Relevance of Security Controller TSF

The following table shows the relevance of the Security Controller security functions for the Composite Security Target:

Security Controller TSF	Relevant	Not Relevant
SF_DPM: Device Phase Management	X	
SF_PS: Protection against Snooping	X	
SF_PMA: Protection against Modifying Attacks	X	
SF_PLA: Protection against Logical Attacks	X	
SF_CS: Cryptographic Support	X	
SF_MAE: Mutual Authentication Extension	X	

Table 17: Relevance of Security Controller TSF for Composite ST

Note regarding SF_CS: Cryptographic support includes Triple-DES (relevant), AES (relevant), RSA (relevant), EC (not relevant), TRNG (relevant) and PRNG (not relevant).
Note regarding SF_MAE: This security function is declared as relevant, because the Security Controller is delivered with activated MAE (Mutual Authentication Extension) and Flash Loader from INFINEON to the manufacturer of the TOE. The Flash Loader will be deactivated during personalization (production phase) of the TOE. Hence the SFRs of the Security Controller mapped to SF_MAE will be not relevant anymore for the operational use of the TOE.

9.2 Security Requirements

9.2.1 Security Functional Requirements

Security Functional Requirements of the TOE

The following SFRs are definitely tachograph specific and have no conflicts with the SFRs of the Security Controller but could not be traced or mapped to the SFRs of the Security Controller:

FAU_GEN.1
FAU_SAR.1
FAU_STG.4
FCO_NRO.1
FCS_CKM.2(*)
FCS_COP.1(6:SHA-1)
FCS_COP.1(2:SHA-2)
FDP_ETC.2
FDP_ITC.1
FDP_ITC.2
FDP_ITC.2/SW-Upgrade
FIA_AFL.1(*)

FIA_ATD.1(*)
FIA_UAU.1(*)
FIA_UAU.2(*)
FIA_UAU.3
FIA_UAU.5
FIA_UAU.6
FIA_UID.2
FMT_MOF.1(*)
FMT_MTD.1
FMT_SMF.1
FMT_SMR.1
FPT_STM.1
FPT_TDC.1(*)
FPT_TDC.1/SW-Upgrade
FTP_ITC.1(*)

Security Functional Requirements of the Security Controller

FAU_SAS.1	not relevant, because not applicable, no conflict
FCS_RNG.1	covered by FCS_RNG.1, FCS_CKM.1(1) and FCS_CKM.1(2)
FCS_COP.1/TDES	not relevant, because not used, no conflict
FCS_CKM.4/TDES	not relevant, because not used, no conflict
FCS_COP.1/AES	not relevant, because not used, no conflict
FCS_CKM.4/AES	not relevant, because not used, no conflict
FCS_COP.1/TDES_SCL	covered by FCS_COP.1(4:TDES)
FCS_CKM.4/TDES_SCL	covered by FCS_CKM.4(2)
FCS_COP.1/AES_SCL	covered by FCS_COP.1(1:AES) and FCS_COP.1/SW-Upgrade
FCS_CKM.4/AES_SCL	covered by FCS_CKM.4(1) and FCS_CKM.4/SW-Upgrade
FCS_COP.1/RSA	covered by FCS_COP.1(5:RSA)
FCS_COP.1/ECDSA	covered by FCS_COP.1(3:ECC)
FCS_COP.1/ECDH	not relevant, because not used, no conflict
FCS_COP.1/SHA	not relevant, because not used, no conflict
FCS_CKM.1/RSA	not relevant, because not used, no conflict
FCS_CKM.1/EC	covered by FCS_CKM.1(1)
FDP_ACC.1	covered by FDP_ACC.1(*) and FDP_ACC.1/SW-Upgrade (see table below)
FDP_ACF.1	covered by FDP_ACF.1(*) and FDP_ACF.1/SW-Upgrade (see table below)
FDP_IFC.1	covered by FDP_RIP.1
FDP_ITT.1	covered by FDP_RIP.1, FDP_ITT.1
FDP_SDC.1	not relevant, because not used, no conflict
FDP_SDI.1	covered by FDP_SDI.2(*), FAU_STG.1
FDP_SDI.2	covered by FDP_SDI.2(*), FAU_STG.1
FMT_LIM.1	covered by FDP_RIP.1
FMT_LIM.2	covered by FDP_RIP.1
FMT_LIM.1/Loader	not relevant, because the Flash Loader will be deactivated during personalization of the TOE, no conflict
FMT_LIM.2/Loader	not relevant, because the Flash Loader will be deactivated during personalization of the TOE, no conflict
FMT_MSA.1	covered by FMT_MSA.1
FMT_MSA.3	covered by FMT_MSA.3(*) (see table below)
FMT_SMF.1	covered by FDP_ACC.1(*), FDP_ACF.1(*) (see table below)
FPT_FLS.1	covered by FPT_FLS.1
FPT_ITT.1	covered by FDP_RIP.1
FPT_PHP.3	covered by FPT_PHP.2, FPT_PHP.3
FPT_TST.2	covered by FPT_TST.1
FRU_FLT.2	covered by FPT_FLS.1
FDP_ACC.1/Loader	not relevant, because the Flash Loader will be deactivated during personalization of the TOE, no conflict

FDP_ACF.1/Loader	not relevant, because the Flash Loader will be deactivated during personalization of the TOE, no conflict
FIA_API.1	not relevant, because the Flash Loader will be deactivated during personalization of the TOE, no conflict

Tracing of Security Controller SFRs to TOE SFRs:

