# EFAS-3 V01

## Security Target

| | | |
|---|---|---|
| File name: | 5340.020.DOC.05_SecurityTarget_public.doc | |
| Release: | 05 | |
| Document number: | 5340.020.DOC.05.DOC | |
| Certification ID | BSI-DSZ-CC-0474 | |
| Creation date: | 15.12.2006 | by: Dr. B. Rose |
| Last change: | 04.04.2008 | by: Dr. B. Rose |
| Status: | approved | |
| Location: | Intranet: Z:_EFAS-3_5340\Zulassungsaktivitäten\Security\Eigene_Dokumente\ and VSS | |

| | **Name:** | **Date:** | **Signature:** |
|---|---|---|---|
| **rendered:** | **B. Hoeppener** | | |
| **reviewed:** | **B. Rogge** | | |
| **approved:** | **Dr. B. Rose** | | |

## Release notes:

| release | date | page | chapter | changes, notes | modified by | quantity pages |
|---|---|---|---|---|---|---|
| 00 | | | | Initial version. | Dr. B. Rose | 81 |
| 01 | 16.03.07 | | | Reviewed draft. | Dr. B. Rose | 97 |
| 02 | 11.05.07 | | | Chapter "Compliance with the generic security target" added. | B. Hoeppener | 106 |
| 03 | 15.06.07 | | | 'Configuration Device' added. 'Software Update' corrected. | B. Hoeppener | 106 |
| | 03.07.07 | | 2.2 | Description of interfaces changed. | B. Hoeppener | 107 |
| | 05.07.07 | | | Approved for evaluation. | B. Hoeppener | 107 |
| 04 | 20.02.08 | | | Changes and adaptations concerning the comments of BSI from 15.02.2008 | B. Hoeppener | 116 |
| | 22.02.08 | 69 | 6.1.2 | first passage stated more precisely | Dr. B. Rose | 116 |
| | | 72 | 6.1.3 | case c) action added | Dr. B. Rose | 116 |
| 05 | 26.03.08 | 14 | 2.2 | More details are added to the logical boundaries | Dr. B. Rose | 116 |
| | | 21-22 | 3.3 | Extension of the threats description | Dr. B. Rose | 116 |
| | | 68-77 | 6.1 | Specification of the security functions of the SC for each security function of the TOE | Dr. B. Rose | 116 |

## Table of Contents

# 1 Introduction

## 1.1 ST Identification

This Document is the Security Target (ST) of the EFAS-3 V01 (the TOE) provided by EFKON mobility GmbH for a Common Criteria evaluation.

| | |
|---|---|
| Document Title: | Security Target - EFAS-3 V01 |
| Document Date: | 04.04.2008 |
| Document Version: | 05 |
| Publisher: | EFKON mobility GmbH (EFKON) |
| TOE: | EFAS-3 V01 |
| TOE Developer: | EFKON mobility GmbH |
| TOE Sponsor: | EFKON AG |
| Certification ID: | BSI-DSZ-CC-0474 |
| IT Evaluation Scheme: | German CC Evaluation Scheme |
| Evaluation Body: | SRC Security Research & Consulting GmbH (SRC) |

This Security Target has been built in conformance with Common Criteria Version 2.3 (ISO/IEC 15408:2005).

## 1.2 ST Overview

Target of Evaluation (TOE) and subject of this security target document is the EFAS-3 V01 developed by EFKON.

This document contains a description of the TOE, of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

The EFAS-3 V01 is a Digital Tachograph device that operates in road vehicles and is therefore commonly called vehicle unit. The vehicle unit records and stores data related to driver activities of road transport vehicles. It is also able to display, print and output information related to the stored data.

To get information about the vehicle's motion, it is connected to a motion sensor that is mounted in the gearbox of the vehicle. To avoid manipulations, the speed pulses from the motion sensor are secured by an additional encrypted communication path between the motion sensor and the vehicle unit.

To identify themselves to the vehicle unit, the drivers of the vehicle have to use tachograph cards. The driver and the co-driver, if present, have to insert their tachograph cards into the dedicated slots of the vehicle unit when using the vehicle. These tachograph cards are also used by vehicle unit to record and store user activities.

The main hardware components of the vehicle unit are the main controller (MC), the security controller (SC), the real time clock (RTC) buffered by an internal battery, a 2 row 16 characters per row LC display, 6 input keys, a thermal printer and two card readers. The main software components of the TOE are the main controller software and the SC software. The security functions are concentrated in the SC and its software. For a security controller the microcontroller AT90SC144144CT (ATMEL) was chosen.

When the TOE is delivered to the customer (i.e. fitter or workshop), it is not activated and not calibrated but personalised by the manufacturer.

The Digital Tachograph EGAS-3 V01 is designed to fulfil the requirements to a Vehicle Unit (VU) of the standardised European Tachograph System described in the Tachograph Specification [EU], Annex 1B main body and its appendices. This Security Target reflects the Vehicle Unit Generic Security Target in appendix 10 of the Tachograph Specification [EU]. In particular, this implies the conformance of the Digital Tachograph EGAS-3 V01 with the following standards:

- Concerning the communication with the motion sensor the vehicle unit is conform with ISO/IEC 16844-3 Road Vehicles - Tachograph systems - Part 3: Motion sensor interface.
- For the communication with the tachograph card the vehicle unit is especially conform with ISO/IEC 7816 Identification cards - Integrated circuits with contacts (Part 3: Electronic signals and transmission protocol, Part 4: Interindustry commands for interchange and Part 8: Security related interindustry commands).
- For the calibration protocol and data download the message structure, types and flow are principally based on the Keyword Protocol 2000 (KWP) (ISO 14230-2 Road vehicles - Diagnostic systems - Keyword protocol 2000 - Part 2: Data link layer). The application layer is principally based on the current draft to date of ISO 14229-1 (Road vehicles - Diagnostic systems - Part 1: Diagnostic services, version 6 of 22 February 2001).
- For tests the vehicle unit is conform with the correspondent standards relevant for tests as specified in appendix 9 of Tachograph Specification [EU], Annex 1B.

The vehicle unit supports also up to two CAN (Controller Area Network) interfaces based on ISO 11898 and parts of SAE J1939 - Recommended Practice for a Serial Control and Communications Vehicle Network.

The TOE shall be evaluated and certificated in accordance with the Common Criteria (CC) under consideration of the interpretations in [JIL]. In order to achieve the required system security, the vehicle unit and the corresponding ST meet all the security requirements and evaluation conditions defined in the “Vehicle Unit Generic Security Target” in [EU], Appendix 10.

The main objectives of this ST are

- to describe the TOE as a Vehicle Unit for the Tachograph System
- to define the limits of the TOE
- to describe the assumptions, threats and security objectives for the TOE
- to describe the security requirements for the TOE
- to define the TOE security functions

## 1.3 CC Conformance

The CC evaluation of the TOE is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.3, August 2005 [CC1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.3, August 2005 [CC2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.3, August 2005 [CC3]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005 [CM]

This Security Target is written in accordance with the above mentioned Common Criteria

Version 2.3 and claims the following CC conformances:

- Part 2 conformant
- Part 3 conformant

Furthermore, the ST will be written in view of the requirements of the Generic Security Target for Vehicle Units within the Tachograph Specification [EU], Appendix 10 and the interpretations and requirements of the Joint Interpretation Library (JIL) [JIL].

The chosen level of assurance for the TOE is **EAL 4 augmented**. The augmentation includes the assurance components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4.

The minimum strength level for the TOE security functions is **SOF-high**.

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 " Secure Microcontroller ATMEL AT90SC320288RCT/AT90SC144144CT rev. G" provided by ATMEL. The IC is evaluated according to Common Criteria EAL 4 augmented with a minimum strength level for its security functions of SOF-high and is listed under the Certification ID 2006/20 by DCSSI. The evaluation of the IC is based on the Protection Profile PP/9806.

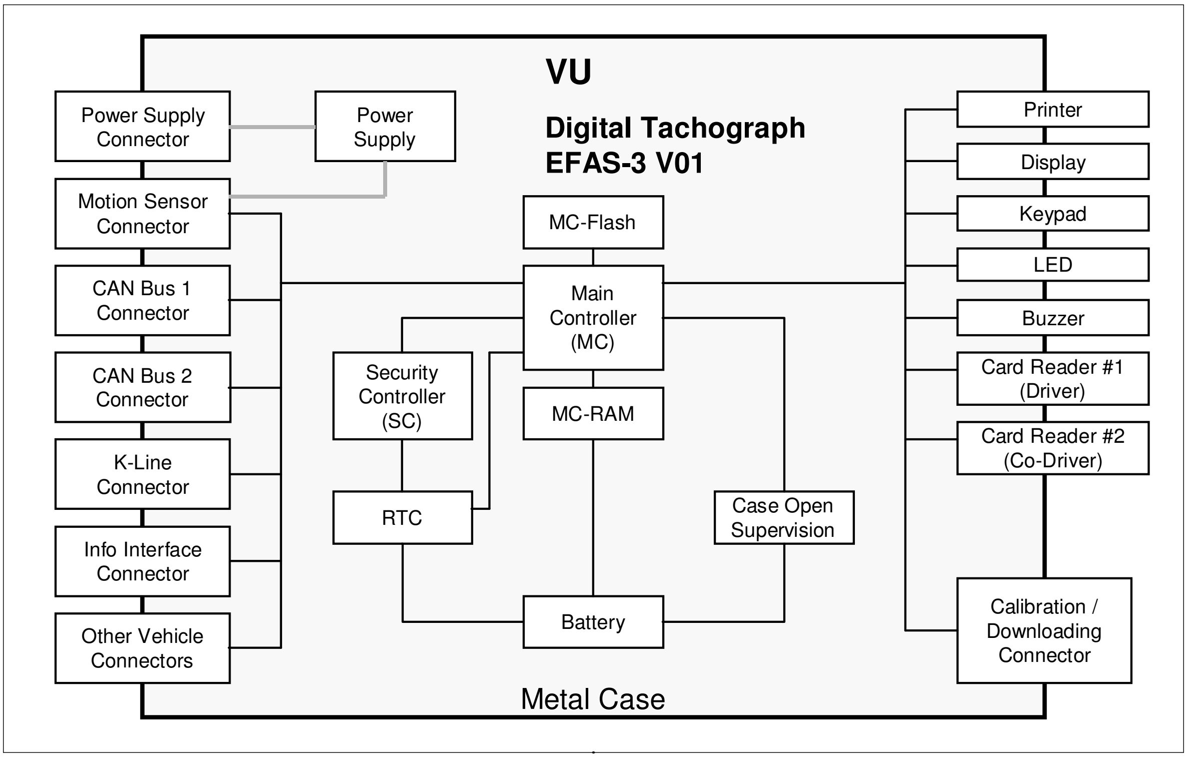
# 2 TOE Description

## 2.1 TOE Definition

### 2.1.1 Architecture Overview

The Target of Evaluation (TOE) is the Digital Tachograph EFAS-3 V01 (EFAS-3 or vehicle unit (VU) for short in the following). It is designed in accordance with the Tachograph Specification [EU]. The security relevant parts are specified in appendix 10 (Vehicle Unit Generic Security Target) and appendix 11 of [EU].

Picture1 shows all physical interfaces of the EFAS-3 and the security relevant internal components.



***Picture 1. TOE architecture overview***

### 2.1.2 TOE Hardware

The hardware components are:

**Security Controller (SC)**

The security controller is micro controller that consist of a central processing unit, a cryptographic coprocessor and embedded RAM and EEPROM 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 and has exclusive access to the VU onboard flash and RAM.

**MC Flash**

The MC flash contains the software for the MC as well as configuration and user data.

**MC RAM**

The MC RAM stores temporary data.

**Real Time Clock (RTC)**

The RTC provides the EFAS-3 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 top cover is opened or the VU battery is unplugged.

**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 sealed screws and the case opening switch, which triggeres the case open supervision circuit when released.

### 2.1.3 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 management device 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 update.

### 2.1.4 TOE Product Scope

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

- The vehicle unit EFAS-3 V01, Hardware/Software

  Delivery configurations are possible for EFAS-3 V01 in accordance with the corresponding type code (see Table 1 below).
- Operating Manual EFAS-3, Document in paper / electronic pdf-form (for all kind of users)

| **EFAS-3 V01** | **24** | **gg** | **D7** | **A1** | **C0** | **R1** | *Code* | *Meaning* |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | R0 =<br>R1 = | no additional data recording<br>additional data recording for rpm, speed and status inputs |
| | | | | | | | C0 =<br>C1 = | no CAN bus on connector C<br>CAN bus on connector C with terminating resistor |
| | | | | | | | A0 =<br>A1 =<br>A2 = | no CAN bus on connector A<br>CAN bus on connector A with terminating resistor<br>CAN bus on connector A without terminating resistor |
| | | | | | | | D7 =<br>D8 = | K-Line connected to D7<br>Info interface connected to D8 |
| | | | | | | | aa =<br>br =<br>gg =<br>yy = | Display, keyboard illumination: amber/amber<br>Display, keyboard illumination: blue/red<br>Display, keyboard illumination: green/green<br>Display, keyboard illumination: yellow/yellow |
| | | | | | | | 12 =<br>24 = | 12 V power supply<br>24 V power supply |

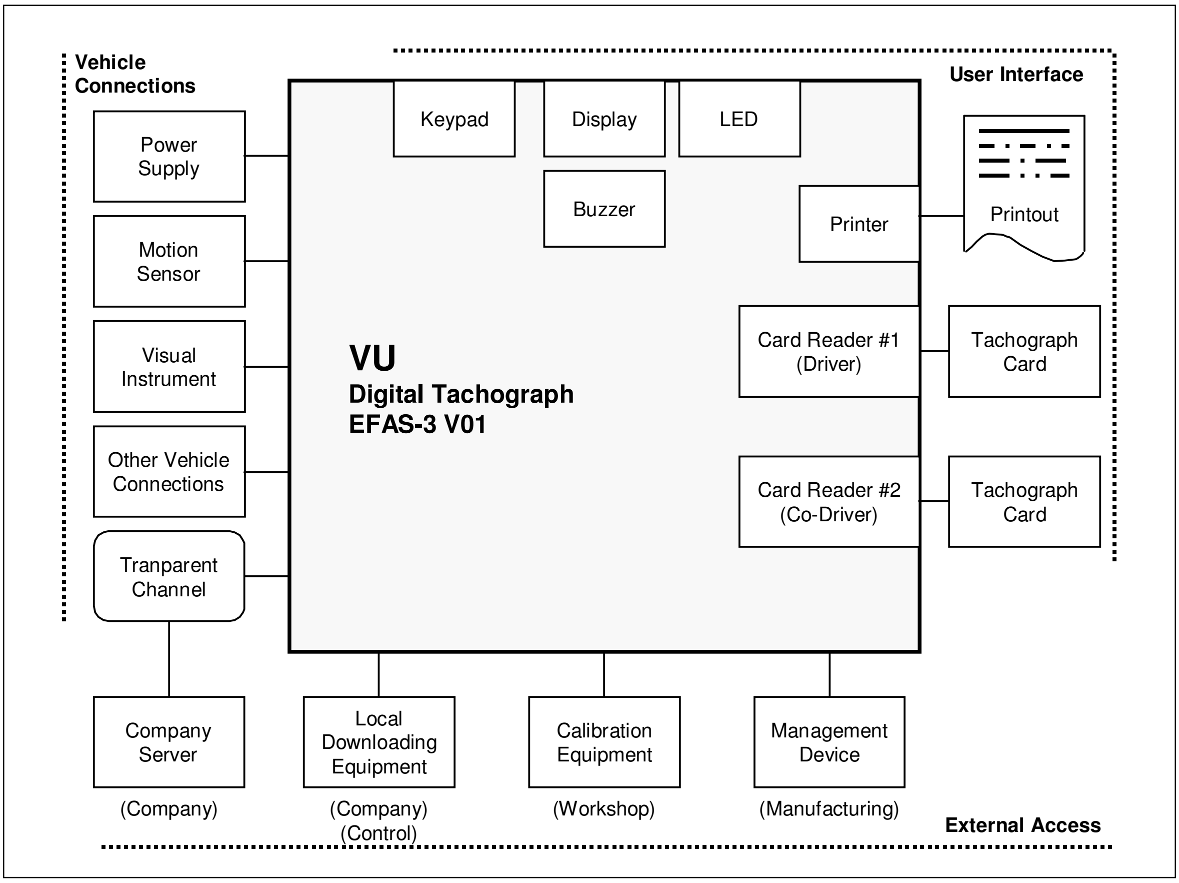
**Table 1: System of the type code**

For workshop personnel Service and Installation Manual EFAS-3, Document in paper / electronic pdf-form will be delivered.