Security Controller SFRs / TOE SFRs	FCS_RNG.1	FCS_COP.1/TDES_SCL	FCS_CKM.4/TDES_SCL	FCS_COP.1/AES_SCL	FCS_CKM.4/AES_SCL	FCS_COP.1/RSA	FCS_COP.1/SHA	FCS_COP.1/ECDSA	FCS_CKM.1/EC	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITT.1	FDP_SDI.1	FDP_SDI.2	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FPT_FLS.1	FPT_ITT.1	FPT_PHP.3	FPT_TST.2	FRU_FLT.2
FAU_STG.1														X	X										
FCS_CKM.1(1)	X								X																
FCS_CKM.1(2)	X																								
FCS_COP.1(4:TDES)		X																							
FCS_COP.1(1:AES)				X																					
FCS_COP.1(5:RSA)						X																			
FCS_COP.1(3:ECC)								X																	
FCS_COP.1/SW-Upgrade				X																					
FCS_RNG.1	X																								
FCS_CKM.4(1)					X																				
FCS_CKM.4(2)			X																						
FCS_CKM.4/SW-Upgrade					X																				
FDP_ACC.1(1:FIL)										X										X					
FDP_ACC.1(2:FUN)										X										X					
FDP_ACC.1(3:DAT)										X										X					
FDP_ACC.1(4:UDE)										X										X					
FDP_ACC.1(5:IS)										X										X					
FDP_ACC.1/SW-Upgrade										X										X					
FDP_ACF.1(1:FIL)											X									X					
FDP_ACF.1(2:FUN)											X									X					
FDP_ACF.1(3:DAT)											X									X					

Security Controller SFRs / TOE SFRs	FCS_RNG.1	FCS_COP.1/TDES_SCL	FCS_CKM.4/TDES_SCL	FCS_COP.1/AES_SCL	FCS_CKM.4/AES_SCL	FCS_COP.1/RSA	FCS_COP.1/SHA	FCS_COP.1/ECDSA	FCS_CKM.1/EC	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITT.1	FDP_SDI.1	FDP_SDI.2	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FPT_FLS.1	FPT_ITT.1	FPT_PHP.3	FPT_TST.2	FRU_FLT.2
FDP_ACF.1(4:UDE)											X									X					
FDP_ACF.1(5:IS)											X									X					
FDP_ACF.1/SW-Upgrade											X									X					
FDP_RIP.1												X	X			X	X					X			
FDP_SDI.2(*)														X	X										
FMT_MSA.1																		X							
FMT_MSA.3(1:FIL)																			X						
FMT_MSA.3(2:FUN)																			X						
FMT_MSA.3(3:DAT)																			X						
FMT_MSA.3(4:UDE)																			X						
FMT_MSA.3(5:IS)																			X						
FPT_FLS.1																					X				X
FPT_PHP.2																							X		
FPT_PHP.3																							X		
FPT_TST.1																								X	

9.2.2 Security Assurance Requirements

The level of assurance of the TOE given in section 2 is EAL4 augmented with the components ATE_DPT.2 and AVA VAN.5.
The level of assurance of the Security Controller is EAL 6 augmented with the component ALC_FLR.1 according to [SCST].
This shows that the Security Assurance Requirements of the TOE matches the Security Assurance Requirements of the hardware.

9.3 Security Objectives

Security Objectives for the Security Controller:

O.Phys-Manipulation	Protection against Physical Manipulation:	No conflict.
O.Phys-Probing	Protection against Physical Probing:	No conflict.
O.Malfunction	Protection against Malfunction due to Environmental Stress:	No conflict.
O.Leak-Inherent	Protection against Inherent Information Leakage:	No conflict.
O.Leak-Forced	Protection against Forced Information Leakage:	No conflict.
O.Abuse-Func	Protection against Abuse of Functionality:	No conflict.
O.Identification	TOE Identification:	No conflict.
O.RND	Random Numbers:	No conflict.
O.Cap_Avail_Loader	Capability and availability of the Loader, valid only for TOE derivatives delivered with activated MAE and Flash Loader	No conflict.
O.TDES	Cryptographic service Triple-DES	No conflict.
O.AES	Cryptographic service AES	No conflict.
O.SHA	Cryptographic service Hash function	No conflict.
O.Add-Functions	Additional specific security functionality:	No conflict.
O.Mem-Access	Area based Memory Access Control:	No conflict.
O.Authentication	Authentication to external entities:	No conflict.
O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF	No conflict.
O.Ctrl_Auth_Loader/Package1+	Access control and authenticity for the Loader	No conflict.

Security Objectives for the Security Controller Environment:

OE.Process-Sec-IC	Protection during composite product manufacturing:	No conflict.
OE.Resp-Appl	Treatment of User Data:	No conflict.
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	No conflict.
OE.Loader_Usage/Package1+	Secure usage of the Loader	No conflict.
OE.TOE_Auth	External entities authenticating of the TOE	No conflict.

Security Objectives of the TOE:

O.Access:	No conflict.
O.Accountability:	No conflict.
O.Audit:	No conflict.
O.Authentication:	No conflict.
O.Integrity:	No conflict.
O.Output:	No conflict.
O.Processing:	No conflict.
O.Reliability:	No conflict.
O.Secure_Exchange:	No conflict.
O.Software_Update:	No conflict.

Security Objectives of the TOE Environment:
(only objectives of the design and manufacturing environment are relevant)

OE.Development	No conflict.
OE.Manufacturing	No conflict.
OE.Data_Generation	No conflict.
OE.Data_Transport	No conflict.
OE.Delivery	No conflict.
OE.Software_Upgrade	No conflict.
OE.Data_Strong	No conflict.
OE.Test_Points	No conflict.