The TOE variants are necessary to operate in the environment of vehicles from different vehicle manufacturers or different categories of vehicles. Therefore, there are two main hardware versions possible for the VU: EFAS-3 V01 24 and EFAS-3 V01 12 for vehicles with a 24 V resp. a 12 V power supply. Based on this variants 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).

## 2.2 TOE Intended Usage

Picture 2 shows the logical interfaces and operational environment of the TOE.



***Picture 2. Operational Environment of the TOE***

As a digital tachograph, the VU is installed in a road vehicle. The main tasks of the VU are:

- To record motion data and driver activities for later examination by a control body.
- To support the driver to meet the legal regulations (road speed limits, driving times).
- To transmit the user activities data for recording in Tachograph Cards or other storage media.

The VU makes use of the following inputs to execute these tasks:

- Motion data from a motion sensor in the gear box.
- Keys pressed by the user.
- Data stored on smartcards ("Tachograph cards"). Two card slots are provided, one for the driver and one for the codriver. (see also the note at the end of this chapter).

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). The motion data and event indications are forwarded to the "Visual Instrument" (tachometer) of the vehicle for better visibility.

The recorded data can be accessed by:

- Printouts generated by the build-in thermal printer.
- Downloading to the 'Local Downloading Equipment' connected to the calibration/downloading connector at the front of the VU.
- Downloading to the 'Company Server' via a wireless downloading connection.

Other logical interfaces:

- Power Supply:

  The VU is connected to the vehicle battery and to the ignition switch.

- Motion Sensor:

  The motion sensor in the gear box is directly connected to the VU. This cable has no interconnections to the remaining vehicle electronics.

- Visual Instrument:

  Display of vehicle speed, alarms etc. on the dashboard of the vehicle. Depending on the vehicle, non-EU relevant operations like acknowledge of diagnostic trouble codes and time zone changes are possible.

- Other Vehicle Connections:

  The VU receives engine speed pulses and optional status input for registration. These connections have no influence on the EU functionality of the TOE.

- Calibration Equipment:

  The calibration equipment is used by workshops to calibrate, to test and to configure the VU. In addition, downloading of recorded data and update of the MC application software is possible.

- Management Device (Security Server):

  The management device is responsible for the personalization of the VU. The management device is available in the manufacturing environment only.

Regarding the security of the Tachograph System the main security objective is the following. The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed. The EFAS-3 provides the operation modes and corresponding access to the data in accordance with the requirements 007 of [EU] (see 5.1.1.1 and the note at the end of this section).

EFAS-3 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 the EFAS-3 generates audit records with associated data. The EFAS-3 preserves a secure state independent from the values of the power supply, including cut-off, and prevents a misuse of security relevant data involved in its operations.

Especially the following security mechanisms contributing to the global security objective are relevant for the EFAS-3:

- mutual authentication between the EFAS-3 and a Tachograph Card, including session key agreement
- confidentiality, integrity and authentication of data transferred between the EFAS-3 and a Tachograph Card
- mutual authentication between the VU and the motion sensor connected to the EFAS-3 including session key agreement during pairing
- confidentiality, integrity and authentication of data transferred between the EFAS-3 and the motion sensor connected to the EFAS-3 after pairing
- integrity and authentication of data downloaded from a EFAS-3 to external storage media (incl. wireless remote downloading connection)
- authentication via a wireless remote connection to the EFAS-3
- authentication of the management device to the EFAS-3

- integrity and authentication of data downloaded from the management device to the EFAS-3

The EFAS-3 offers a RSA public key cryptographic system to provide the following security mechanisms:

- authentication between the EFAS-3 and a Tachograph Card
- transport of Triple-DES session keys between the EFAS-3 and a Tachograph Card
- digital signature of data downloaded from the EFAS-3 to an external storage medium
- digital signature of data downloaded from the management device to the EFAS-3

Furthermore, the EFAS-3 offers Triple DES symmetric cryptographic systems to provide

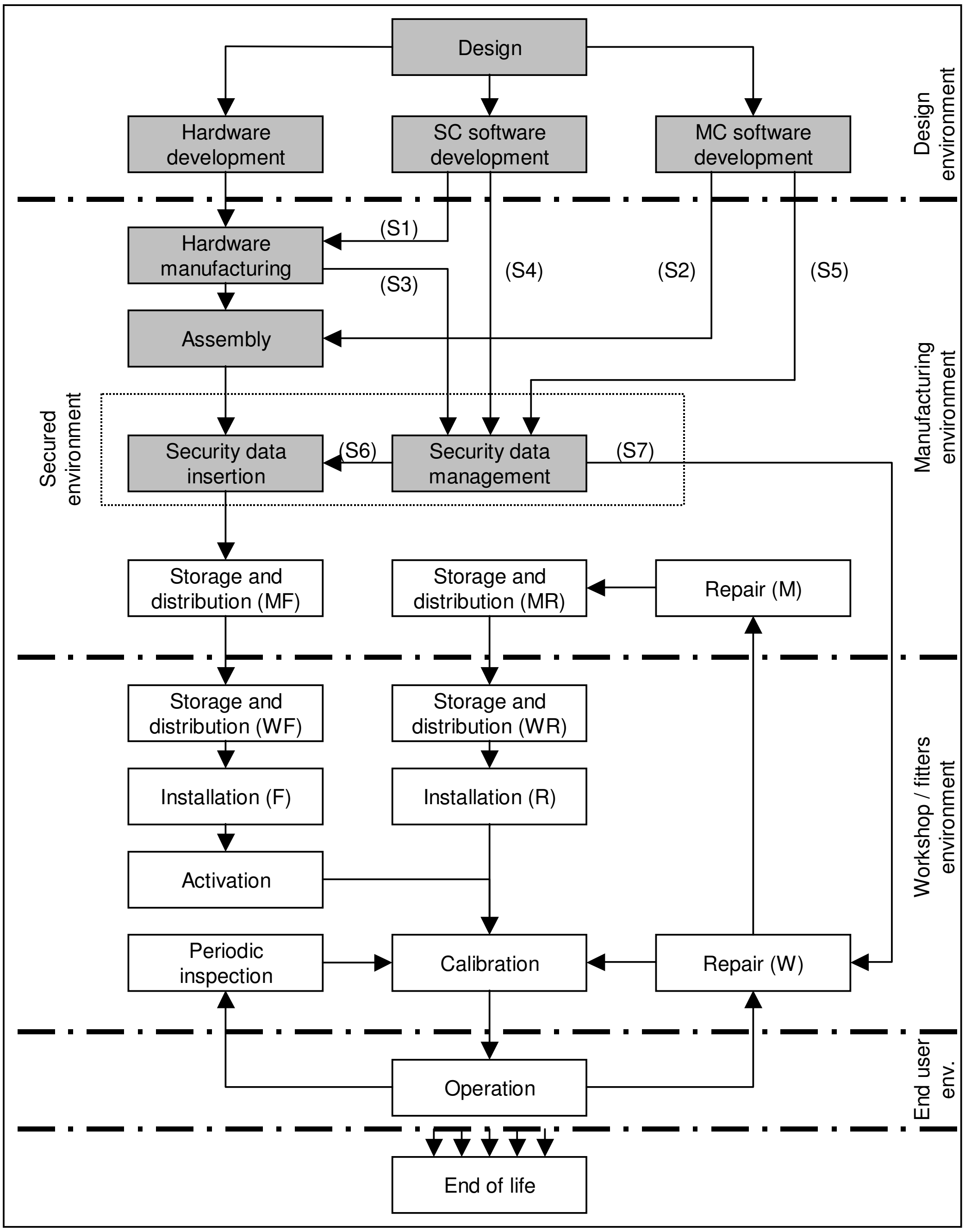
- a mechanism for data integrity during data exchange between the EFAS-3 and a Tachograph Card, and to provide, where applicable, confidentiality of data exchange between the EFAS-3 and a Tachograph Card
- a mechanism for data integrity during data exchange between the EFAS-3 and the connected motion sensor, and to provide, where applicable, confidentiality of data exchange between the EFAS-3 and the connected motion sensor and to provide a scheme for session key agreement during pairing between the EFAS-3 and the connected motion sensor
- a mechanism for mutual authentication between the VU and the management device as well as for data integrity during data exchange between the EFAS-3 and the management device
- a mechanism for mutual authentication between the VU and a remote company server (with connection to a Company Card) as well as for data integrity during data exchange between the EFAS-3 and the remote company server

Note: A Tachograph Card may be of the following types:

- Company Card: a Tachograph Card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment; identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company.
- Control Card: a Tachograph Card issued by the authorities of a Member State to a national competent control authority; identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading.
- Driver Card: a Tachograph Card issued by the authorities of a Member State to a particular driver identifying the driver and allowing for storage of driver activity data.
- Workshop Card: a Tachograph Card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop approved by that Member State; identifies the cardholder and allows for testing, calibration, downloading, configuration and software update of the recording equipment.

## 2.3 TOE Life-Cycle

The life cycle of the EFAS-3 is based on the principles described in [EU], appendix 10, chapter 3.2, as shown in Picture 3. Grayed blocks indicate the developing and manufacturing steps before delivery.



*Picture 3. TOE Life Cycle*

### 2.3.1 Design Phase

The design of the TOE includes the complete specification of the hardware and software, the implementation and testing of the EFAS-3 software.

### 2.3.2 Production Phase

During the production phase (blocks "Hardware manufacturing" and "Assembly"), the VU hardware is manufactured and assembled.

As part of hardware manufacturing, the SC (security controller) software is inserted into the SC (S1) and secured against any modification and read out. The MC (main controller) software is inserted into the MC as part of the assembly (S2).

The production phase results in a completely assembled and tested EFAS-3 containing the final software and ready for personalization. The case is closed and sealed.

### 2.3.3 Personalization

The personalization (block "Security data insertion")

During the personalization (block "Security data insertion") the security data are inserted into the VU:

- The EU certificate $C_{EU}$, containing the EU public key
- The member state certificate $C_{MS}$, signed by EU, containing member state public key.
- The VU certificate $C_{MS}$, signed by the member state authorities, containing the VU public key.
- The VU secret key.
- The VU identification data.
- The the partial initialisation key of the motion sensor ($KM_{VU}$).
- The current time.

The personalization is only executed if the security server (part of the security management) is able to establish the authenticity of the VU based on the 'transport code' generated during SC manufacturing (S3) and the expected SC (S4) and MC (S5) software identities.

Before the personalization is executed successfully, the VU is in life cycle state 'PRODUCTION'. After the personalization, the VU is in life cycle state 'STORAGE' and ready for distribution.

### 2.3.4 First Installation and Activation

The VU is installed in a vehicle and activated by insertion of a workshop card. The VU activation comprises the pairing with the motion sensor.

At the end of the VU activation, all data recording and security enforcing functions are fully operational. The life cycle state of the EFAS-3 is 'ACTIVATED'. The EFAS-3 remains in this state for the rest of its life.

### 2.3.5 Calibration

Before the vehicle leaves the premises of the fitter / workshop, a calibration has to be performed.

If this is the first calibration after installation in a vehicle (either of a new or a repaired VU), the vehicle identification must be stored in the VU.

After calibration the VU is ready for operation.

### 2.3.6 Periodic Inspection

The VU is inspected at least every two years by a workshop. According to [EU], definition (cc), a "periodic inspection" means "set of operations performed to control that the recording equipment works properly and that its settings".

### 2.3.7 Repair by Workshop

A workshop can replace the printer and the battery. After repair, a calibration has to be executed.

### 2.3.8 Repair by Manufacturer

A repair by the manufacturer is restricted to the replacement of parts which do not contain stored data or code.

### 2.3.9 Software Update

A software update can be executed by a workshop on the basis of crypted update data prepared by the management device in the manufacturing environment (S7).

### 2.3.10 Installation of a Repaired VU

In most cases, the repaired VU is installed in a different vehicle. During the following calibration the data of the new vehicle have to be written to the VU.

## 2.4 TOE Environment

### 2.4.1 Development Environment

The EFAS-3 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 organised based on formal methods. Suitable measures enforces the usage of the guidelines. The complete development of the TOE is well documented supported by ISO 9001:2000 certified procedures. The confidentiality and integrity of development results is protected (usage of files 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.

### 2.4.2 Manufacturing Environment

In the manufacturing environment responsibilities are assigned in manner which maintains IT security and the EFAS-3 is protected from physical attacks which might compromise IT security. The manufacturing environment is well documented supported by procedures based on ISO 9001:2000. Measures are defined to protect security data like cryptographic keys against disclosure and manipulation. Security data generation algorithms are accessible to authorised and trusted persons only. Security data are generated, transported, and inserted into the EFAS-3, in such a way to preserve its appropriate confidentiality and integrity.

Leaving the manufacturing environment the TOE is complete and delivered to the customer.

### 2.4.3 Fitters and Workshop Environment

Installation, calibration and repair of recording equipment are carried by trusted and approved fitters or workshops. Recording equipment are periodically inspected and calibrated. Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.

EFAS-3 manufacturers, vehicle manufacturers and fitters or workshops ensures that handling of non activated EFAS-3 is done in a manner which maintains EFAS-3 security. Vehicle manufacturers and fitters or workshops activate the EFAS-3 after its installation before the vehicle leaves the premises where installation took place.

### 2.4.4 End User Environment

In this environment drivers play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, ...). Law enforcement controls are performed regularly and randomly, and include security audits. Software revisions are granted security certification before they can be implemented in a EFAS-3.

# 3 TOE Security Environment

## 3.1 Assets

Assets are security-relevant elements to be directly protected by the TOE whereby assets have to be protected in terms of confidentiality and integrity. Confidentiality of assets is always intended with respect to not trusted users of the TOE, whereas the integrity of assets is relevant for the correct operation and the for the main functionality of the TOE (i.e. to operate, store and make available user data). Note: Limiting to the TOE excluding the environment only the cryptographic keys and the PIN of the workshop card are secrecy assets.

### 3.1.1 Primary Assets

Primary assets are application specific user data related to requirements 081 to 093 and 102 to 105b inclusive once recorded. User data are any data, other than security data, recorded or stored by the VU, required by chapter III.1.2 of Annex 1B (see Annex, chapter 9.3).

### 3.1.2 Secondary Assets

Secondary assets are

- data exchanged with the motion sensor, representative of speed and distance travelled (motion data).
- specific data needed to support TSF (e.g. cryptographic keys)
- logical, physical design data of the TOE hardware
- software specifications, code and other related documentation
- development aids, test data, user data related documentation
- TSF data
- material for software development
- special functions for the communication with an external interface device
- the SC and the RTC

The SC and its internal components belong to the assets by reason of the [ATMEL_ST], chap. 3.1.

## 3.2 Assumptions

### 3.2.1 General Assumptions for the TOE

For the description of the assumptions related to the SC refer to [ATMEL_ST], chap. 3.2.4. The assumptions related to the SC environment are considered in this ST as OSP P.Design (SC assumptions A.SOFT_ARCHI, A.DEV_ORG, A.DLV_PROTECT, A.DLV_AUDIT, A.DLV_RESP, A.USE_TEST and A.USE_PROD) and as EFAS-3 security objectives O.Authentication and O.Integrity (SC assumptions A.USE_DIAG and A.USE_SYS)

The general assumptions made on the environment of the TOE are defined according to [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 3.6. This paragraph describes physical, personnel or procedural requirements that contribute to the security of the environment of the TOE. The physical, personnel and procedural means are translated into assumptions for the environment of the TOE. Thereby all assumptions are for the non-IT-environment.