Tracing of security objectives of the Security Controller to security objectives of the TOE:

Objectives for the TOE / Objectives for the Security Controller hardware	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secure_Exchange	O.Software_Update
O.Phys-Manipulation			X			X	X	X		
O.Phys-Probing						X	X	X		
O.Malfunction		X	X		X	X		X		
O.Leak-Inherent	X					X	X	X		
O.Leak-Forced	X		X			X	X	X		
O.Abuse-Func	X	X	X		X	X	X	X		
O.RND	X	X	X		X	X	X	X	X	
O.TDES									X	
O.AES										X
O.SHA										X
O.Add-Functions									X	X
O.Mem-Access	X						X	X	X	X

Table 18: Mapping of Security Controller objectives to TOE objectives

The security objectives of the design and manufacturing environment of the TOE include in general meaning parts of the security objectives of the Security Controller. Other parts are covered by the security objectives of the TOE (O.Access, O.Authenticate, O.Integrity, O.Processing, O.Secure_Exchange, O.Software_Upgrade), see assumption section 3.3.

The security objective of the Security Controller O.Identification cannot be mapped because it is related to the production life cycle phase only. The security objectives of the Security Controller O.Cap_Avail_Loader, O.Authentication, O.Prot_TSF_Confidentiality, O.Ctrl-Auth_Loader/Package+1 cannot be mapped because the Flash Loader is deactivated during personalisation of the TOE in the production life cycle phase (before operational use).

Tracing of security objectives of the Security Controller Environment to security objectives of the TOE and its environment:

Security objectives for the environment of the Security Controller	Security objectives of the TOE and TOE environment covering them
OE.Process-Sec-IC	OE.Development, OE.Manufacturing, OE.Data_Transport
OE.Resp-Appl	OE.Development, OE.Manufacturing, OE.Data_Transport, OE.Test_Points, O.Access, O.Authenticate, O.Integrity, O.Processing, O.Secure_Exchange, O.Software_Update
OE.Lim_Block_Loader	OE.Development, OE.Manufacturing, OE.Data_Transport, OE.Test_Points
OE.Loader_Usage/Package1+	OE.Development, OE.Manufacturing, OE.Data_Transport, OE.Test_Points
OE.TOE_Auth	OE.Development, OE.Manufacturing, OE.Data_Transport, OE.Test_Points

Table 19: Mapping of Security Controller Environment objectives to TOE objectives

9.4 Conclusion

Overall no contradictions between the Security Targets of the TOE and the Security Controller hardware are found.

10 Annex

10.1 Glossary and list of acronyms

A.x	Assumption
CA	Certification Authority
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Management Board
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (DSRC)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES)
EEPROM	Multiple programmable ROM
EQTj.C	Equipment Certificate
EQTj.PK	Equipment Public Key
EQTj.SK	Equipment Private Key
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
EUR.PK	European Public Key
SF.x	Security Function
Flash	Multiple programmable ROM memory with sector erase.
ITSEC	Information Technology Security Evaluation Criteria
ISO	International Standardisation Organisation
JIL	Joint Interpretation Library
KID	Identification key, will manage the pairing between a motion sensor and the vehicle unit
Km	Master key, will manage the pairing between a motion sensor and the vehicle unit
KmVU	Part of the Master key stored in the VU, will manage the pairing between a motion sensor and the vehicle unit
Km-wc	Part of the Master key stored in the workshop card, will manage the pairing between a motion sensor and the vehicle unit
KP	Pairing key, will manage the pairing between a motion sensor and the vehicle unit
KSM	Session key between motion sensor and vehicle unit
KST	Session key between tachograph cards and vehicle unit
LED	Light Emitting Diode
MAC	Message Authentication Code
MC	Main Controller
MD	Management Device as defined in [SR]
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
MSi.C	Member State certificate
NCA	National Certification Authority
NMEA	National Marine Electronics Association

O.x	Security Objective of the TOE
OE.x	Security Objective of the Environment
OS	Operating System
OSP	Organisational security policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
RAD	Reference Authentication Data
RAM	Random Access Memory (loses data if detached from a power supply)
REQxxx	A requirement from [EU], where ‘xxx’ represents the requirement number.
ROM	Read Only Memory (stores data independent of a power supply)
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
RTC	Real time clock
SC	Security Controller
SEF	Security Enforcing Function
SF	Security Function
SFP	Security Function Policy (see [CC2])
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
ToSS	TOE Security Service
TSF	TOE Security Functionality
T.x	Threat
UDI.PK	public key of the update issuer
UDI.SK	private key of the update issuer
VAD	Verification Authentication Data
VU	Vehicle Unit

10.2 Bibliography

[CC1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017

[CC2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017

[CC3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017

[CM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017

[AIS36] Anwendungshinweise und Interpretationen zum Schema, AIS36, Version 5, 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik

[CSM] Appendix 11 of Annex 1C of Commission Implementing Regulation (EU) 2016/799 – Common Security Mechanisms

[EU] 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 1C

[EU1B] Annex 1B of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 77)

[SR] Appendix 10 of Annex 1C of Commission Implementing Regulation (EU) 2016/799 – Security Requirements

[SCST] Security Target Lite, Common Criteria EAL6 augmented / EAL6+, M7892 Design Steps D11 and G12, Document version 1.2 of 2017-11-21, Author: Dr. Oleg Rudakov

[ISO9001] ISO 9001:2008, First edition: 2000
http://www.iso.org/iso/rss.xml?csnumber=46486&rss=detail

[ISO7816] ISO/IEC 7816-2 Information technology. Identification cards. Integrated circuit(s) cards with contacts. Part 2: Dimensions and location of the contacts. First edition: 1999.

ISO/IEC 7816-3 Information technology. Identification cards. Integrated circuit(s) cards with contacts. Part 3: Electronic signals and transmission protocol. Edition 2: 1997.

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

ISO/IEC 7816-6 Information technology. Identification cards. Integrated circuit(s) cards with contacts. Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998.

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

[ISO16844-3] ISO 16844-3:2004 with Technical Corrigendum 1:2006, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface

[ISO16844-4] ISO 16844-4:2015, Road Vehicles – Tachograph Systems – Part 4: CAN interface

[JIL] JIL Security Evaluation and Certification of Digital Tachographs, Version 1.12, JIL Working Group (BSI, CESG, DCSSI, NLNCSA), June 2003.

[PPT] Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)', BSI-CC-PP-0094-2017, Version 1.0 as of 19th May 2017

[TR-02102] Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI-Technische Richtlinie, Version 2017-01, 08.02.2017

[FIPS 186-4] National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013

[FIPS 197] Federal Information Processing Standards Publication 197 (FIPS PUB 197). Advanced Encryption Standard (AES), 2001

[NIST SP800-38A] NIST. Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication SP800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001

[NIST SP800-38B] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication SP800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001

[NIST SP800-38D] NIST Special Publication 800-38D. November, 2007, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

[NIST SHA] FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015

[NIST SHA-USAGE] NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms, August 2012

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

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

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

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

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

[FIPS 180-1] FIPS PUB 180-1: Secure Hash Standard, NIST, April 1995.
[FIPS 180-4] FIPS PUB 180-4: Secure Hash Standard, NIST, March 2012 DTCO 1381 Security Target [Revision 1.28]
[NIST_46_3] FIPS PUB 46-3 Federal Information Processing Standards Publication Data Encryption Standard (DES) Reaffirmed 1999 October 25
[ANSI X9.19] ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanismus using a block cipher
[ANSI X9.62] ANSI X9.62:2005 Public Key Cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)
[PKCS.1] PKCS #1: RSA Cryptography Specifications, Version 2.0. RSA Laboratories, September 1998
[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

11 Annex A – Key & Certificate Tables

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

Table 20	First-generation asymmetric keys generated, used or stored by a VU
Table 21	First-generation symmetric keys generated, used or stored by a VU
Table 22	First-generation certificates used or stored by a VU
Table 23	Second-generation asymmetric keys generated, used or stored by a VU
Table 24	Second-generation symmetric keys generated, used or stored by a VU
Table 25	Second-generation certificates used or stored by a VU

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

a) When support for the Generation-1 cryptography is suppressed by a workshop, as described in Application note 2;
b) When the (Gen. 2) vehicle unit sign certificate has reached its end of validity.

If other circumstances necessitate the decommissioning of a vehicle unit, making unavailable the permanently stored keys mentioned in this table, if feasible, is a matter of organizational policy.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
VU.SK	VU private key	Used by the VU to perform VU authentication towards tachograph cards and for signing downloaded data files	RSA	Generated by VU manufacturer at the end of the manufacturing phase	Out of scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory
EUR.PK	Public key of ERCA	Used by VU to perform verification of MS certificates presented by (foreign) cards during mutual authentication. See also notes for EUR.KID in Table 22	RSA	Generated by ERCA; inserted in VU by VU manufacturer at the end of the manufacturing phase	Out of scope of this ST	Not applicable	VU non-volatile memory
Card.PK (conditional, possibly multiple)	Card public key	Used by VU to perform card authentication (see also notes for Card.C contents in Table 22)	RSA	Generated by card or card-Manufacturer; obtained by VU in card certificate during mutual authentication	Out of scope of this ST	Not applicable	VU non-volatile memory
MS.PK (conditional, possibly multiple)	Public key of an MSCA other than the MSCA responsible for signing the VU certificate	Used by VU to perform verification of card certificates signed by this (foreign) MSCA. See also notes for MS.C contents in Table 22.	RSA	Generated by (foreign) MSCA; obtained by VU in MS certificate presented by a card during mutual authentication	Out of scope of this ST	Not applicable	VU non-volatile memory

Table 20 - First-generation asymmetric keys generated, used or stored by a VU

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
K_{MAC}	Secure Messaging session key	Session key for data protection between VU and a card during a Secure Messaging session	TDES	Agreed between VU and card during mutual authentication	See section 6.1.3.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored

Table 21 - First-generation symmetric keys generated, used or stored by a VU

Application note 37: Note: As it is not possible to pair a second-generation VU to a first-generation motion sensor, the VU does not contain any symmetric keys related to first-generation motion sensors.

Certificate Symbol	Description	Purpose	Source	Stored in	Note
VU.C	VU certificate for signing and Mutual Authentication	Used by cards or IDE to obtain and verify the VU.PK that they will subsequently use to perform VU authentication or verification of signatures created by the VU	Created and signed by MSCA based on VU manufacturer input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
MS.C	Certificate of MSCA responsible for signing VU certificate	Used by cards or IDE to obtain and verify the MS.PK that they will subsequently use to verify the VU.C	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
Card.C contents (conditional, possibly multiple)	CHR and other card certificate contents	If a VU has verified a card certificate before, it may store the public key (see Table 18), the CHR and possibly the validity period and other data in order to authenticate that card again in the future	Created and signed by MSCA based on card manufacturer input; inserted in card by card manufacturer; obtained and stored by VU during a previous successful card authentication.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store card certificate contents for future reference and has encountered cards in the past. The VU may store the contents of multiple Card.C.