#### 3.2.1.1 Equipment design

| | |
|---|---|
| A.Development | It is assumed that the EFAS-3 developers ensure that the assignment of responsibilities during development is done in a manner which maintains IT security. |
| A.Manufacturing | It is assumed that the EFAS-3 manufacturers ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the EFAS-3 is protected from physical attacks which might compromise IT security. |

**Table 2: Equipment design**

#### 3.2.1.2 Equipment delivery and activation

| | |
|---|---|
| A.Delivery | It is assumed that the EFAS-3 manufacturers, vehicle manufacturers and fitters or workshops ensure that handling of non activated EFAS-3 is done in a manner which maintains EFAS-3 security. |
| A.Activation | It is assumed that vehicle manufacturers and fitters or workshops activate the EFAS-3 after its installation before the vehicle leaves the premises where installation took place. |

**Table 3: Equipment delivery and activation**

#### 3.2.1.3 Security data generation and delivery

| | |
|---|---|
| A.Sec_Data_Generation | It is assumed that security data generation algorithms are accessible to authorised and trusted persons only. |
| A.Sec_Data_Transport | It is assumed that security data are generated, transported and inserted into the EFAS-3 in such a way to preserve its appropriate confidentiality and integrity. |

**Table 4: Security data generation and delivery**

#### 3.2.1.4 Cards delivery

| | |
|---|---|
| A.Card_Availability | It is assumed that tachograph cards are available and delivered to authorised persons only. |
| A.Driver_Card_Uniqueness | It is assumed that drivers possess, at one time, one valid driver card only. |
| A.Card_Traceability | It is assumed that card delivery is traceable (white lists, black lists), and black lists are used during security audits. |

**Table 5: Cards delivery**

#### 3.2.1.5 Recording equipment installation, calibration and inspection

| | |
|---|---|
| A.Approved_Workshops | It is assumed that installation, calibration and repair of recording equipment are carried by trusted and approved fitters or workshops. |
| A.Regular_Inpections | It is assumed that recording equipment is periodically inspected and calibrated. |
| A.Faithful_Calibration | It is assumed that approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration. |

**Table 6: Recording equipment installation, calibration, and inspection**

#### 3.2.1.6 Equipment operation

| | |
|---|---|
| A.Faithful_Drivers | It is assumed that drivers play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, ...). |

**Table 7: Equipment operation**

#### 3.2.1.7 Law enforcement control

| | |
|---|---|
| A.Controls | It is assumed that law enforcement controls are performed regularly and randomly, and include security audits. |

**Table 8: Law enforcement control**

#### 3.2.1.8 Software upgrades

| | |
|---|---|
| A.Software_Upgrade | It is assumed that software revisions are granted security certification before they can be implemented in a EFAS-3. |

**Table 9: Software upgrades**

### 3.2.2 Specific Assumptions for the TOE

There do not exist any Vehicle Unit specific assumptions for the environment of the TOE.

## 3.3 Threats

For the definition of the threats related to the SC refer to [ATMEL_ST], chap. 3.3. As the SC and its components belong to the assets of the EFAS-3 all threats of the SC are relevant for the TOE.

The TOE is required to counter different types of attacks against its specific assets. A threat agent could try to threaten these assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

Based on the specific functionality of the VU only drivers or their company representatives are interested in the manipulation of the motion and driver activity data to avoid the corresponding legal requirements. Possible workshop personal could be in attacker range. For the organized crime it is not really profitable to invest time and money for attacks because the price for the manipulated data or even manipulated devices would not cover the attack costs. The same applies for the attacks with the aim to damage a company image. However, attackers with high attack potential have to be considered because of the evaluation level.

Generally, threats can be split into the following types:

- threats against which a specific protection by the TOE is required
- threats against which a specific protection by the environment is required
- threats against which a specific protection by a combination of the TOE and the environment is required

The following tables list the threats. The threats are provided by the Tachograph Specification [EU], Appendix 10, Vehicle Unit Generic Security Target, chapter 3.3 and are supplemented for the TOE´s personalisation.

### 3.3.1 Threats to identification and access control policies

| | |
|---|---|
| T.Access | Drivers (or other unauthorised users) could try to access functions not allowed to them (e.g. drivers gaining access to calibration function) |
| T.Identification | Drivers could try to use several identifications or no identification. |

**Table 10: Threats to identification and access control policies**

No special knowledge is needed to identify the general possibility because drivers know that the calibration mode exists. The driver could attack the TOE by trial and error or could try to gain a workshop card and perform the brute force attacks to guess the PIN. The efforts in time and money to perform such attacks could be very high.

### 3.3.2 Design related threats

| | |
|---|---|
| T.Faults | Faults in hardware, software or communication procedures could place the EFAS-3 in unforeseen conditions compromising its security |

| | |
|---|---|
| T.Tests | The use of non invalidated test modes or of existing back doors could compromise the EFAS-3 security |
| T.Design | Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, ...) or from reverse engineering |

**Table 11: Design related threats**

A special technical background is required to perform attacks based on vulnerabilities resulted from design errors This kind of attack usually presupposes special knowledge about the TOE and often special equipment (attackers with high attack potential). Which kind of knowledge or equipment is needed is highly dependent on the identified vulnerability the threat tries to exploit.

### 3.3.3 Operation oriented threats

| | |
|---|---|
| T.Calibration_Parameters | Users could try to use mis-calibrated equipment (through calibration data modification, or through organisational weaknesses) |
| T.Card_Data_Exchange | Users could try to modify data while exchanged between EFAS-3 and tachograph cards (addition, modification, deletion, replay of signal) |
| T.Clock | Users could try to modify internal clock |
| T.Environment | Users could compromise the EFAS-3 security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, ...) |
| T.Fake_Devices | Users could try to connect fake devices (motion sensor, tachograph card) to the EFAS-3 |
| T.Hardware | Users could try to modify EFAS-3 hardware |
| T.Motion_Data | Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal) |
| T.Non_Activated | Users could use non activated equipment |
| T.Output_Data | Users could try to modify data output (print, display or download) |
| T.Power_Supply | Users could try to defeat the EFAS-3 security objectives by modifying (cutting, reducing, increasing) its power supply |
| T.Security_Data | Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment |
| T.Software | Users could try to modify EFAS-3 software |
| T.Stored_Data | Users could try to modify stored data (security or user data). |

**Table 12: Operation oriented threats**

The direction of the attacks is the TOE itself resp. the interfaces of the TOE. A special technical background is required to perform such attacks (attackers with high attack potential). An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. An attacker may cause a malfunction of the software by applying environmental stress in order to deactivate or modify security features or functions of the TOE or circumvent or deactivate or modify security functions. This kind of attack usually presupposes special knowledge about the TOE and often special equipment. Which kind of knowledge or equipment is needed is highly dependent on the identified vulnerability the threat tries to exploit.

## 3.4 Organisational Security Policies of the TOE

The security functionality of the TOE is dependent on a correct and effective implementation of the Security Controller software. In particular this means that the SC software has to fulfil the relevant assumptions for the SC as defined in the Security Target for the SC [ATMEL_ST], chap. 3.2.4.

The relevant assumptions for the SC (A.SOFT_ARCHI, A.DEV_ORG, A.DLV_PROTECT, A.DLV_AUDIT, A.DLV_RESP, A.USE_TEST and A.USE_PROD) are suitably redefined in terms of Organisational Security Policies P.Design for the TOE as follows:

| | |
|---|---|
| P.Design | To ensure that the SC is used in a secure manner the SC software shall be designed so that the requirements from the SC developer belong to software implementation are met. |

Furthermore, the OSP P.CRYPTO (Cryptographic entities, data authentication, and approval functions must be in accordance with ISO, associated industry, or organizational standards or requirements) defined in the Security Target for the SC [ATMEL_ST], chap. 3.4. is relevant for the EFAS-3.

# 4 Security Objectives

The main security objective of the digital tachograph system is the following:

| | |
|---|---|
| O.Main | The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed |

**Table 13: Main security objective of the digital tachograph system**

The security objectives for the TOE are drawn from the Tachograph Specification [EU], Appendix 10, Vehicle Unit Generic Security Target, chapter 3.4 and 3.5.

The security objectives of the TOE, contributing to the global security objective, are the following:

| | |
|---|---|
| O.VU_Main | The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed. |
| O.VU_Export | The EFAS-3 must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity. |

**Table 14: Global security objectives**

The following security objectives refine the fundamental security objectives O.VU_Main and O.VU_Export and represent as a whole the security objectives O.VU_Main and O.VU_Export.

## 4.1 Security Objectives for the TOE

For the definition of the security objectives related to the SC refer to [ATMEL_ST], chap. 4.1. All security objectives for the SC are relevant for the EFAS-3 and are included to the Security Objectives for the TOE.

The specific IT security objectives of the TOE contributing to its main security objectives, are the following:

| | |
|---|---|
| O.Access | The EFAS-3 must control user access to functions and data |
| O.Accountability | The EFAS-3 must collect accurate accountability data. |
| O.Audit | The EFAS-3 must audit attempts to undermine system security and should trace them to associated users |
| O.Authentication | The EFAS-3 should authenticate users and connected entities (when a trusted path needs to be established between entities) |
| O.Integrity | The EFAS-3 must maintain stored data integrity. |

| | |
|---|---|
| O.Output | The EFAS-3 must ensure that data output reflects accurately data measured or stored |
| O.Processing | The EFAS-3 must ensure that processing of inputs to derive user data is accurate |
| O.Reliability | The EFAS-3 must provide a reliable service |
| O.Secured_Data_Exchange | The EFAS-3 must secure data exchanges with the motion sensor and with tachograph cards |
| O.Design | The EFAS-3SC software must be designed in accordance with the requirements of the SC developer, so that the SC is used in secure manner. |

**Table 15: Information technology security objectives**

## 4.2 Security Objectives for the Environment

The security objectives related to the SC environment are defined in chapter 4.2 of [ATMEL_ST]: O.DEV_DIS, O.SOFT_DLV, O.SOFT_MECH, O.DEV_TOOLS, O.SOFT_ACS, O.DESIGN_ACS, O.DSOFT_ACS, O.MASK_FAB, O.MECH_ACS, O.TI_ACS, O.TOE_PRT, O.IC_DLV, O.DLV_PROTECT, O.DLV_AUDIT, O.DLV_RESP, O.TEST_OPERATE, O.USE_DIAG and O.USE_SYS. All security objectives for the SC environment except the two last objectives (O.USE_DIAG and O.USE_SYS) are taken into account as security objectives for the EFAS-3 environment OE.Development, OE.Manufacturing and OE.Delivery. The security objectives O.USE_DIAG and O.USE_SYS are included as the security objectives for the EFAS-3 O.Authentication and O.Integrity.

The general assumptions made on the environment of the TOE are defined according to [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 3.6. This paragraph describes physical, personnel or procedural requirements that contribute to the security of the environment of the TOE. The physical, personnel and procedural means are translated into assumptions and security objectives for the environment of the TOE. Thereby all security objectives are for the non-IT-environment.

### 4.2.1 Equipment design

| | |
|---|---|
| OE.Development | The EFAS-3 developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security |
| OE.Manufacturing | The EFAS-3 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 EFAS-3 is protected from physical attacks which might compromise IT security |

**Table 16: Equipment design**

### 4.2.2 Equipment delivery and activation

| | |
|---|---|
| OE.Delivery | The EFAS-3 manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of non activated EFAS-3 is done in a manner which maintains EFAS-3 security |
| OE.Activation | Vehicle manufacturers and fitters or workshops must activate the EFAS-3 after its installation before the vehicle leaves the premises where installation took place |

**Table 17: Equipment delivery and activation**

### 4.2.3 Security data generation and delivery

| | |
|---|---|
| OE.Sec_Data_Generation | Security data generation algorithms must be accessible to authorised and trusted persons only. |
| OE.Sec_Data_Transport | Security data must be generated, transported, and inserted into the EFAS-3, in such a way to preserve its appropriate confidentiality and integrity. |

**Table 18: Security data generation and delivery**

### 4.2.4 Cards delivery

| | |
|---|---|
| OE.Card_Availability | Tachograph cards must be available and delivered to authorised persons only. |
| OE.Driver_Card_Uniqueness | Drivers must possess, at one time, **one** valid driver card only. |
| OE.Card_Traceability | Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits. |

**Table 19: Cards delivery**

### 4.2.5 Recording equipment installation, calibration, and inspection

| | |
|---|---|
| OE.Approved_Workshops | Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops. |
| OE.Regular_Inspections | Recording equipment must be periodically inspected and calibrated. |
| OE.Faithful_Calibration | Approved fitters and workshops must be entered proper vehicle parameters in recording equipment during calibration. |

**Table 20: Recording equipment installation, calibration, and inspection**

### 4.2.6 Equipment operation

| | |
|---|---|
| OE.Faithful_Drivers | Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, ...). |

**Table 21: Equipment operation**

### 4.2.7 Law enforcement control

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

**Table 22: Table 21: Law enforcement control**

### 4.2.8 Software upgrades

| | |
|---|---|
| OE.Software_Upgrade | Software revisions must be granted security certification before they can be implemented in EFAS-3. |

**Table 23: Software upgrades**

# 5 IT Security Requirements

## 5.1 TOE Security Requirements

For the definition of the SFRs related to the SC refer to the Security Target [ATMEL_ST], chap. 5.2 and 5.3.

This section consists of the subsection “TOE Functional Requirements” and “TOE Security Assurance Requirements”.

### 5.1.1 TOE Security Functional Requirements

The TOE security functional requirements (SFRs) define the functional requirements for the TOE using functional requirement components drawn from CC Part 2 [CC2], functional components of CC Part 2 [CC2] with extensions. This chapter contains the security function policy and all SFRs concerning the TOE.

#### 5.1.1.1 Security Function Policy for Access Control (AC_SFP)

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so. It must be noted that the user data recorded by the VU, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011, see below) is not the subject of a security enforcing function.

Requirement 011:

The recording equipment can output any data to display, printer or external interfaces with the following exceptions:

- in the operational mode, any personal identification (surname and first name(s)) not corresponding to a tachograph card inserted shall be blanked and any card number not corresponding to a tachograph card inserted shall be partially blanked (every odd character . from left to right . shall be blanked),
- in the company mode, driver related data (requirements 081, 084 and 087) can be output only for periods not locked by another company (as identified by the first 13 digits of the company card number),
- when no card is inserted in the recording equipment, driver related data can be output only for the current and eight previous calendar days.

##### *5.1.1.1.1 Access Control Policy*

Appendix 10, ACC_201:

The VU shall manage and check access control rights to functions and to data.

##### *5.1.1.1.2 Access Rights to functions*

Appendix 10, ACC_202:

The VU shall enforce the mode of operation selection rules according to the following requirements:

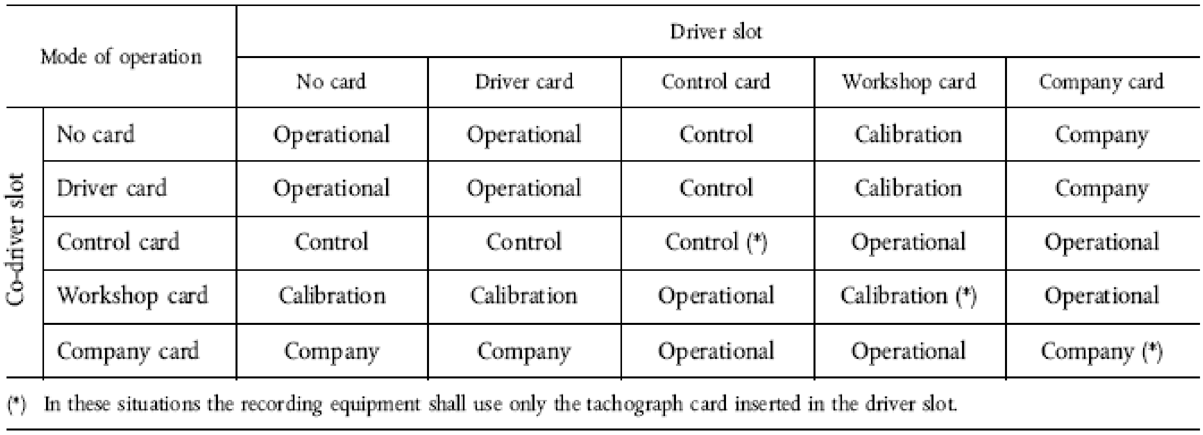
(Requirement 006):

According to the recording equipment shall possess four modes of operation:

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

(Requirement 007 and 008):

The recording equipment shall switch to the following mode of operation according to the valid tachograph cards inserted into the card interface devices:



| 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 (*) |

(*) In these situations the recording equipment shall use only the tachograph card inserted in the driver slot.

(Requirement 009):

The recording equipment shall ignore non-valid cards inserted, except displaying, printing or downloading data held on an expired card which shall be possible.

Appendix 10, ACC_203:

The VU shall use the mode of operation to enforce the functions access control rules according to:

(Requirement 010):

All functions listed in II.2. of [EU], Annex 1B shall work in any mode of operation with the following exceptions:

- the calibration function is accessible in the calibration mode only,
- the time adjustment function is limited when not in the calibration mode,
- the driver manual entries functions are accessible in operational or calibration modes only,
- the company locks management function is accessible in the company mode only,
- the monitoring of control activities function is operational in the control mode only,
- the downloading function is not accessible in the operational mode (except as provided for in (Requirement 150): In addition and as an optional feature, the recording equipment may, in any mode of operation, download data through another connector to a company authenticated through this channel. In such a case, company mode data access rights shall apply to this download.).

#### *5.1.1.1.3 Access rights to data*

Appendix 10, ACC_204:

The VU shall enforce the VU identification data write access rules as following:

(Requirement 076):

Vehicle unit identification data are recorded and stored once and for all by the Vehicle Unit manufacturer, except the software-related data and the approval number which may be changed in case of software upgrade.