MS.C contents (conditional, possibly multiple)	CHR and other MS certificate contents	If a VU has verified a MS certificate before, it may store the public key (see Table 18), the CHR and possibly the validity period and other data in order to verify card certificates based on that MS certificate in the future	Created and signed by ERCA based on MSCA input, inserted in card by card manufacturer; obtained and stored by VU after successful verification during a previous mutual authentication process with a (foreign) card.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store MSCA certificate contents for future reference and has encountered cards containing a foreign MS certificate in the past. The VU may store the contents of multiple MS.C.
EUR.KID	Key Identifier for public key of ERCA	This identifier will be used by the VU to reference the European root public key during mutual authentication towards cards or EGFs	Inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	

Table 22 - First-generation certificates used or stored by a VU

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
VU_MA.SK	VU private key for Mutual Authentication	Used by the VU to perform VU authentication towards tachograph cards and external GNSS facilities	ECC	Generated by VU or VU manufacturer at the end of the manufacturing phase	See section 6.1.2.1 if done by VU. Otherwise, not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory
VU_Sign.SK	VU private key for signing	Used by the VU to sign downloaded data files	ECC	Generated by VU or VU manufacturer at the end of the manufacturing phase	See section 6.1.2.1 if done by VU. Otherwise, not in scope of this ST.	Made unavailable when the VU has reached end of life	VU non-volatile memory

EUR.PK (current)	The current public key of ERCA (at the time of issuing of VU)	Used by the VU for the verification of MSCA certificates issued under the current ERCA root certificate. See also notes for EUR.C (current) contents in Table 25.	ECC	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	Out of scope of this ST	Not applicable	VU non-volatile memory
EUR.PK (previous)	The previous public key of ERCA (at the time of issuing of VU)	Used by the VU to verify MSCA certificates issued under the previous ERCA root certificate. See also notes for EUR.C (previous) contents in Table 25	ECC	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	Out of scope of this ST	Not applicable	VU non-volatile memory (conditional; only present if existing at time of VU issuance)
EUR.Link.PK	The public key of ERCA following the public key that was current at the time of issuing of the VU	Used by the VU to verify MSCA certificates issued under the next ERCA root certificate. Note that EUR.Link.PK is the same as the next EUR.PK. See also Application note 36:. and notes for EUR.Link.C contents in Table 25.	ECC	Generated by ERCA; inserted by manufacturer in a card or EGF issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by VU during mutual authentication towards such card or EGF	Out of scope of this ST	Not applicable	VU general non-volatile memory (conditional; only if the VU has successfully authenticated a next-generation card or EGF)
$VU.SK_{EPH}$	VU ephemeral private key	Used by the VU to perform session key agreement with a tachograph card or external GNSS facility	ECC	Generated by VU during mutual authentication with a card or EGF	See section 6.1.2.1	Made unavailable at the latest when the Secure Messaging session is aborted	Not permanently stored
$VU.PK_{EPH}$	VU ephemeral public key	Used by tachograph cards or external GNSS facilities to perform session key agreement with the VU	ECC	Generated by VU during mutual authentication with a card or EGF, together with $VU.SK_{eph}$	See section 6.1.2.1	Not applicable	Not permanently stored

Card_MA.PK	Card public key for Mutual Authentication	Used by VU to perform card authentication and session key agreement (See also notes for Card_MA.C contents in Table 25)	ECC	Generated by card or card manufacturer; obtained by VU in card certificate during mutual authentication	Out of scope of this ST	Not applicable	VU non-volatile memory(conditional, possibly multiple)
EGF_MA.PK	EGF public key for Mutual Authentication	Used by VU to perform EGF authentication and session key agreement (See also notes for Card_MA.C contents in Table 25)	ECC	Generated by EGF or EGF manufacturer; obtained by VU in EGF certificate during mutual authentication as part of the coupling process	Out of scope of this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)
MSCA_Card.PK	Public key of MSCA responsible for signing card certificates	Used by VU to verify the certificate of a card signed by this (foreign) MSCA. See also notes for MSCA_Card.C contents in Table 25	ECC	Generated by MSCA ; obtained by VU in MSCA_Card certificate during mutual authentication	Out of scope of this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)
MSCA_VU-EGF.PK	Public key of MSCA responsible for signing VU and EGF certificates	Used by VU to verify the certificate of an EGF signed by this (foreign) MSCA. See also notes for MSCA_VU-EGF.C contents in Table 25.	ECC	Generated by MSCA ; obtained by VU in MSCA_VU-EGF certificate during coupling to an EGF	Out of scope of this ST	Not applicable	VU non-volatile memory (conditional, possibly multiple)

Table 23 - Second-generation asymmetric keys generated, used or stored by a VU

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
K_{M-VU}	Motion sensor master key – VU part	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU	AES	Generated by ERCA; inserted by VU manufacturer at the end of the manufacturing phase. Note: as explained in [5] Annex 1C, Appendix 11, section 12.2, a VU contains only one $K_{M-VU.}$	Out of scope of this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory
K_{M-WC}	Motion sensor master key – workshop card part	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU	AES	Generated by ERCA; retrieved by VU from inserted workshop card. Note: as explained in [5] Annex 1C, Appendix 11, section 12.2, a workshop card may contain up to three keys K_{M-WC} (of consecutive key generations). However, a VU will retrieve only one of these keys during the pairing process.	Out of scope of this ST	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2^{nd} generation motion sensor
K_M	Motion sensor master key	Key used for authentication between the VU and a motion sensor during pairing	AES	Derived by the VU from K_{M-VU} and K_{M-WC}	Not independently generated	Made unavailable at the latest by end of calibration phase	Not permanently stored;(only during pairing to a 2^{nd} generation motion sensor)