(Requirement 079):

The Vehicle Unit shall be able to record and store in its data memory the following currently paired motion sensor identification data:

- serial number,
- approval number,

- first pairing date.

(Requirement 155):

Pairing the motion sensor to the VU shall consist, at least, in:

- updating motion sensor installation data held by the motion sensor (as needed),
- copying from the motion sensor to the VU data memory necessary motion sensor identification data.

Appendix 10, ACC_205:

The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155).

Appendix 10, ACC_206:

After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory:

(Requirement 154):

The calibration function shall allow:

- to automatically pair the motion sensor with the VU,
- to digitally adapt the constant of the recording equipment (k, as defined in the definition part of [EU], Annex 1B) to the characteristic coefficient of the vehicle (w, as defined in the definition part of [EU], Annex 1B) (vehicles with two or more axle ratios shall be fitted with a switch device whereby these various ratios will automatically be brought into line with the ratio for which the equipment has been adapted to the vehicle),
- to adjust (without limitation) the current time,
- to adjust the current odometer value,
- to update motion sensor identification data stored in the data memory,
- to update or confirm other parameters known to the recording equipment: vehicle identification, w (as defined in the definition part of [EU], Annex 1B), l (as defined in the definition part of [EU], Annex 1B), tyre size and speed limiting device setting if applicable.

(Requirement 156):

The calibration function shall be able to input necessary data through the calibration/ downloading connector in accordance with the calibration protocol defined in Appendix 8.

Appendix 10, ACC_207:

After the VU activation, the VU shall enforce calibration data write and delete access rules:

(Requirement 097):

The recording equipment shall record and store in its data memory data relevant to:

- known calibration parameters at the moment of activation,
- its very first calibration following its activation,
- its first calibration in the current vehicle (as identified by its Vehicle Identification Number (VIN)),
- the five most recent calibrations (If several calibrations happen within one calendar day, only the last one of the day shall be stored).

Appendix 10, ACC_208:

After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory. This requirement does not apply to small time adjustments allowed by

(Requirement 157):

The time adjustment function shall allow for adjusting the current time in amounts of one minute maximum at intervals of not less than seven days.

(Requirement 158):

The time adjustment function shall allow for adjusting the current time without limitation, in calibration mode.

Appendix 10, ACC_209:

After the VU activation, the VU shall enforce time adjustment data write and delete access rules as following:

(Requirement 100):

The recording equipment shall record and store in its data memory data relevant to:

- the most recent time adjustment,
- the five largest time adjustments, since last calibration, performed in calibration mode outside the frame of a regular calibration (definition (f)).

Appendix 10, ACC_210:

The VU shall enforce appropriate read and write access rights to security data as the following security elements:

(Requirement 080):

The recording equipment shall be able to store the following security elements:

- European public key,
- Member State certificate,
- equipment certificate,
- equipment private key.

Recording equipment security elements are inserted in the equipment by the Vehicle Unit manufacturer.

CSP_204 If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.

##### *5.1.1.1.4 File structure and access conditions*

Appendix 10, ACC_211:

Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

##### *5.1.1.1.5 Update and Downloading*

The VU enables a software update of the MC or a download of user activities data to external storage media (incl. wireless remote downloading connection) if the corresponding authentication was successful.

The VU enables the deletion of all data (incl. Security data) if the corresponding authentication of the management device was successful.

#### 5.1.1.2 List of TOE Security Functional Requirements

This chapter contains all SFRs concerning the TOE. The SFRs for the TOE are listed within tables. Thereby, the tables contain in the left column the original definition of the respective SFR and its elements, dependencies, hierarchical information, management and audit functions. The right column supplies the iterations, selections, assignments and refinements chosen for the TOE.

For the SFRs of the TOE, the SFRs are numbered by taking the original name of the SFRs respective its elements and adding "/name" for the iteration(s).

#### *5.1.1.2.1 FAU Security Audit*

| **FAU**<br>**Security Audit** | |
|---|---|
| **FAU_GEN**<br>**Security Audit Data Generation** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.4 |
| **FAU_GEN.1**<br>**Audit Data Generation** | **FAU_GEN.1** |
| **FAU_GEN.1.1**<br>The TSF shall be able to generate an audit record of the following auditable events:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and<br>**c) [assignment: *other specifically defined auditable events*].**<br><br>**FAU_GEN.1.2**<br>The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]<br><br><u>Hierarchical to:</u><br>No other components | **FAU_GEN.1.1**<br>The TSF shall be able to generate an audit record of the following auditable events:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the **[not specified]** level of audit; and<br>c) [none].<br><br>**FAU_GEN.1.2**<br>The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[none]**<br><br>**Refinement**<br>AUD_201: The VU shall, for events impairing the security of the VU, record those events with associated data ([EU], Annex 1B (requirements 094, 096 and 109).<br>AUD_203: The VU shall enforce audit records storage rules [EU], Annex 1B (requirement 094 and 096).<br>AUD_204: The VU shall store audit records generated by the motion sensor in its data memory.<br>AUD_205:It shall be possible to print, display and download<br>audit records.<br><br>**Note**<br>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 event if relevant for security.<br><br><u>Hierarchical to:</u><br>No other components |

| | |
|---|---|
| Dependencies:<br>- FPT_STM.1 Reliable time stamps<br>Management:<br>There are no management activities foreseen.<br>Audit:<br>There are no auditable events foreseen. | Dependencies:<br>- FPT_STM.1 Reliable time stamps<br>Management:<br>Not applicable |
| **FAU_SAA**<br>**Security Audit Analysis** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic<br>Security Target, chapter 4.4 |
| **FAU_SAA.1**<br>**Potential Violation Analysis** | **FAU_SAA.1** |
| **FAU_SAA.1.1**<br>The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.<br>**FAU_SAA.1.2**<br>The TSF shall enforce the following rules for monitoring audited events:<br>a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;<br>b) [assignment: *any other rules*]. | **FAU_SAA.1.1**<br>The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.<br>**FAU_SAA.1.2**<br>The TSF shall enforce the following rules for monitoring audited events:<br>a) Accumulation or combination of<br>[<br>- **security breach attempts**<br>○ **motion sensor authentication failure,**<br>○ **tachograph card authentication failure,**<br>○ **unauthorized change of motion sensor,**<br>○ **card data input integrity error,**<br>○ **stored user data integrity error,**<br>○ **internal data transfer error,**<br>○ **unauthorised case opening,**<br>○ **hardware sabotage,**<br>- **last card session not correctly closed,**<br>- **motion data error event,**<br>- **power supply interruption event,**<br>- **VU internal fault.**<br>]<br>known to indicate a potential security violation;<br>b)<br>[<br>- **The VU shall, for events impairing the security of the VU, record those events with associated data ([EU], Annex 1B (requirements 094, 096 and 109).**<br>- **The VU shall enforce audit records storage rules [EU], Annex 1B (requirements 094 and 096).**<br>- **The VU shall store audit records generated by the motion sensor in its data memory.**<br>- **It shall be possible to print, display and download audit records.**<br>]. |

| | |
|---|---|
| Hierarchical to:<br>No other components<br>Dependencies:<br>- FAU_GEN.1 Audit data generation<br>Management:<br>a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules<br>Audit:<br>a) Minimal: Enabling and disabling of any of the analysis mechanisms<br>b) Minimal: Automated responses performed by the tool | **Note**<br>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 event if relevant for security.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FAU_GEN.1 Audit data generation<br>Management:<br>Not applicable |

#### *5.1.1.2.2 FCO Communication*

| **FCO**<br>**Communication** | |
|---|---|
| **FCO_NRO**<br>**Non-Repudiation of Origin** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic<br>Security Target, chapter 4.8.2 |
| **FCO_NRO.1**<br>**Selective Proof of Origin** | **FCO_NRO.1** |
| **FCO_NRO.1.1**<br>The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient, [assignment: list of third parties]*].<br>**FCO_NRO.1.2**<br>The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.<br>**FCO_NRO.1.3**<br>The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of origin*]. | **FCO_NRO.1.1**<br>The TSF shall be able to generate evidence of origin for transmitted [**user data (download function)**] at the request of the [**recipient**].<br>**Refinement**<br>DEX_206: The VU shall generate an evidence of origin for data downloaded to external media.<br>**FCO_NRO.1.2**<br>The TSF shall be able to relate the [**VU identity given by the VU specific private signature key**] of the originator of the information, and the [**hash value of the data area**] of the information to which the evidence applies.<br>**Refinement**<br>DEX_208: The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.<br>**FCO_NRO.1.3**<br>The TSF shall provide a capability to verify the evidence of origin of information to [**the recipient**] given [**no limitation**].<br>**Refinement**<br>DEX_207: The VU shall provide a capability to |

| | |
|---|---|
| Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UID.1 Timing of identification<br>Management:<br>a) The management of changes to information types, fields, originator attributes and recipients of evidence.<br>Audit:<br>a) Minimal: The identity of the user who requested that evidence of origin would be generated.<br>b) Minimal: The invocation of the non-repudiation service.<br>c) Basic: Identification of the information, the destination, and a copy of the evidence provided.<br>d) Detailed: The identity of the user who requested a verification of the evidence. | verify the evidence of origin of downloaded data to the recipient.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UID.1 Timing of identification<br>Management:<br>Not applicable |

#### *5.1.1.2.3 FCS Cryptograpic Support*

| **FCS**<br>**Cryptographic Support** | |
|---|---|
| **FCS_CKM**<br>**Cryptographic Key Management** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.9 |
| **FCS_CKM.1**<br>**Cryptographic Key Generation** | **FCS_CKM.1** |
| **FCS_CKM.1.1**<br>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. | **FCS_CKM.1.1**<br>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[generation of a 3-DES session key]** and specified cryptographic key sizes **[of double length (128 bits with 112 bits entropy, no parity bits set)]** that meets the following:<br>**[**<br>- **ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 3.1.3 (CSM_012), 3.2 (CSM_015) and 4 (CSM_020)**<br>- **ISO/DIS 16844-3 - Road vehicles — Tachograph systems — Part 3: Motion sensor interface**<br>**].** |

| | |
|---|---|
| Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.2 Cryptographic key distribution<br>- or<br>- FCS_COP.1 Cryptographic operation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys) | Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.2/Session_key Cryptographic key distribution]<br>- FCS_CKM.4 Cryptographic key destruction<br><br>Management:<br>Not applicable |
| **FCS_CKM.2**<br>**Cryptographic Key Distribution** | **FCS_CKM.2/Session_key** |
| **FCS_CKM.2.1**<br>The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or | **FCS_CKM.2.1/Session_key**<br>The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[3-DES session key agreement by an internal-external authentication mechanism]** that meets the following:<br>**[**<br>- **ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 3.1.3 (CSM_012) and 4 (CSM_020), Appendix 2, chapter 3.6.8 and 3.6.9**<br>- **ISO/DIS 16844-3 - Road vehicles — Tachograph systems — Part 3: Motion sensor interface**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction |

| | |
|---|---|
| FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys) | Management:<br>Not applicable |
| **FCS_CKM.2**<br>**Cryptographic Key Distribution** | **FCS_CKM.2/RSA_cert** |
| **FCS_CKM.2.1**<br>The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) | **FCS_CKM.2.1/RSA_cert**<br>The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[import respective export of public RSAkeys by certificates (verifiable certificates in conformance with ISO/IEC 9796-2 respective ISO/IEC 7816-8)]** that meets the following:<br>**[**<br>- **Tachograph specification [EU], Annex 1B, Appendix 11, chapter 3.3, esp. 3.3.1 (CSM_017), 3.3.2 (CSM_018) and 3.3.3 (CSM_019)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes]<br><br>Management:<br>**Not applicable** |

| | |
|---|---|
| <u>Audit:</u><br>a) Minimal: Success and failure of the activity<br>b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys) | |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/RSA_private_sig** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br><u>Hierarchical to:</u><br>No other components<br><u>Dependencies:</u><br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><u>Management:</u><br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><u>Audit:</u><br>a) Minimal: Success and failure of the activity<br>b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys) | **FCS_CKM.3.1/RSA_private_sig**<br>The TSF shall perform **[the access to a private RSAkey for the generation of a digital signature]** in accordance with a specified cryptographic key access method **[access to the key by its implicitly known reference before the execution of External Authenticate]** that meets the following:<br>**[**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 4 (CSM_020)**<br>**].**<br><u>Hierarchical to:</u><br>No other components<br><u>Dependencies:</u><br>Not applicable<br><u>Management:</u><br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/RSA_public_sig** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*]. | **FCS_CKM.3.1/RSA_public_sig**<br>The TSF shall perform **[the access to a public RSAkey for the verification of a digital signature]** in accordance with a specified cryptographic key access method **[access to the key by its reference explicitly set within the execution of tachograph card commands]** that |

| | |
|---|---|
| Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | meets the following:<br>**[**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 4 (CSM_020)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/RSA_private_enc** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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.3.1/RSA_private_enc**<br>The TSF shall perform **[the access to a private RSAkey for the encryption operation]** in accordance with a specified cryptographic key access method **[access to the key by its implicitly known reference before the execution of the command External Authenticate]** that meets the following:<br>**[**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 4 (CSM_020)**<br>**].**<br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable |

| | |
|---|---|
| - FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | Management:<br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/RSA_public_dec** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | **FCS_CKM.3.1/RSA_public_dec**<br>The TSF shall perform **[the access to a public RSAkey for the decryption operation]** in accordance with a specified cryptographic key access method **[access to the key by its reference explicitly set within the execution of the command Internal Authenticate]** that meets the following:<br>**[**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 4 (CSM_020)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |

| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/Session_key** |
|---|---|
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | **FCS_CKM.3.1/Session_key**<br>The TSF shall perform **[the access to a 3-DES session key for secure messaging: encryption, decryption, MAC generation and MAC verification operations]** in accordance with a specified cryptographic key access method **[access to the session key by its reference implicit set by the VU before the execution of commands, if Secure Messaging is required]** that meets the following:<br>**[**<br>- **- EU Tachograph Specification [EU], Annex 1B, Appendix 11,, chapter 5.1 (CSM_013)**<br>**].**<br><br>**Refinement**<br>CSP_301: (...) Generated cryptographic session keys shall have a limited (specified in the assurance class development by manufacturer and not more than 240) number of possible uses.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br><br>Management:<br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/Key_motion_sensor** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of* | **FCS_CKM.3.1/Key_motion_sensor**<br>The TSF shall **perform [the access to 3-DES keys for pairing, encryption and decryption operations]** in accordance with a specified cryptographic key access method **[access to the keys by its reference implicit set by the VU]** |

| | |
|---|---|
| *standards*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | that meets the following:<br>**[**<br>- **- ISO/DIS 16844-3 - Road vehicles — Tachograph systems — Part 3: Motion sensor interface**<br>**].**<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- [FCS_CKM.1-1 Cryptographic key generation]<br>- FCS_CKM.4-1 Cryptographic key destruction<br>Management:<br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/RSA_private_IDD** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br>Hierarchical to:<br>No other components | **FCS_CKM.3.1/RSA_private_IDD**<br>The TSF shall perform **[the access to a private RSAkey for the generation of a digital signature]** in accordance with a specified cryptographic key access method **[access to the key by its implicitly known reference before the execution of data download to the intelligent dedicated device]** that meets the following:<br>**[**<br>- **PKCS#1 (with SHA-1) encryption / decryption primitive, RSA Encryption Standard Version 2.0, October 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 7**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 6 (CSM_032), (CSM_033) and (CSM_034)**<br>**].**<br>Hierarchical to:<br>No other components |

| | |
|---|---|
| Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_CKM.3**<br>**Cryptographic Key Access** | **FCS_CKM.3/Ext_device** |
| **FCS_CKM.3.1**<br>The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or | **FCS_CKM.3.1/Ext_device**<br>The TSF shall perform **[the access to a 3-DES session key for encryption, decryption, MAC generation and MAC verification operations (for the verification of the identity of the external device[1])]** in accordance with a specified cryptographic key access method **[calculation of a session key based on secrets stored in TSF and external device and dynamic data portions provided by both components at connection time (mutual authentication mechanism).]** that meets the following:<br>**[**<br>**TDES** **National Institute of Standards and Technology (NIST). FIPS Publication 46-3: DataEncryption Standard, Draft 1999**<br>**TDES-OP** **ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, 1998**<br>**[EU]** **COMMISSION REGULATION (EC) No 1360/2002 Annex 1b**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable |

[1] Management device or remote company server (with connection to a Company Card)

| | |
|---|---|
| FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption)<br><br>Audit:<br>a) Minimal: Success and failure of the activity<br>**b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)** | Management:<br>Not applicable |
| **FCS_CKM.4**<br>**Cryptographic Key Destruction** | **FCS_CKM.4** |
| **FCS_CKM.4.1**<br>The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) | **FCS_CKM.4.1**<br>The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwrite session keys after usage with 0xff so that they cannot be restored]** that meets the following:<br>**[**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 3.1.3 (CSM_013)**<br>**].**<br><br>**Refinement**<br>CSP_205: If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1 Cryptographic key generation]<br><br>Management:<br>Not applicable |

| | |
|---|---|
| Audit:<br>a) Minimal: Success and failure of the activity<br>b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys) | |
| **FCS_COP**<br>**Cryptographic Operation** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.9 |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/RSA_card_cert** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes | **FCS_COP.1.1/RSA_card_cert**<br>The TSF shall perform **[the implicit signature verification when getting the card certificate]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[of 1024 bits]** that meet the following:<br>**[**<br>- **PKCS#1 (with SHA-1) signature generation / verification scheme, RSA Encryption Standard Version 2.0, October 1998**<br>- **SHA-1, FIPS Pub. 180-1, NIST, April 1995**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 4 (CSM_020)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/RSA_Signature** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a | **FCS_COP.1.1/RSA_Signature**<br>The TSF shall perform **[the implicit signature generation and verification (commands** |

| | |
|---|---|
| specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | **Internal Authenticate and External Authenticate)]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[of 1024 bits]** that meet the following:<br>**[**<br>- **ISO/IEC 9796-2 Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Mechanisms Using a Hash Function, First Edition 1997**<br>- **SHA-1, FIPS Pub. 180-1, NIST, April 1995**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 2.2.1 (CSM_003), 2.2.2 (CSM_004), 4 (CSM_020), 3.3.2 and 3.3.3**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/RSA_enc_dec** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. | **FCS_COP.1.1/RSA_enc_dec**<br>The TSF shall perform **[the implicit encryption and decryption operations concerning asymmetric cryptography (commands Internal Authenticate and External Authenticate)]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[of 1024 bits]** that meet the following:<br>**[**<br>- **PKCS#1 (with SHA-1) encryption / decryption primitive, RSA Encryption Standard Version 2.0, October 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 2.2.1** |

| | |
|---|---|
| Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | **(CSM_003) and 4**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/3-DES** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction | **FCS_COP.1.1/3-DES**<br>The TSF shall perform **[the encryption and decryption operations concerning symmetric cryptography]** in accordance with a specified cryptographic algorithm **[3-DES in CBC mode with ICV = 0]** and cryptographic key sizes **[of 128 bits (112 bits entropy, no parity bits set)]** that meet the following:<br>**[**<br>- **Data Encryption Standard, FIPS Pub. 46-3, NIST, Draft 1999**<br>- **ANSI9.52 Triple Data Encryption Algorithm Modes of Operations 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 2.2.3 (CSM_005) and 5.4 (CSM_031)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction |

| | |
|---|---|
| - FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/MAC** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | **FCS_COP.1.1/MAC**<br>The TSF shall perform **[the MAC generation and the MAC verification concerning symmetric cryptography]** in accordance with a specified cryptographic algorithm **[DES Retail-MAC (with consideration of the send sequence counter)]** and cryptographic key sizes **[of 128 bits (112 bits entropy, no parity bits set)]** that meet the following:<br>**[**<br>- **ANSI9.19 Financial Institution Retail Message Authentication 1986**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 2.2.3 (CSM_005) and 5.3 (CSM_028)**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1-1 Cryptographic key generation]<br>- FCS_CKM.4-1 Cryptographic key destruction<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/3-DES_motion_sensor** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of* | **FCS_COP.1.1/3-DES_motion_sensor**<br>The TSF shall perform **[cryptographic** |

| | |
|---|---|
| *cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | **operations like pairing, encryption, decryption, MAC generation and MAC verification]** in accordance with a specified cryptographic algorithm **[3-DES]** and cryptographic key **sizes [of 128 bits (112 bits entropy, no parity bits set)]** that meet the following:<br>**[**<br>- **ISO/DIS 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 3.1.3 (CSM_036) and (CSM_037)**<br>**].**<br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/RSA_IDD** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. | **FCS_COP.1.1/RSA_IDD**<br>The TSF shall perform **[an explicit signature generation on data to be downloaded from the VU to an intelligent dedicated equipment]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[of 1024 bits]** that meet the following:<br>**[**<br>- **PKCS#1 (with SHA-1) encryption / decryption primitive, RSA Encryption Standard Version 2.0, October 1998**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 7**<br>- **EU Tachograph Specification [EU], Annex 1B, Appendix 11, chapter 6 (CSM_032) (CSM_033) (CSM_034)**<br>**].** |

| | |
|---|---|
| Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [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]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable<br><br>Management:<br>Not applicable |
| **FCS_COP.1**<br>**Cryptographic Operation** | **FCS_COP.1/Ext_device** |
| **FCS_COP.1.1**<br>The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with | **FCS_COP.1.1/Ext_device**<br>The TSF shall perform **[the verification of the identity of the external device**[2]**, confidential exchange of sensitive data**] in accordance with a specified cryptographic algorithm **[TDES, SHA1, Retail MAC]** and cryptographic key sizes **[of 112 bits]** that meet the following:<br>**[**<br>**SHA-1** **National Institute of Standards and Technology (NIST). FIPSPublication 180-1: Secure Hash Standard, April 1995**<br>**TDES** **National Institute of Standards and Technology (NIST). FIPS Publication 46-3: DataEncryption Standard, Draft 1999**<br>**TDES-OP** **ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, 1998**<br>**[EU]** **COMMISSION REGULATION (EC) No 1360/2002 Annex 1b**<br>**].**<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>Not applicable |

[2] Management device or remote company server (with connection to a Company Card)

| | |
|---|---|
| security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>- FCS_CKM.4 Cryptographic key destruction<br>- FMT_MSA.2 Secure security attributes<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Minimal: Success and failure, and the type of cryptographic operation<br>**b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes** | Management:<br>Not applicable |

### 5.1.1.2.4 FDP User Data Protection

| **FDP<br>User Data Protection** | |
|---|---|
| **FDP_ACC<br>Access Control Policy** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.2 |
| **FDP_ACC.2<br>Complete Access Control** | **FDP_ACC.2** |
| **FDP_ACC.2.1**<br>The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.<br><br>**FDP_ACC.2.2**<br>The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. | **FDP_ACC.2.1**<br>The TSF shall enforce the **[AC_SFP]** on<br>**[**<br>**subjects:**<br>- **user,**<br>- **tachograph card,**<br>- **motion sensor,**<br>- **calibration equipment,**<br>- **local downloading equipment,**<br>- **remote company server,**<br>- **management device (security server)**<br>**objects:**<br>- **TOE security data**<br>- **TOE identification data**<br>- **calibration parameters**<br>- **TimeDate**<br>- **HighResolutionTotalVehicleDistance**<br>- **configuration data**<br>- **stored user data**<br>- **TOE software code**<br>**]**<br>and all operations among subjects and objects covered by the SFP.<br><br>**FDP_ACC.2.2**<br>The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.<br><br>**Refinements**<br>ACR_201: The VU shall ensure that user data |

| | |
|---|---|
| Hierarchical to:<br>FDP_ACC.1<br><br>Dependencies:<br>- FDP_ACF.1 Security attribute based access control<br><br>Management:<br>Not applicable<br><br>Audit:<br>Not applicable | related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:<br>- vehicle motion data,<br>- VU's real time clock,<br>- recording equipment calibration parameters,<br>- tachograph cards,<br>- user's inputs.<br>ACR_201a: The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal current insertion (requirement 050a).<br><br>Hierarchical to:<br>FDP_ACC.1<br><br>Dependencies:<br>- FDP_ACF.1 Security attribute based access control<br><br>Management:<br>Not applicable |
| **FDP_ACF**<br>**Access Control Functions** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.2 |
| **FDP_ACF.1**<br>**Security Attribute Based Access Control** | **FDP_ACF.1** |
| **FDP_ACF.1.1**<br>The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].<br><br>**FDP_ACF.1.2**<br>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. | **FDP_ACF.1.1**<br>The TSF shall enforce the **[AC_SFP]** to objects based on the following: **[as defined in the security functional policy AC_SFP**].<br><br>**FDP_ACF.1.2**<br>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[AC_SFP].**<br><br>**Refinements**<br>ACT_201: The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).<br><br>ACT_202: The VU shall hold permanent identification data (requirement 075).<br><br>ACT_203: The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).<br><br>ACT_204: The VU shall ensure that controllers are accountable for their activities (requirements |

| | |
|---|---|
| | 102, 103 and 109).<br>ACT_205: The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).<br>ACT_206: The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.<br>ACT_207: The VU shall ensure that it does not modify data already stored in a **tachograph card** (requirements 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1 Note. |
| **FDP_ACF.1.3**<br>The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. | **FDP_ACF.1.3**<br>The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**In case of data download via another connector than the calibration/ downloading connector, company mode data access rights shall apply to this download**]. |
| **FDP_ACF.1.4**<br>The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FDP_ACC.1 Subset access control<br>- FMT_MSA.3 Static attribute initialisation<br>Management:<br>a) Managing the attributes used to make explicit access or denial based decisions<br>Audit:<br>a) Minimal: Successful requests to perform an operation on an object covered by the SFP<br>b) Basic: All requests to perform an operation on an object covered by the SFP<br>c) Detailed: The specific security attributes used in making an access check | **FDP_ACF.1.4**<br>The TSF shall explicitly deny access of subjects to objects based on the **[none]**.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FDP_ACC.1 Subset access control<br>Management:<br>Not applicable |
| **FDP_ITC**<br>**Import from Outside TSF Control** | |
| **FDP_ITC.1**<br>**Import of User Data without Security Attributes** | **FDP_ITC.1** |

| | |
|---|---|
| **FDP_ITC.1.1**<br>The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.<br><br>**FDP_ITC.1.2**<br>The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.<br><br>**FDP_ITC.1.3**<br>The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]<br>- FMT_MSA.3 Static attribute initialisation<br><br>Management:<br>a) The modification of the additional control rules used for import<br><br>Audit:<br>a) Minimal: Successful import of user data, including any security attributes<br>b) Basic: All attempts to import user data, including any security attributes<br>c) Detailed: The specification of security attributes for imported user data supplied by an authorised user | **FDP_ITC.1.1**<br>The TSF shall enforce the **[AC_SFP]** when importing user data, controlled under the SFP, from outside of the TSC.<br><br>**FDP_ITC.1.2**<br>The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.<br><br>**FDP_ITC.1.3**<br>The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[none]**.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- [FDP_ACC.2 Subset access control]<br><br>Management:<br>Not applicable |
| **FDP_RIP**<br>**Residual Information Protection** | |
| **FDP_RIP.1**<br>**Subset Residual Information Protection** | **FDP_RIP.1** |
| **FDP_RIP.1.1**<br>The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].<br><br>Hierarchical to:<br>No other components | **FDP_RIP.1.1**<br>The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[allocation of the resource to]** the following objects: **[security relevant data (as secret or private keys) stored in the SC].**<br><br>**Refinement**<br>REU_201: The VU shall ensure that temporary storage objects can be re-used without this involving inadmissible information flow.<br><br>Hierarchical to:<br>No other components |

| | |
|---|---|
| Dependencies:<br>No dependencies<br>Management:<br>a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE<br>Audit:<br>Not applicable | Dependencies:<br>No dependencies<br>Management:<br>Not applicable |
| **FDP_SDI**<br>**Stored Data Integrity** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.6.3 |
| **FDP_SDI.2**<br>**Stored Data Integrity Monitoring and Action** | **FDP_SDI.2** |
| **FDP_SDI.2.1**<br>The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].<br>**FDP_SDI.2.2**<br>Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].<br>Hierarchical to:<br>FDP_SDI.1<br>Dependencies:<br>No dependencies<br>Management:<br>a) The actions to be taken upon the detection of an integrity error could be configurable<br>Audit:<br>a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check<br>b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed<br>c) Detailed: The type of integrity error that occurred<br>d) Detailed: The action taken upon detection of an integrity error | **FDP_SDI.2.1**<br>The TSF shall monitor user data stored within the TSC for **[integrity errors]** on all objects, based on the following attributes: **[stored user data]**.<br>**FDP_SDI.2.2**<br>Upon detection of a (stored user) data integrity error, the TSF shall **[generate an audit record]**.<br>Hierarchical to:<br>FDP_SDI.1<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |

#### *5.1.1.2.5 FIA Identification & Authentication*

| | |
|---|---|
| **FIA**<br>**Identification & Authentication** | |
| **FIA_AFL**<br>**Authentication Failures** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.1.1, 4.1.2, 4.1.3 |
| **FIA_AFL.1** | **FIA_AFL.1/Motion_sensor** |

| **Authentication Failure Handling** | |
|---|---|
| **FIA_AFL.1.1**<br>The TSF shall detect when [selection: [assignment: *positive integer number*], *"an administrator configurable positive integer within [assignment: range of acceptable values*]"] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].<br><br>**FIA_AFL.1.2**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br><br>Management:<br>a) management of the threshold for unsuccessful authentication attempts<br>b) management of actions to be taken in the event of an authentication failure<br><br>Audit:<br>a) Minimal: the reaching of the threshold for the unsuccesful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal) | **FIA_AFL.1.1/Motion_sensor**<br>The TSF shall detect when **[the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment and/or 10 consecutive]** unsuccessful authentication attempt occurs related to **[motion sensor identification and authentication].**<br><br>**FIA_AFL.1.2/Motion_sensor**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[generate an audit record of the event, warn the user, continue to accept and use non secured motion data sent by the motion sensor]**.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br><br>Management:<br>Not applicable |
| **FIA_AFL.1**<br>**Authentication Failure Handling** | **FIA_AFL.1/Card** |
| **FIA_AFL.1.1**<br>The TSF shall detect when [selection: [assignment: *positive integer number*], *"an administrator configurable positive integer within [assignment: range of acceptable values*]"] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].<br><br>**FIA_AFL.1.2**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*]. | **FIA_AFL.1.1/Card**<br>The TSF shall detect when **[5 consecutive]** unsuccessful authentication attempt occurs related to **[user identification and authentication].**<br><br>**FIA_AFL.1.2/Card**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[generate an audit record of the event, warn the user, assume the user as UNKNOWN, and the card as non valid (see [EU], Annex 1B (requirement 007)].**<br><br>**Note**<br>Non valid card means:<br>- a card detected as faulty, or |

| | |
|---|---|
| Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br>Management:<br>a) management of the threshold for unsuccessful authentication attempts<br>b) management of actions to be taken in the event of an authentication failure<br>Audit:<br>a) Minimal: the reaching of the threshold for the unsuccesful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal) | - which initial authentication failed, or<br>- which start of validity date is not yet reached, or<br>- which expiry date has passed.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br>Management:<br>Not applicable |
| **FIA_AFL.1**<br>**Authentication Failure Handling** | **FIA_AFL.1/Company** |
| **FIA_AFL.1.1**<br>The TSF shall detect when [selection: [assignment: *positive integer number*], *"an administrator configurable positive integer within [assignment: range of acceptable values*]"] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].<br>**FIA_AFL.1.2**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br>Management:<br>a) management of the threshold for unsuccessful authentication attempts<br>b) management of actions to be taken in the event of an authentication failure<br>Audit:<br>a) Minimal: the reaching of the threshold for the unsuccesful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the | **FIA_AFL.1.1/Company**<br>The TSF shall detect when **[5 consecutive]** unsuccessful authentication attempt occurs related to **[company identification and authentication].**<br>**FIA_AFL.1.2/Company**<br>When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[warn the remotely connected company].**<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UAU.1 Timing of authentication<br>Management:<br>Not applicable |

| | |
|---|---|
| normal state (e.g. re-enabling of a terminal) | |
| **FIA_UAU**<br>**User Authentication** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.1.1, 4.1.2, 4.1.3, 4.1.4 |
| **FIA_UAU.1**<br>**Timing of Authentication** | **FIA_UAU.1** |
| **FIA_UAU.1.1**<br>The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.<br>**FIA_UAU.1.2**<br>The TSF shall require each user to be successfully authenticated before allowing any other TSF- mediated actions on behalf of that user.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UID.1 Timing of identification<br>Management:<br>a) management of the authentication data by an administrator<br>b) management of the authentication data by the associated user<br>c) managing the list of actions that can be taken before the user is authenticated<br>Audit: | **FIA_UAU.1.1**<br>The TSF shall allow **[none of the TSF-mediated actions]** on behalf of the user to be performed before the user is authenticated.<br>**FIA_UAU.1.2**<br>The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.<br>**Refinements**<br>UIA_209: The VU shall authenticate its users at card insertion.<br>UIA_211: Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.<br>UIA_212: Workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long. In case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.<br>UIA_217: The VU shall successfully authenticate the remotely connected company before allowing any data export to it.<br>UIA_218: Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>- FIA_UID.1 Timing of identification<br>Management:<br>Not applicable |