K_P	Motion sensor pairing key	Key used for encrypting the motion sensor session key when sending it to the motion sensor during pairing	AES	Generated by the motion sensor manufacturer; stored in motion sensor (encrypted under K_M) at the end of the manufacturing phase; obtained and decrypted by VU during pairing	Out of scope of this ST	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2nd generation motion sensor
K_{ID}	Motion sensor identification key	Key used for authentication between the VU and a motion sensor during pairing	AES	Derived by VU from K_M and a constant vector	Not independently generated	Made unavailable at the latest by end of calibration phase	Not permanently stored; only present during pairing to a 2nd generation motion sensor conditional
K_S	Motion sensor session key	Session key for confidentiality between VU and motion sensor in operational phase	AES	Generated by VU during pairing to a motion sensor	See section 6.1.2.1	Made unavailable when the VU is paired to another (or the same) motion sensor.	VU non-volatile memory (conditional, only if the VU has been paired with a motion sensor)
K_{MAC}	Secure Messaging session key for authenticity	Session key for authenticity between VU and a card or EGF during a Secure Messaging session	AES	Agreed between VU and card or EGF during mutual authentication	See section 6.1.2.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored

K_{ENC}	Secure Messaging session key for confidentiality	Session key for confidentiality between VU and a card or EGF during a Secure Messaging session	AES	Agreed between VU and card or EGF during mutual authentication	See section 6.1.2.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored
K_VU_{DSRC} _ENC	VU-specific DSRC key for confidentiality	To ensure confidentiality of data sent over a remote communication channel between a VU and a remote early detection communication reader	AES	Derived by MSCA based on DSRC Master Key and VU serial number received from VU manufacturer; inserted by VU manufacturer at the end of the manufacturing phase	Out of scope of this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory
K_VU_{DSRC} _MAC	VU-specific DSRC key for authenticity	To ensure integrity and authenticity of data sent over a remote communication channel between a VU and a remote early detection communication reader	AES	Derived by MSCA based on DSRC Master Key and VU serial number received from VU manufacturer; inserted by VU manufacturer at the end of the manufacturing phase	Out of scope of this ST	Made unavailable when the VU has reached end of life	VU non-volatile memory

Table 24 - Second-generation symmetric keys generated, used or stored by a VU

Certificate Symbol	Description	Purpose	Source	Stored in	Note
VU_MA.C	VU certificate for Mutual Authentication	Used by card or EGF to obtain and verify the VU_MA.PK they will subsequently use to perform VU authentication	Created and signed by MSCA based on VU manufacturer input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
VU_Sign.C	VU certificate for signing	Used by IDE or control card to obtain and verify the VU_Sign.PK they will subsequently use to verify the signature over a data file signed by the VU.	Created and signed by MSCA based on VU manufacturer input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
MSCA_VU-EGF.C	Certificate of MSCA responsible for signing the VU_MA and VU_Sign certificates	Used by a card, EGF or IDE to obtain and verify the MSCA_VU-EGF.PK they will subsequently use to verify the VU_MA or VU_Sign certificate	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
EUR.Link.C	Link Certificate signed by previous EUR.SK (see Application Note below)	Used by a card, EGF or IDE issued under the previous ERCA root certificate to obtain and verify the current EUR.PK they will subsequently use to verify the MSCA_VU-EGF certificate	Created and signed by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	Presence in VU is conditional; only if a previous ERCA root certificate existed at the moment of VU manufacturing

EUR.C (current) contents	CHR and other contents of current European root certificate	This CHR will be used by the VU to reference the current European root public key during verification of the VU certification chain by a card or EGF. The VU will also read this CHR from the MSCA certificate of a card or EGF issued under the current European root public key during verification of the card or EGF certificate chain. The CHR then serves to reference the VU's EUR.PK (current) key (see Table 21). The VU may store the validity period and other certificate data as well.	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	
EUR.C (previous) contents	CHR and other contents of previous European root certificate	: The VU will read this CHR from the MSCA certificate of a card or EGF issued under the previous European root key during verification of the card or EGF certificate chain. The CHR serves to reference the VU's EUR.PK (previous) key (see Table 21). The VU may store the validity period and other certificate data as well.	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase	VU general non-volatile memory	Presence in VU is conditional; only if a previous ERCA root certificate existed at the moment of VU manufacturing

EUR.Link.C contents	CHR and other contents of next European root certificate	The VU will read this CHR from the MSCA certificate of a card or EGF issued under the next European root key during verification of the card or EGF certificate chain. The CHR serves to reference the VU's EUR.Link.PK key (see Table 21). The VU may store the validity period and other certificate data as well.	Generated by ERCA; inserted by manufacturer in a card or EGF issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by VU during mutual authentication towards such card or EGF	VU general non-volatile memory	Presence in VU is conditional; only if the VU has successfully authenticated a next-generation card or EGF
Card_MA.C contents	CHR and other contents of Card certificate for Mutual Authentication	If a VU has verified a Card_MA certificate before, it may store the public key (see Table 21), the CHR and possibly the validity period and other data in order to authenticate that card again in the future	Created and signed by MSCA based on card manufacturer input; inserted in card by card manufacturer; obtained and stored by VU during mutual authentication after successful verification.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store card certificate contents for future reference and has encountered cards in the past. The VU may store the contents of multiple Card_MA.C.
EGF_MA.C content	CHR and other contnents of EGF certificate for Mutual Authentication	If a VU has verified an EGF_MA certificate before, it may store the public key (see Table 21), the CHR and possibly the validity period and other data in order to authenticate that EGF again in the future	Created and signed by MSCA_VU-EGF based on EGF manufacturer input, inserted in EGF by EGF manufacturer, obtained and stored by VU during mutual authentication after successful verification.	VU general non-volatile memory	Presence in VU is conditional; only if VU has been coupled to an EGF. The VU shall store the contents of only one EGF_MA.C at any given time.