| | |
|---|---|
| a) Minimal: Unsuccessful use of the authentication mechanism<br>b) Basic: All use of the authentication mechanism<br>c) Detailed: All TSF mediated actions performed before authentication of the user | |
| **FIA_UAU.3**<br>**Unforgeable Authentication** | **FIA_UAU.3** |
| **FIA_UAU.3.1**<br>The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.<br>**FIA_UAU.3.2**<br>The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable<br>Audit:<br>a) Minimal: Detection of fraudulent authentication data<br>b) Basic: All immediate measures taken and results of checks on the fraudulent data | **FIA_UAU.3.1**<br>The TSF shall **[detect and prevent]** use of authentication data that has been forged by any user of the TSF.<br>**FIA_UAU.3.2**<br>The TSF shall **[detect and prevent]** use of authentication data that has been copied from any other user of the TSF.<br>**Note**<br>Forged authentication data includes replayed authentication data.<br>This SFR is valid for all identification and authentication, i.e. Motion sensor identification and authentication, user identification and authentication and external device identification and authentication.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |
| **FIA_UAU.6**<br>**Re-authenticating** | **FIA_UAU.6** |
| **FIA_UAU.6.1**<br>The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management: | **FIA_UAU.6.1**<br>The TSF shall re-authenticate the user under the conditions **[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]**.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management: |

| | |
|---|---|
| a) If an authorised administrator could request reauthentication, the management includes a reauthentication request.<br><br>Audit:<br>a) Minimal: Failure of reauthentication;<br>b) Basic: All reauthentication attempts. | not applicable |
| **FIA_UID**<br>**User Identification** | **[EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.1.1, 4.1.2, 4.1.3, 4.1.4** |
| **FIA_UID.1**<br>**Timing of Identification** | **FIA_UID.1** |
| **FIA_UID.1.1**<br>The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.<br><br>**FIA_UID.1.2**<br>The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>No dependencies | **FIA_UID.1.1**<br>The TSF shall allow **[none of the TSF-mediated actions]** on behalf of the user to be performed before the user is identified.<br><br>**FIA_UID.1.2**<br>The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.<br><br>**Refinements**<br>UIA_207: The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.<br><br>UIA_208: The user identity shall consist of:<br>- a user group:<br>o DRIVER (driver card),<br>o CONTROLLER (control card),<br>o WORKSHOP (workshop card),<br>o COMPANY (company card),<br>o UNKNOWN (no card inserted),<br>- a user ID, composed of:<br>o the card issuing Member State code and of the card number,<br>o UNKNOWN if user group is UNKNOWN.<br>UNKNOWN identities may be implicitly or explicitly be known.<br><br>UIA_215: For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.<br><br>UIA_216: The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>No dependencies |

| | |
|---|---|
| Management:<br>a) the management of the user identities<br>b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists<br><br>Audit:<br>a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided<br>b) Basic: All use of the user identification mechanism, including the user identity provided | Management:<br>Not applicable |

#### *5.1.1.2.6 FPT Protection of TOE Security Functions*

| **FPT**<br>**Protection of TOE Security Functions** | |
|---|---|
| **FPT_FLS**<br>**Fail Secure** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.7.4, 4.7.5 |
| **FPT_FLS.1**<br>**Failure with Preservation of Secure State** | **FPT_FLS.1** |
| **FPT_FLS.1.1**<br>The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF].<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- ADV_SPM.1 Informal TOE security policy model<br><br>Management:<br>Not applicable<br><br>Audit:<br>a) Basic: Failure of the TSF | **FPT_FLS.1.1**<br>The TSF shall preserve a secure state when the following types of failures occur: **[Detection of deviations from specified values of the power supply, including cut-off]**.<br><br>**Refinements**<br>RLB_210: In the case described above, the TSF shall - generate an audit record (except in calibration mode),<br>- preserve the secure state of the VU,<br>- maintain the security functions, related to components or processes still operational,<br>- preserve the stored data integrity.<br><br>RLB_211: In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, the VU shall be reset clearly.<br><br>Hierarchical to:<br>No other components<br><br>Dependencies:<br>- ADV_SPM.1 Informal TOE security policy model<br>-<br>Management:<br>Not applicable |
| **FPT_ITA**<br>**Availability of exported TSF data** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.7.6 |

| | |
|---|---|
| **FPT_ITA.1**<br>**Inter-TSF availability within a defined availability metric** | **FPT_ITA.1** |
| **FPT_ITA.1.1**<br>The TSF shall ensure the availability of [assignment: *list of types of TSF data*] provided to a remote trusted IT product within [assignment: *a defined availability metric*] given the following conditions [assignment: *conditions to ensure availability*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies.<br>Management:<br>management of the list of types of TSF data that must be available to a remote trusted IT product.<br>Audit:<br>Minimal: the absence of TSF data when required by a TOE. | **FPT_ITA.1.1**<br>The TSF shall ensure the availability of **[data according to the following refinements]** provided to a remote trusted IT product within **[the metric as specified in the refinements]** given the following conditions **[according to the following refinements]**.<br>**Refinements**<br>RLB_212: The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.<br>RLB_213: The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015) and (requirement 016) of [EU], Annex 1B.<br>RLB_214: In the case described above, the TSF shall generate an audit record of the event.<br>**Note**<br>Requirements 015: The recording equipment shall be so designed that the tachograph cards are locked in position on their proper insertion into the card interface devices.<br>Requirement 016: 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.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>Not applicable<br>Management:<br>Not applicable |
| **FPT_PHP**<br>**Physical Protection** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.7.3 |
| **FPT_PHP.1**<br>**Passive detection of physical attack** | **FPT_PHP.1** |
| **FPT_PHP.1.1**<br>The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. | **FPT_PHP.1.1**<br>The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. |

| | |
|---|---|
| **FPT_PHP.1.2**<br>The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.<br><br>Hierarchical to:<br>No other components.<br><br>Dependencies:<br>No dependencies<br><br>Audit:<br>Minimal: if detection by IT means, detection of intrusion. | **FPT_PHP.1.2**<br>The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.<br><br>**Refinements**<br>RLB_206: [..] The VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection). The VU shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).<br><br>RLB_207: After its activation, the VU shall detect specified (specified in the assurance class development by manufacturer) hardware sabotage.<br><br>RLB_208: In the case described above, the TSF shall generate an audit record and the VU shall: (specified in the assurance class development by manufacturer).<br><br>Hierarchical to:<br>No other components.<br><br>Dependencies:<br>No dependencies |
| **FPT_SEP**<br>**Domain Separation** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.7.2 |
| **FPT_SEP.1**<br>**TSF Domain Separation** | **FPT_SEP.1** |
| **FPT_SEP.1.1**<br>The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.<br><br>**FPT_SEP.1.2**<br>The TSF shall enforce separation between the security domains of subjects in the TSC. | **FPT_SEP.1.1**<br>The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.<br><br>**FPT_SEP.1.2**<br>The TSF shall enforce separation between the security domains of subjects in the TSC.<br><br>**Refinements**<br>RLB_204: There shall be no way to analyse, debug or modify TOE's software in the field after the VU activation.<br><br>RLB_205: Inputs from external sources shall not be accepted as executable code.<br><br>RLB_215: If the VU provides applications to other than the Tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active |

| | |
|---|---|
| Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable<br>Audit:<br>Not applicable | at a time.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |
| **FPT_STM**<br>**Time Stamps** | |
| **FPT_STM.1**<br>**Reliable Time Stamps** | **FPT_STM.1** |
| **FPT_STM.1.1**<br>The TSF shall be able to provide reliable time stamps for its own use.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies.<br>Management:<br>The following actions could be considered for the management functions in FMT:<br>a) management of the time.<br>Audit:<br>The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP / ST:<br>a) Minimal: changes to the time;<br>b) Detailed: providing a timestamp. | **FPT_STM.1.1**<br>The TSF shall be able to provide reliable time stamps for its own use.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |
| **FPT_TST**<br>**TSF Self Test** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.7.1 |
| **FPT_TST.1**<br>**TSF Testing** | **FPT_TST.1** |
| **FPT_TST.1.1**<br>The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur*] to demonstrate the correct operation of the [selection: *[assignment: parts of TSF], the TSF*]. | **FPT_TST.1.1**<br>The TSF shall run a suite of self tests **[during initial start-up and during normal operation]** to demonstrate the correct operation of the **[parts of TSF]**.<br>**Refinements**<br>RLB_201: All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. It shall not be possible to restore them for later use.<br>RLB_202: The VU self tests shall include a |

| | |
|---|---|
| | verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).<br>RLB_203: Upon detection of an internal fault during self test, the TSF shall generate an audit record (except in calibration mode) (VU internal fault), preserve the data integrity. |
| **FPT_TST.1.2**<br>The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*]. | **FPT_TST.1.2**<br>The TSF shall provide authorised users with the capability to verify the integrity of **[TSF data]**.<br>**Refinement**The software itself is understood as „authorised user“. |
| **FPT_TST.1.3**<br>The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. | **FPT_TST.1.3**<br>The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.<br>**Refinement**<br>The integrity check over the executable code stored outside the ROM area is covered by FPT_TST.1.1 and the related refinement. |
| Hierarchical to:<br>No other components<br>Dependencies:<br>- FPT_AMT.1 Abstract machine testing<br>Management:<br>a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions<br>b) management of the time interval if appropriate<br>Audit:<br>a) Basic: Execution of the TSF self tests and the results of the tests | Hierarchical to:<br>No other components<br>Dependencies:<br>Not applicable<br>Management:<br>Not applicable |

#### *5.1.1.2.7 FTP Trusted Path / Channels*

| **FTP**<br>**Trusted Path/Channels** | |
|---|---|
| **FTP_ITC**<br>**Inter-TSF Trusted Channel** | [EU], Annex 1B, Appendix 10, Vehicle Unit Generic Security Target, chapter 4.8.1, 4.8.2 |
| **FTP_ITC.1**<br>**Inter-TSF Trusted Channel** | **FTP_ITC.1/Motion_sensor** |
| **FTP_ITC.1.1**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication | **FTP_ITC.1.1/Motion_sensor**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product **(motion sensor)** that is logically distinct from |

| | |
|---|---|
| channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. | other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.<br>**Refinements**<br>UIA_201: The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.<br>UIA_202: The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.<br>UIA_203: The VU shall authenticate the motion sensor it is connected to:<br>- at motion sensor connection,<br>- at each calibration of the recording equipment,<br>- at power supply recovery.<br>Authentication shall be mutual and triggered by the VU.<br>UIA_204: The VU shall periodically (period specified in the assurance class development by manufacturer and more frequently than once per hour) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.<br>DEX_201: The VU shall verify the integrity and authenticity of motion data imported from the motion sensor<br>DEX_202: Upon detection of a motion data integrity or authenticity error, the SEF shall:<br>- generate an audit record,<br>- continue to use imported data. |
| **FTP_ITC.1.2**<br>The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. | **FTP_ITC.1.2/Motion_sensor**<br>The TSF shall permit **[the TSF]** to initiate communication via the trusted channel. |
| **FTP_ITC.1.3**<br>The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. | **FTP_ITC.1.3/Motion_sensor**<br>The TSF shall initiate communication via the trusted channel for **[data import from motion sensor, data export to motion sensor]**. |
| Hierarchical to:<br>No other components | Hierarchical to:<br>No other components |
| Dependencies:<br>No dependencies | Dependencies:<br>No dependencies |
| Management:<br>a) Configuring the actions that require trusted | Management:<br>Not applicable |

| | |
|---|---|
| channel, if supported<br>Audit:<br>a) Minimal: Failure of the trusted channel functions<br>b) Minimal: Identification of the initiator and target of failed trusted channel functions<br>c) Basic: All attempted uses of the trusted channel functions<br>d) Basic: Identification of the initiator and target of all trusted channel functions | |
| **FTP_ITC.1**<br>**Inter-TSF Trusted Channel** | **FTP_ITC.1/Card** |
| **FTP_ITC.1.1**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product 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.<br>**FTP_ITC.1.2**<br>The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.<br>**FTP_ITC.1.3**<br>The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>a) Configuring the actions that require trusted channel, if supported | **FTP_ITC.1.1/Card**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product **(tachograph card)** that is logically distinct from other com munication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.<br>**Refinements**<br>DEX_203: The VU shall verify the integrity and authenticity of data imported from **tachograph card**s.<br>DEX_204: Upon detection of card data integrity or authenticity error, the VU shall:<br>- generate an audit record,<br>- not use the data.<br>DEX_205: The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.<br>**FTP_ITC.1.2/Card**<br>The TSF shall permit **[the TSF]** to initiate communication via the trusted channel.<br>**FTP_ITC.1.3/Card**<br>The TSF shall initiate communication via the trusted channel for **[data import from tachograph card, data export to tachograph card]**.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |

| | |
|---|---|
| Audit:<br>a) Minimal: Failure of the trusted channel functions<br>b) Minimal: Identification of the initiator and target of failed trusted channel functions<br>c) Basic: All attempted uses of the trusted channel functions<br>**d) Basic: Identification of the initiator and target of all trusted channel functions** | |
| **FTP_ITC.1**<br>**Inter-TSF Trusted Channel** | **FTP_ITC.1/Ext_device** |
| **FTP_ITC.1.1**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product 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.<br>**FTP_ITC.1.2**<br>The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.<br>**FTP_ITC.1.3**<br>The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>a) Configuring the actions that require trusted channel, if supported<br>Audit:<br>a) Minimal: Failure of the trusted channel functions<br>b) Minimal: Identification of the initiator and target of failed trusted channel functions<br>c) Basic: All attempted uses of the trusted channel functions<br>**d) Basic: Identification of the initiator and** | **FTP_ITC.1.1/Ext_device**<br>The TSF shall provide a communication channel between itself and a remote trusted IT product **(external device)** 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.<br>**Refinements**<br>UIA_221: For every interaction with a management device, the VU shall be able to establish the device identity<br>UIA_222: Before allowing any further interaction, the VU shall successfully authenticate the management device.<br>**FTP_ITC.1.2/Ext_device**<br>The TSF shall permit **[the remote trusted IT product (external device)]** to initiate communication via the trusted channel.<br>**FTP_ITC.1.3/Ext_device**<br>The TSF shall initiate communication via the trusted channel for **[data download]**.<br>Hierarchical to:<br>No other components<br>Dependencies:<br>No dependencies<br>Management:<br>Not applicable |

| target of all trusted channel functions | |
|---|---|

### 5.1.2 SOF Claim for TOE Security Functional Requirements

The required level for the Strength of Function of the TOE security functional requirements listed in the preceding chapter 5.1.1.2 is “SOF-high” according to the requirements in the Tachograph specification [EU], main body and Appendix 10 (Vehicle Unit Generic Security Target), and to the JIL interpretations [JIL]. This complies to the claimed assurance level with its augmentation by the assurance component AVA_VLA.4 (see chapter 5.1.3).

### 5.1.3 TOE Security Assurance Requirements

The evaluation of the Vehicle Unit according to ITSEC E3 high as required in the Tachograph Specification [EU], Appendix 10 (Vehicle Unit Generic Security Target) will be replaced by a comparable evaluation according to Common Criteria, whereby the requirements in the JIL interpretations [JIL], Annex A have to be considered. The TOE security assurance level is fixed as

**EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4,**

and therefore the CC evaluation of the TOE meets the evaluation assurance requirements stated in the Tachograph Specification [EU], Appendix 10 (Vehicle Unit Generic Security Target).