MSCA_Card.C contents	CHR and other of certificate of MSCA responsible for signing card certificates	If a VU has verified a MSCA certificate before, it may store the public key (see Table 21), the CHR and possibly the validity period and other data in order to verify card certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in card by card manufacturer obtained and stored by VU after successful verification during a previous mutual authentication process with a card.	VU general non-volatile memory	Presence in VU is conditional; only if VU is designed to store card certificate contents for future reference and has encountered cards in the past. The VU may store the contents of multiple MSCA_Card.C, e.g. different MSCAs and/or generations.
MSCA_VU-EGF.C contents	CHR and other contents of certificate of MSCA responsible for signing VU and EGF certificates	If a VU has verified a MSCA certificate before, it may store the public key (see Table 21), the CHR and possibly the validity period and other data in order to verify EGF certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in EGF by EGF manufacturer; obtained and stored by VU after successful verification during a previous mutual authentication process with a card.	VU general non-volatile memory	Presence in VU is conditional; only if VU has been coupled to an EGF and is designed to store MSCA certificate contents for future reference.

Table 25 - Second-generation certificates used or stored by a VU

Application note 38: During its lifetime, the VU can be confronted with two different link certificates:

- If at the time of issuance of the VU, there are cards or EGFs in the field that are issued under a previous EUR.C, then the VU shall be issued with both the previous EUR.C and a EUR.Link.C signed with the previous EUR.SK. The VU will need the first one to check the authenticity of the old cards. The VU will need the second one to prove its authenticity towards old cards.
- If, after the issuance of the VU, a new EUR.C is generated and cards or EGFs are issued under this new root certificate, then such a new card or EGF will present the VU with a EUR.Link.C signed by the current EUR.SK to prove its authenticity. The VU can check this certificate with its current EUR.PK. If correct, the VU shall store the EUR.Link.PK as a new trust point.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
SeedVu	Base for key derivation	Derive keys and IV values during VU personalization	AES	Generated by the VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU SC non-volatile memory
K_Depers	Key for de-personalization	VU specific key used by the VU to verify a de-personalization request	AES	Derived by the VU from the SeedVu at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU SC non-volatile memory
KCOMP	SW Update: Key for MAC of compatibility header	Product specific key used by the VU to ensure integrity and authenticity of the SW update compatibility header	AES	Generated by the VU manufacturer once for a product line	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU SC non-volatile memory
$KENC_{UpdateVu}$	SW Update: Encryption key for credentials	VU specific key used by the VU to ensure confidentiality of the SW update credentials	AES	Derived by the VU from the SeedVu at the end of the manufacturing phase	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU SC non-volatile memory
$KAUTH_{UpdateVu}$	SW Update: Authentication key for credentials	VU specific key used by the VU to ensure integrity and authenticity of the SW update credentials	AES	Derived by the VU from the SeedVu at the end of the manufacturing phase	Out of scope for this ST	Made unavailable when the VU has reached end of life	VU SC non-volatile memory

$K_{Firmware}$-SC	SW Update: Key for SC code update	SW version specific key used by the VU to decrypt SC code during SW update	AES	Generated by the VU manufacturer before distribution of a SW update package	Out of scope for this ST	Made unavailable at the end of the SW update process	VU SC non-volatile memory
$K_{Firmware}$-MC	SW Update: Key for MC code and parameter update	SW version specific key used by the VU to decrypt MC code and parameters during SW update	AES	Generated by the VU manufacturer before distribution of a SW update package	Out of scope for this ST	Made unavailable at the end of the SW update process	VU SC non-volatile memory
K_ErrorLog_Sign	ErrorLog: Key for signing	VU specific key used by the manufacturer to ensure integrity and authenticity of the downloaded logging data.	ECC	Generated by the VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU SC non-volatile memory
K_ErrorLog_Enc	ErrorLog: Key for download encryption	VU specific key used by the manufacturer to ensure confidentiality of the downloaded logging data.	AES	Generated by the VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU SC non-volatile memory
K_ErrorLog_MC	ErrorLog: Key for MC data encryption	VU specific key used by the VU to ensure confidentiality of the logging data stored in the MC memory.	AES	Generated by the VU manufacturer at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU MC non-volatile memory
K_DataSe_MAC	Data storage: Key	VU specific key used by the VU to ensure	AES	Generated by the VU at the end of the manufacturing	Out of scope for this ST	Not applicable.	VU SC non-

	for MAC of security elements	authenticity of the security elements stored in the SC NVM.		phase			volatile memory
K_DataMc_MAC	Data storage: Key for MAC calculation	VU specific key used by the VU to ensure authenticity of the user data stored in the MC flash memory.	AES	Generated by the VU at the end of the manufacturing phase	Out of scope for this ST	Not applicable.	VU SC non-volatile memory

Table 26: Manufacturer specific keys and certificates used or stored by the VU

12 Annex B – Operations for FCS_RNG.1

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

12.1 Class PTG.2

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

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

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 [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered [selection: *externally, at regular intervals, continuously, applied upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical

properties of the raw random numbers within an acceptable period of time.

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

(PTG.2.6) Test procedure A [26] [assignment: *additional standard test suites*] does not distinguish the internal random numbers from output sequences of an ideal RNG.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

12.2 Class PTG.3

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

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

Hierarchical to: -

Dependencies: -

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

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

(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5) The online test procedure checks the raw random

[26] See [FCRNG] Section 2.4.4.

number sequence. It is triggered [selection: *externally, at regular intervals, continuously, upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

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

(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A[27] [assignment: *additional test suites*].

(PTG.3.8) The internal random numbers shall [selection: *use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work*]].

[27] See [FCRNG] Section 2.4.4.

13 Annex C – Cryptographic Methods

This annex lists the cryptographic methods that are provided by EFAS-4.10 at its external interfaces.