The following table lists the security assurance requirements (SARs) for the TOE:

| **SAR** | | |
|---|---|---|
| Class ACM<br>Configuration Management | ACM_AUT.1<br>ACM_CAP.4<br>ACM_SCP.2 | Partial CM Automation<br>Generation Support and Acceptance Procedures<br>Problem Tracking CM Coverage |
| Class ADO<br>Delivery and Operation | ADO_DEL.2<br>ADO_IGS.2 | Detection of Modification<br>Generation Log |
| Class ADV<br>Development | ADV_FSP.2<br>ADV_HLD.2<br>ADV_IMP.2<br>ADV_LLD.1<br>ADV_RCR.1<br>ADV_SPM.1 | Fully Defined External Interfaces<br>Security Enforcing High-Level Design<br>Implementation of the TSF<br>Descriptive Low-Level Design<br>Informal Correspondence Demonstration<br>Informal TOE Security Policy Model |
| Class AGD<br>Guidance Documents | AGD_ADM.1<br>AGD_USR.1 | Administrator Guidance<br>User Guidance |
| Class ALC<br>Life Cycle Support | ALC_DVS.1<br>ALC_LCD.1<br>ALC_TAT.1 | Identification of Security Measures<br>Developer Defined Life-Cycle Model<br>Well-defined Development Tools |
| Class ATE<br>Tests | ATE_COV.2<br>ATE_DPT.2<br>ATE_FUN.1<br>ATE_IND.2 | Analysis of Coverage<br>Testing: Low-Level Design<br>Functional Testing<br>Independent Testing - Sample |
| Class AVA<br>Vulnerability Assessment | AVA_MSU.2<br>AVA_SOF.1<br>AVA_VLA.4 | Validation of Analysis<br>Strength of TOE Security Function Evaluation<br>Highly Resistant |

### 5.1.4 Refinements of the TOE Security Assurance Requirements

All assurance components given in the table of chapter 5.1.3 are used as defined in Common Criteria Part 3 [CC3] and CEM [CM]. Additionally, the following refinements respective interpretations are taken into account according to JIL Digital Tachograph [JIL], Annex A.3, Note 2 and 9:

**ADO_IGS.2**

ADO_IGS.2 is interpreted respective refined according to ITSEC E3.32 and ITSEC-JIL, Section 16.2 as follows:

- The term “generation” is always interpreted as “installation”.
- "While installing the TOE, any configuration options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how the TOE was initially configured and when the TOE was installed."

**AVA_MSU.2**

ITSEC 3.33 additionally requires evaluator tests where necessary. This testing, can be part of the penetration testing under AVA_VLA. It is decided on a case by case basis if the evaluator performs misuse-testing as additional part of penetration testing to confirm or disprove the misuse analysis. Specifically, if high attack potential is assumed, such independent misuse-testing is performed.

## 5.2 Security Requirements for the Environment of the TOE

### 5.2.1 Security Requirements for the IT-Environment

There are no security requirements for the IT-Environment of the TOE defined.

### 5.2.2 Security Requirements for the Non-IT-Environment

There are no security requirements for the Non-IT-Environment of the TOE defined.

# 6 TOE Summary Specification

## 6.1 TOE Security Functions

For the definition of the TOE Security Functions (TSF) related to the SC refer to the Security Target [ATMEL_ST], chap. 6.1. All Security Functions of the SC are relevant for the EFAS-3. The following section gives a survey of the TSFs of the TOE under consideration of the requirements in the Tachograph specification [EU], main body and Appendix 10 (Vehicle Unit Generic Security Target).

### 6.1.1 Access Control

**F.ACS Security Attribute Based Access Control**

The TSF enforces the SFP Access Control (AC_SFP) as defined in chapter 5.1.1.1.

Additionally the TSF ensures that access to resources is obtained when required and that resources are not requested nor retained unnecessarily. The TSF ensures that cards cannot be released before relevant data have been stored to them:

- The recording equipment is so designed 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.

In the case described above, the TSF shall generate an audit record of the event.

The TSF ensures that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 ([EU], Annex 1B) may only be processed from the right input sources:

- vehicle motion data,
- VU's real time clock,

- recording equipment calibration parameters,
- tachograph cards,
- user's inputs.

The TSF ensures that user data related to requirement 109a ([EU], Annex 1B) may only be entered for the period last card withdrawal — current insertion (requirement 050a).

There is no way to analyse, debug or modify TOE's software in the field after the EFAS-3 activation. Inputs from external sources are not accepted as executable code. Software update of the MC is only possible after the corresponding authentication. EFAS-3 provides no application other than the tachograph application. Therefore the requirements in [EU] RLB_215 about application separation are not applicable.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which is used for authentication before any access is possible and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### 6.1.2 Security Audit

**F.SECAUDIT Audit**

The TSF generates an audit record inter alia of the following auditable events: start-up and shutdown of the audit functions. 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 the TSF records within each audit record at least the information date and time of the begin and end of the event and the type of event.

The TSF, for events impairing the security of the EFAS-3, records those events with associated data ([EU], Annex 1B (requirements 094, 096 and 109). The TSF enforces audit records storage rules [EU], Annex 1B (requirement 094) and (requirement 096). The TSF stores audit records generated by the motion sensor in its data memory. The TSF makes it possible to print, display and download audit records.

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

The TSF 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,
  - unauthorised case opening,
  - hardware sabotage,
- last card session not correctly closed,
- motion data error event,
- power supply interruption event,
- EFAS-3 internal fault.

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 event if relevant for security.

The TSF is also able to provide reliable **time stamps** for its own use.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which is used for authentication and together with SF5 (Data Error Detection) for integrity checks as well as the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### 6.1.3 Identification and Authentication

**F.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-3 shall authenticate the motion sensor it is connected to:

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

Authentication shall be mutual and triggered by the EFAS-3. I.e. the TOE itself is authenticated with regard to the motion sensor as well by means of challenge-response procedure.

b) **User identification and authentication via tachograph card:**
The EFAS-3 shall authenticate its users at card insertion. Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute.

Authentication shall be mutual and triggered by the EFAS-3. I.e. the TOE itself is authenticated with regard to the tachograph card as well by means of challenge-response procedure.

Note: The external authentication of the EFAS-3 corresponds to the internal authentication of the tachograph card and vice versa.

c) **External device[3] identification and authentication:**
Before allowing any further interaction, the EFAS-3 shall successfully authenticate the external device. Authentication shall be mutual. I.e. the TOE itself is authenticated with regard to the external device as well by means of challenge-response procedure.

Cryptography:

In the cases

a) the TSF makes use of symmetric cryptography according to ISO/DIS 16844-3,

b) the TSF makes use of asymmetric cryptography according to ISO 9796-2 and with hash algorithm SHA-1 and

c) the TSF 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-3 and the external device.

Cryptographic Protocol:

In the case a):

[3] Management device or remote company server (with connection to a Company Card)

The TSF operates the **initial identification and authentication** as described in chapter 7.4 of ISO/DIS 16844-3.

The extended serial-number of the motion sensor is sent to the EFAS-3. The EFAS-3 encrypts the extended serial number of the motion sensor, using the “identification key”. The motion sensor transmits a pairing key which is encrypted with the “master key” to the EFAS-3.

The “session key” is transmitted from the EFAS-3 to the motion sensor encrypted with the “pairing key”. Pairing information is transmitted from the EFAS-3 to the motion sensor encrypted with the “pairing key”.

The initial identification and authentication leads to a generation of the “session key” which secure based on a challenge response mechanism the following communication between the EFAS-3 and the motion sensor.

In the case b):

The TSF 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-3”, “Decryption” and “Verification of a digital signature” for the external authentication.

The private key necessary on the EFAS-3´s side for authentication purposes is stored on the EFAS-3 and is implicitly connected with the corresponding commands. The access to the keys is controlled by the SFP Access Control (AC_SFP) as defined in chapter 5.1.1.1, which is realised by the TSF F.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 send sequence counter) which will be used for securing the following data transfer. The generation of session keys is task of the TSF F.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-3 only transfers the PIN from the keypad to the Workshop Card this not a TSF of EFAS-3.

Case c):

The TSF operates using a challenge response protocol with TDES-cryptographic mechanisms with calculation of a session key based on secrets stored in TSF and external device and 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 authorised (i.e. while not during a calibration of the recording equipment), the TSF

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

Case b):

After 5 consecutive unsuccessful authentication attempts have been detected, the TSF:

- generates an audit record of the event,
- warns the user,
- assumes the user as UNKNOWN, and the card as non valid.

Case c)

In case of unsuccessful authentification the user will be informed.

Re-authentication and re-identification:

Case a):

The TSF periodically (period specified in the assurance class development by manufacturer and more frequently than once per hour) re-identifies and reauthenticates the motion sensor it is connected to, and ensures that the motion sensor identified during the last calibration of the recording equipment has not been changed. Thereby the session key generated during the initial identification and authentication is used.

The TSF is able to establish, for every interaction, the identity of the motion sensor it is connected to. The identity of the motion sensor consists of the sensor approval number and the sensor serial number.

Case b):

The TSF 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).

The TSF permanently and selectively tracks the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the codriver slot of the equipment.

Case c):

For every interaction with an external device, the TSF is able to establish the device identity.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which is used for authentication and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### 6.1.4 Integrity of Stored Data

**F.DATA_INT Stored Data Integrity Monitoring and Action**

This TSF protects the integrity of user data (defined in [EU], Annex 1B, III.12). User data include cryptographic keys. User data is stored

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

Monitoring

This TSF 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.

The TSF protects the user data in the data memory of the main processor by a hash value stored in the SC.

The TSF 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 the data download.

Action

Upon detection of a stored user data integrity error, the TSF generates an audit record.

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

The TSF is effective only with support of the Security Functions of the SC, in particular the SF5 (Data Error Detection) for integrity checks as well as SF10 (Cryptography) for hash calculations.

### 6.1.5 Data Exchange

**F.EX_CONF Confidentiality of Data Exchange**

The TSF protects the confidentiality of secret data being exchanged between the TOE and the external subjects

a) tachograph card

b) motion sensor and

c) external device.

For this purpose, encryption based on symmetric cryptography is used.

The data transfer between the EFAS-3 and

a) tachograph cards is secured according to ISO/IEC 7816-4,

b) the motion sensor is secured according to ISO/DIS 16844-3 and

c) the external device is secured with TDES-cryptographic mechanisms with calculation of a session key based on secrets stored in TSF and external device and dynamic data portions provided by both components at connection time (mutual authentication mechanism).

The cryptographic keys used for securing the data transfer are session keys which are generated during the preceding mutual authentication process between the EFAS-3 and the subject (see TSF F.IA_KEY and F.GEN_SKEYS).

For the encryption, the TSF makes use of the symmetric cryptographic algorithm Triple-DES defined by the standard FIPS 46-3 and the ANSI Standard 9.52 - 1998.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which provides the cryptographic support and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

**F.EX_INT Integrity and Authenticity of Data Exchange**

The TSF protects the authenticity and integrity of data being exchanged between the TOE and the external subjects

a) tachograph card,

b) motion sensor,

c) external device and

d) local downloading equipment

The data transfer between the EFAS-3 and

a) tachograph cards is secured according to ISO/IEC 7816-4.

The TSF verifies the integrity and authenticity of data imported from tachograph cards. Upon detection of card data integrity or authenticity error, the TSF generates an audit record and does not use the data. The TSF exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

b) the motion sensor is secured according to ISO/DIS 16844-3.

The TSF verifies the integrity and authenticity of motion data imported from the motion sensor. Upon detection of a motion data integrity or authenticity error, the TSF generates an audit record and continues to use imported data.

c) the external device is secured due to symmetric cryptography for mutual authentication between the VU and the external device as well as for data integrity during data exchange between the EFAS-3 and the external device

d) the local downloading equipment is secured according to PKCS#1 V2.0 and with hash algorithm SHA-1.
(Note: The source equipment (EFAS-3) identification and its security certification (Member state and equipment) are also downloaded. The verifier of the data must possess independently a trusted European public key.)

The cryptographic keys used for securing the data transfer for a) and b) are session keys which are generated during the preceding mutual authentication process between the EFAS-3 and the user (see TSF F.IA_KEY and F.GEN_SKEYS).

For the generation of message authentication codes for a) and b), the TSF makes use of the symmetric cryptographic algorithm Triple-DES defined by the standard FIPS 46-3 and the ANSI Standard9.52 - 1998.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which provides the cryptographic support and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### 6.1.6 Object Re-use

**F.INF_PROT Residual Information Protection**

The TSF ensures that any previous information content of a resource is explicitly erased upon the allocation of the resource used for volatile and non-volatile memories in the SC of the EFAS-3 used for operations in which security relevant material is involved.

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

The TSF is effective only with support of the Security Functions of the SC, in particular the SF6 (FireWall), SF8 (Event Action), the SF10 (Cryptography) and SF9 (Unobservability).

### 6.1.7 Protection

**F.FAIL_PROT Failure and Tampering Protection**

The TSF 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, the TSF shall

- generate an audit record (except in calibration mode),
- preserve the secure state of the EFAS-3,
- maintain the security functions, related to components or processes still operational,
- preserve the stored data integrity.

In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, the TSF resets the EFAS-3 clearly.

The TSF provides the capability to determine whether **physical tampering** with the TSF's devices or TSF's elements has occurred. The EFAS-3 is designed so 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). All other physical tampering attempts can be easily detected by visual inspection.

After its activation, the EFAS-3 detects specified hardware sabotage (specified in the assurance class development, e.g. sabotage of the real time clock generating time stamps). In the case of the sabotage of the real time clock, the TSF generates an audit record and the EFAS-3 will be blocked (other cases are specified in the assurance class development).

The TSF is effective only with support of the Security Functions of the SC, in particular the SF6 (FireWall) and SF8 (Event Action).

**F.SELFTEST Self Test**

The TSF provides the capability of running self tests during initial start-up, and during normal operation to verify its correct operation.

The EFAS-3 self tests include the verification of the integrity of security data and the verification of stored executable code.

Security data and executable code are stored

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

The SC respective the main processor verifies the integrity of security data and executable code stored in the memory of the SC respective memory of the main processor.

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

Classification:

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

An audit record is generated, if necessary.

All commands, actions or test points, specific to the testing needs of the manufacturing phase of the EFAS-3 are disabled or removed before the EFAS-3 is activated. It is not possible to restore them for later use.

The TSF is supported by F.DATA_INT.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF5 (Data Error Detection), SF6 (FireWall), SF7 (Event Audit), SF8 (Event Action) and SF10 (Cryptography).

### 6.1.8 Cryptographic Operations

**F.GEN_SKEYS Generation of Session Keys**

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

a) tachograph card,

b) motion sensor and

c) external device.

The TSF enforces that the key material meets the following requirements:

- random numbers generated by the EFAS-3 and used in the key generation process have a high quality and
- the 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.

- Only for c): Calculation of a session key based on secrets stored in TSF and external device and dynamic data portions provided by both components at connection time.

Random numbers are generated by the random number generator of the SC.

The TSF for generation of session keys is directly connected with the TSF F.IA_KEY which realises the internal and external authentication process.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which provides the cryptographic support and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### F.GEN_DIGSIG Generation of Digital Signatures optionally with Encryption

The TSF provides a digital signature functionality based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024 bit.

The TSF 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.
- Within authentication processes between the EFAS-3 and the tachograph card for the creation of authentication tokens using the signature scheme with message recovery (signature generation operation) according to the standard ISO 9796-2 and with hash algorithm SHA-1.

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

The TSF provides the functionality to encrypt data based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024. The encryption function will be used for the following purpose:

- Within the authentication process between the EFAS-3 and the tachograph card for the generation of authentication tokens using the encryption primitive according to the standard PKCS#1 V2.0.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which provides the cryptographic support and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

### F.VER_DIGSIG Verification of Digital Signatures optionally with Decryption

The TSF provides a functionality to verify digital signatures based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024 bit.

The TSF function 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.
- Within authentication processes between EFAS-3 and tachograph card for the verification of authentication tokens using the signature scheme with message recovery (signature verification operation) according to the standard ISO 9796-2 and with hash algorithm SHA-1.
- 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 and with hash algorithm SHA-1.

The TSF provides the functionality to decrypt data based on asymmetric cryptography, particularly the RSA algorithm with a key of 1024 bit. The TSF decryption function will be used for the following purpose:

- Within the authentication processes between EFAS-3 and tachograph card for the verification of authentication tokens using the decryption primitive according to the standard PKCS#1 V2.0.

The TSF is effective only with support of the Security Functions of the SC, in particular the SF10 (Cryptography) which provides the cryptographic support and the SF9 (Unobservability) which guaranties the secure execution of cryptographic operations.

## 6.2 SOF Claim for TOE Security Functions

All TOE security functions which are relevant for the assurance requirement AVA_SOF.1 are identified in this section according to Common Criteria, Part 1 [CC1] and Part 3 [CC3].

The TOE security functions using mechanisms which can be analysed for their probabilistic properties and which contribute to AVA_SOF.1 are the following:

- The generation of random numbers within the TSFs F.IA_KEY and F.GEN_SKEYS can be analysed with probabilistic methods.
- The implementation for the hash function SHA-1 in the TSFs F.GEN_DIGSIG and F.VER_DIGSIG can be analysed with permutational or probabilistic methods.

For all TOE security functions an explicit claim of “SOF-high” is made.