No.	Purpose of case	Cryptographic mechanism	Implementing standard	Key length	Application standard	Validity period
First-generation tachograph system						
1	Secure messaging authenticated mode VU ↔ tachograph card	Retail-MAC	[ANSI X9.19]	112	[EU] app. 11, sec. 5.3 [ISO_9797_1] [EU] app. 11, sec. 2.2.3	Until the 'ability to use first generation tachograph cards,' is revoked (by workshops on request by EU).
2	Secure messaging encrypted mode VU ↔ tachograph card	Triple-DES in CBC mode	[NIST_46_3] [NIST SP800-38A]	112	[EU] app. 11, sec. 5.4 [EU] app. 11, sec. 2.2.3	
3	Mutual authentication and session key agreement VU ↔ tachograph card	RSA	[PKCS.1]	1024	[EU] CSM_020 [EU] app. 11, sec. 2.2.1	
		SHA-1	[FIPS 180-1]	n/a	[EU] CSM_020 [EU] app. 11, sec. 2.2.2	
4	Digital signature for downloading to external media	RSA	[PKCS.1]	1024	[EU] CSM_020 [EU], app. 11, sec. 2.2.1	Until the 'ability to use first generation tachograph cards,' is revoked: No first-generation tachograph cards available to trigger a first-generation download.
		SHA-1	[FIPS 180-1]	n/a	[EU] CSM_034 [EU] app. 11, sec. 2.2.2	
Second-generation tachograph system						
5	Secure messaging VU ↔ Motion Sensor	AES in CBC mode	[FIPS 197] [NIST SP800-38A]	AES-128; AES-192; AES-256	[EU] CSM 42 [ISO16844-3], sec. 7.6	Until 'VuEndOfOperation' (about 15 years after personalisation)
6	Secure messaging encryption VU ↔ tachograph card	AES in CBC mode	[FIPS 197] [ISO_10116]	AES-128; AES-192; AES-256	[EU] CSM 40 [EU] CSM_186	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
7	Secure messaging authentication VU ↔ tachograph card	AES in CMAC mode	[NIST SP800-38B]	AES-128; AES-192; AES-256	[EU] CSM_187	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)

No.	Purpose of case	Cryptographic mechanism	Implementing standard	Key length	Application standard	Validity period
8	Certificate Chain Verification by VU depending on Domain parameters	ECDSA Signature Verification and Validation	[RFC_5639], [RFC_5480], [FIPS 186-4], [FIPS 180-4]	Brainpool-P256r1 with SHA-256; NIST-P256 with SHA-256; Brainpool-P384r1 with SHA-384; NIST-P384 with SHA-384; Brainpool-P512r1 with SHA-512; NIST-P521 with SHA-512	[EU] CSM_48, [EU] CSM_160	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
9	Mutual authentication VU ↔ tachograph card depending on Domain parameters	Ephemeral ECDH key pair generation depending on cards domain parameters	According to [SCST] FCS_CKM.1.1/EC: - According to the appendix A4.3 in ANSI X9.62-2005 [25]: The cofactor h is not supported. - According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002	Brainpool-P256r1; NIST-P256; Brainpool-P384r1; NIST-P384; Brainpool-P512r1; NIST-P521	[EU] CSM_162	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
		ECDSA signing algorithm depending on domain parameters of VU	[RFC_5639], [RFC_5480], [FIPS 186-4], [TR_03111], [FIPS 180-4]	Brainpool-P256r1 with SHA-256; NIST-P256 with SHA-256; Brainpool-P384r1 with SHA-384; NIST-P384 with SHA-384; Brainpool-P512r1 with SHA-512; NIST-P521 with SHA-512	[EU] CSM_173, [EU] CSM_174	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)

No.	Purpose of case	Cryptographic mechanism	Implementing standard	Key length	Application standard	Validity period
		ECKA (ECDH) key agreement algorithm depending on cards domain parameters	[RFC_5639], [RFC_5480], [FIPS 186-4], [TR_03111]	Brainpool-P256r1; NIST-P256; Brainpool-P384r1; NIST-P384; Brainpool-P512r1; NIST-P521	[EU] CSM_176	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
		Session key derivation depending on cards domain parameters	[TR_03111], [FIPS 180-4]	SHA-256; SHA-384; SHA-512	[EU] CSM_179	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
10	Authenticity and confidentiality of data communicated from a vehicle unit to a control authority over a DSRC remote communication channel	AES (in CBC Mode, CMAC mode)	[FIPS 197] [ISO_10116] [NIST SP800-38B]	AES-128; AES-192; AES-256	[EU] CSM_119, [EU] CSM_226	Until 'VuEndOfOperation' (about 15 years after personalisation)
11	Signature for downloading data	ECDSA signing algorithm depending on domain parameters of VU	[RFC_5639], [FIPS 186-4], [FIPS 180-4]	Brainpool-P256r1 with SHA-256; NIST-P256 with SHA-256; Brainpool-P384r1 with SHA-384; NIST-P384 with SHA-384; Brainpool-P512r1 with SHA-512; NIST-P521 with SHA-512	[EU], CSM_233,	Until 'VuEndOfOperation' plus 3 months (about 15 years after personalisation)
SW-Update						
14	Confidentiality of credentials	AES in CBC mode	[FIPS 197]	AES-128	n/a	Until 'VuEndOfOperation' (about 15 years after personalisation)
15	Authenticity of credentials	AES-CMAC	[NIST SP800-38B]	AES-128	n/a	
16	Authenticity of compatibility header	AES-CMAC	[NIST SP800-38B]	AES-128	n/a	
17	Confidentiality of update data	AES in GCTR mode	[NIST 800-38D]	AES-128	n/a	
18	Authenticity of update data	SHA	[FIPS 180-4]	SHA-256	n/a	

Table 27: Cryptographic Methods