The implementation of the TSF F.DATA_INT is partly realised by attaching CRC-sums to defined data areas. The mechanisms of calculating and verifying CRC-sums can be analysed with permutational or probabilistic methods. But these mechanisms are not relevant for AVA_SOF.1 since the protection of data areas by CRC-sums is intended only to protect against accidental data modification. The CRC mechanism can not be attacked directly. It is not possible to manipulate data and concerning CRC values.

The TOE´s cryptographic algorithms itself can also be analysed with permutational or probabilistic methods but this is not in the scope of CC evaluations.

## 6.3 Assurance Measures

To satisfy the security assurance requirements defined in chapter 5.1.3 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.

| Assurance Class | Family | Document(s) containing the relevant information |
|---|---|---|
| ACM Configuration Management | ACM_AUT | Document Configuration Management |
| | ACM_CAP | Document Configuration Management<br>Document Life-Cycle Model |
| | ACM_SCP | Document Configuration Management<br>Document Life-Cycle Model |
| ADO Delivery and Operation | ADO_DEL | Document Life-Cycle Model |
| | ADO_IGS | Document Installation, Generation and Start-Up Procedures |

| | | |
|---|---|---|
| ADV Development | ADV_FSP | Document Functional Specification |
| | ADV_HLD | Document High-Level Design<br>Development documents like design specifications, ... |
| | ADV_LLD | Document Low-Level Design<br>Development documents like design specifications, ... |
| | ADV_IMP | Hardware Design and Source Code<br>Development documents like design specifications, ... |
| | ADV_RCR | Document Functional Specification<br>Document High-Level Design<br>Document Low-Level Design |
| | ADV_SPM | Document Security Policy Model |
| AGD Guidance Documents | AGD_ADM | Part of the Operating manual EFAS-3 |
| | AGD_USR | Operating manual EFAS-3<br>Service and installation manual EFAS-3 |
| ALC Life Cycle Support | ALC_DVS | Document Development Environment Security |
| | ALC_LCD | Document Life-Cycle Model |
| | ALC_TAT | Configuration List |
| ATE Tests | ATE_COV | Document Test Documentation<br>Detailed test documentation like test specifications, ... |
| | ATE_DPT | Document Test Documentation<br>Detailed test documentation like test specifications, ... |
| | ATE_FUN | Document Test Documentation<br>Detailed test documentation like test specifications, ... |
| | ATE_IND | Samples of the TOE Source Code and Hardware |
| AVA Vulnerability Assessment | AVA_MSU | Document Guidance Document Analysis |
| | AVA_SOF | Document Security Function Evaluation |
| | AVA_VLA | Document Vulnerability Analysis |

**Table 24: Overview of Developer´s TOE related Documents**

## 6.4 Compliance with the generic security target

The table below shows the relationship between the described TOE Security Functions and the SFRs as well as the Security enforcing functions of the generic security target [EU], Appendix 10. The left column contains the Security enforcing functions of the generic security target [EU], the middle column refers to the corresponding SFRs of this ST and the left column indicates the security functions of the TOE which implementations meet the the Security enforcing functions of the generic security target [EU].

| **Security enforcing function, generic security target [EU], Appendix 10** | **SFR, Chapter 5.1.1.2** | **TOE Security Functions, Chapter 6.1** |
|---|---|---|

| 4.1. Identification and authentication<br>4.1.1. Motion sensor identification and authentication | | |
|---|---|---|
| UIA_201 The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to. | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| UIA_202 The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number. | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| UIA_203 The VU shall authenticate the motion sensor it is connected to:<br>- at motion sensor connection,<br>- at each calibration of the recording equipment,<br>- at power supply recovery.<br>Authentication shall be mutual and triggered by the VU. | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| UIA_204 The VU shall periodically (period TBD by manufacturer and more frequently than once per hour) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed. | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| UIA_205 The VU shall detect and prevent use of authentication data that has been copied and replayed. | FIA_UAU.3.2 | F.IA_KEY |
| UIA_206 After (TBD by manufacturer and not more than 20) consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the SEF shall:<br>- generate an audit record of the event,<br>- warn the user,<br>- continue to accept and use non secured motion data sent by the motion sensor. | FIA_AFL.1.1/ Motion_sensor | F.IA_KEY |
| **4.1.2. User identification and authentication** | | |
| UIA_207 The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment. | FIA_UID.1.2 | F.IA_KEY |

| | | |
|---|---|---|
| UIA_208 The user identity shall consist of:<br>.- a user group:<br>- DRIVER (driver card),<br>- CONTROLLER (control card),<br>- WORKSHOP (workshop card),<br>- COMPANY (company card),<br>-. UNKNOWN (no card inserted),<br>- a user ID, composed of:<br>- the card issuing Member State code and of the card number,<br>- UNKNOWN if user group is UNKNOWN.<br>UNKNOWN identities may be implicitly or explicitly known. | FIA_UID.1.2 | F.IA_KEY |
| UIA_209 The VU shall authenticate its users at card insertion. | FIA_UAU.1.2 | F.IA_KEY |
| UIA_210 The VU shall re-authenticate its users:<br>- at power supply recovery,<br>- periodically or after occurrence of specific events (TBD by manufacturers and more frequently than once per day). | FIA_UAU.6.1 | F.IA_KEY |
| UIA_211 Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU. | FIA_UAU.1.2 | F.IA_KEY |
| UIA_212 In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long.<br>Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer. | FIA_UAU.1.2 | F.IA_KEY |
| UIA_213 The VU shall detect and prevent use of authentication data that has been copied and replayed. | FIA_UAU.3.2 | F.IA_KEY |
| UIA_214 After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall:<br>- generate an audit record of the event,<br>- warn the user,<br>- assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007). | FIA_AFL.1.1/ Card | F.IA_KEY |
| **4.1.3. Remotely connected company identification and authentication** | | |
| UIA_215 For every interaction with a remotely connected company, the VU shall be able to establish the company's identity. | FIA_UID.1.2 | F.IA_KEY |
| UIA_216 The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number. | FIA_UID.1.2 | F.IA_KEY |
| UIA_217 The VU shall successfully authenticate the remotely connected company before allowing any data export to it. | FIA_UAU.1.2 | F.IA_KEY |

| | | |
|---|---|---|
| UIA_218 Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute. | FIA_UAU.1.2 | F.IA_KEY |
| UIA_219 The VU shall detect and prevent use of authentication data that has been copied and replayed. | FIA_UAU.3.2 | F.IA_KEY |
| UIA_220 After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:<br>- warn the remotely connected company. | FIA_AFL.1.1/ Company | F.IA_KEY |
| **4.1.4. Management device identification and authentication** | | |
| UIA_221 For every interaction with a management device, the VU shall be able to establish the device identity. | FTP_ITC.1.1/ Ext_device | F.IA_KEY<br>F.EX_INT<br>F.EX_CONF |
| UIA_222 Before allowing any further interaction, the VU shall successfully authenticate the management device. | FTP_ITC.1.1/ Ext_device | F.IA_KEY<br>F.EX_INT<br>F.EX_CONF |
| UIA_223 The VU shall detect and prevent use of authentication data that has been copied and replayed. | FIA_UAU.3.2 | F.IA_KEY |
| **4.2. Access control**<br>**4.2.1. Access control policy** | | |
| ACC_201 The VU shall manage and check access control rights to functions and to data. | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| **4.2.2. Access rights to functions** | | |
| ACC_202 The VU shall enforce the mode of operation selection rules (requirements 006 to 009). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_203 The VU shall use the mode of operation to enforce the functions access control rules (requirement 010). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| **4.2.3. Access rights to data** | | |
| ACC_204 The VU shall enforce the VU identification data write access rules (requirement 076) | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_205 The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155) | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_206 After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_207 After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_208 After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| ACC_209 After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100). | FDP_ACF.1.1 (AC_SFP) | F.ACS |

| | | |
|---|---|---|
| ACC_210 The VU shall enforce appropriate read and write access rights to security data (requirement 080). | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| **4.2.4. File structure and access conditions** | | |
| ACC_211 Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion. | FDP_ACF.1.1 (AC_SFP) | F.ACS |
| **4.3. Accountability** | | |
| ACT_201 The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a). | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_202 The VU shall hold permanent identification data (requirement 075). | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_203 The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109). | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_204 The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109). | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_205 The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093). | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_206 The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data. | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| ACT_207 The VU shall ensure that it does not modify data already stored in a tachograph card (requirements 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1. | FDP_ACF.1.2 (AC_SFP) | F.ACS |
| **4.4. Audit**<br>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 to security. | | |
| AUD_201 The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109). | FAU_GEN.1.2 | F.SECAUDIT |

| | | |
|---|---|---|
| AUD_202 The events affecting the security of the VU are the following:<br>- Security breach attempts,<br>- motion sensor authentication failure,<br>- tachograph card authentication failure,<br>- unauthorised change of motion sensor,<br>- card data input integrity error,<br>- stored user data integrity error,<br>- internal data transfer error,<br>- unauthorised case opening,<br>- hardware sabotage,<br>- last card session not correctly closed,<br>- motion data error event,<br>- power supply interruption event,<br>- VU internal fault. | FAU_SAA.1.2 | F.SECAUDIT |
| AUD_203 The VU shall enforce audit records storage rules (requirement 094 and 096). | FAU_GEN.1.2 | F.SECAUDIT |
| AUD_204 The VU shall store audit records generated by the motion sensor in its data memory. | FAU_GEN.1.2 | F.SECAUDIT |
| AUD_205 It shall be possible to print, display and download audit records. | FAU_GEN.1.2 | F.SECAUDIT |
| **4.5. Object re-use** | | |
| REU_201 The VU shall ensure that temporary storage objects can be re-used without this involving inadmissible information flow. | FDP_RIP.1.1 | F.INF_PROT |
| **4.6. Accuracy**<br>**4.6.1. Information flow control policy** | | |
| ACR_201 The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:<br>- vehicle motion data,<br>- VU's real time clock,<br>- recording equipment calibration parameters,<br>- tachograph cards,<br>- user's inputs. | FDP_ACC.2.2 | F.ACS |
| ACR_201a The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal<br>- current insertion (requirement 050a). | FDP_ACC.2.2 | F.ACS |

| | | |
|---|---|---|
| **4.6.2. Internal data transfers**<br>The requirements of this paragraph apply only if the VU makes use of physically separated parts. | | |
| ACR_202 If data are transferred between physically separated parts of the VU, the data shall be protected from modification. | Not applicable | Not applicable |
| ACR_203 Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event. | Not applicable | Not applicable |
| **4.6.3. Stored data integrity** | | |
| ACR_204 The VU shall check user data stored in the data memory for integrity errors. | FDP_SDI.2.1 | F.ACS<br>F.DATA_INT |
| ACR_205 Upon detection of a stored user data integrity error, the SEF shall generate an audit record. | FDP_SDI.2.2 | F.ACS<br>F.DATA_INT |
| **4.7. Reliability of service**<br>**4.7.1. Tests** | | |
| RLB_201 All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. It shall not be possible to restore them for later use. | FPT_TST.1.1 | F.SELFTEST |
| RLB_202 The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM). | FPT_TST.1.1 | F.SELFTEST |
| RLB_203 Upon detection of an internal fault during self test, the SEF shall:<br>- generate an audit record (except in calibration mode) (VU internal fault),<br>- Preserve the stored data integrity. | FPT_TST.1.1 | F.SELFTEST |
| **4.7.2. Software** | | |
| RLB_204 There shall be no way to analyse or debug software in the field after the VU activation. | FPT_SEP.1.2 | F.ACS |
| RLB_205 Inputs from external sources shall not be accepted as executable code. | FPT_SEP.1.2 | F.ACS |
| **4.7.3. Physical protection** | | |
| RLB_206 If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).<br>If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection). | FPT_PHP.1.2 | F.FAIL_PROT |
| RLB_207 After its activation, the VU shall detect specified (TBD by manufacturer) hardware sabotage. | FPT_PHP.1.2 | F.FAIL_PROT |
| RLB_208 In the case described above, the SEF shall generate an audit record and the VU shall: (TBD by manufacturer). | FPT_PHP.1.2 | F.FAIL_PROT |

| **4.7.4. Power supply interruptions** | | |
|---|---|---|
| RLB_209 The VU shall detect deviations from the specified values of the power supply, including cut-off. | FPT_FLS.1.1 | F.FAIL_PROT |
| RLB_210 In the case described above, the SEF shall:<br>- generate an audit record (except in calibration mode),<br>- preserve the secure state of the VU,<br>- maintain the security functions, related to components or processes still operational,<br>- preserve the stored data integrity. | FPT_FLS.1.1 | F.FAIL_PROT |
| **4.7.5. Reset conditions** | | |
| RLB_211 In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall be reset cleanly. | FPT_FLS.1.1 | F.FAIL_PROT |
| **4.7.6. Data availability** | | |
| RLB_212 The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily. | FPT_ITA.1.1 | F.ACS |
| RLB_213 The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016) | FPT_ITA.1.1 | F.ACS |
| RLB_214 In the case described above, the SEF shall generate an audit record of the event. | FPT_ITA.1.1 | F.ACS |
| **4.7.7. Multiple applications** | | |
| RLB_215 If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time. | FPT_SEP.1.2 | F.ACS |
| **4.8. Data exchange**<br>**4.8.1. Data exchange with motion sensor** | | |
| DEX_201 The VU shall verify the integrity and authenticity of motion data imported from the motion sensor | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| DEX_202 Upon detection of a motion data integrity or authenticity error, the SEF shall:<br>- generate an audit record,<br>- continue to use imported data. | FTP_ITC.1.1/ Motion_sensor | F.IA_KEY<br>F.EX_INT |
| **4.8.2. Data exchange with tachograph cards** | | |
| DEX_203 The VU shall verify the integrity and authenticity of data imported from tachograph cards. | FTP_ITC.1.1/ Card | F.IA_KEY<br>F.EX_INT |
| DEX_204 Upon detection of card data integrity or authenticity error, the VU shall:<br>- generate an audit record,<br>- not use the data. | FTP_ITC.1.1/ Card | F.IA_KEY<br>F.EX_INT |

| | | |
|---|---|---|
| DEX_205 The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity. | FTP_ITC.1.1/ Card | F.IA_KEY<br>F.EX_INT |
| **4.8.3. Data exchange with external storage media (downloading function)** | | |
| DEX_206 The VU shall generate an evidence of origin for data downloaded to external media. | FCO_NRO.1.1 | F.ACS<br>F.GEN_DIGSIG |
| DEX_207 The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient. | FCO_NRO.1.3 | F.ACS<br>F.GEN_DIGSIG |
| DEX_208 The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified. | FCO_NRO.1.2 | F.ACS<br>F.GEN_DIGSIG |
| **4.9. Cryptographic support**<br>The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions. | | |
| CSP_201 Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size. | FCS_COP.1.1/* | F.ACS, F.EX_INT, F.EX_CONF, F.GEN_DIGSIG, F.VER_DIGSIG |
| CSP_202 If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. | FCS_CKM.1.1 | F.IA_KEY<br>F.GEN_SKEYS |
| CSP_203 If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods. | FCS_CKM.2.1/* | F.ACS, F.IA_KEY, F.GEN_SKEYS, F.GEN_DIGSIG, F.VER_DIGSIG |
| CSP_204 If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods. | FCS_CKM.3.1/* | F.ACS |
| CSP_205 If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods. | FCS_CKM.4.1 | F.INF_PROT |

**Table 25: Compliance with the generic security target**

# 7 PP Claims

Not applicable.

# 8 Rationale

The following chapters cover the security objectives rationale, the security requirements rationale and the TOE summary specification rationale.

## 8.1 Security Objectives Rationale

According to the requirements of Common Criteria, Part 1 [CC1] and Part 3 [CC3] the security objective rationale shows that each security objective of the TOE and its environment counters at least one threat or matches at least to one assumption. Inversely, the security objectives rationale shows that the stated security objectives for the TOE and its environment cover all identified assumptions and counter all identified threats to security.

### 8.1.1 Threats - Security Objectives

The threats of the SC as refered in chap. 3 are covered completely by the security objectives for the SC refered in chap. 4. The mapping of the threats of the SC to the relevant security objectives is done within the CC evaluation of the SC resp. within the associated Security Target [ATMEL_ST].

The security objectives listed in chapter 4.1 and 4.2 refine the security objectives O.VU_Main and O.VU_Export. In the following tables is shown that the security objectives of chapter 4.1 and 4.2 counter all threats listed in chapter 3.3 and therefore the security objectives O.VU_Main and O.VU_Export are met.

| **Threats** | **Objectives** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | O.Access | O.Accountability | O.Audit | O.Authentication | O.Integrity | O.Output | O.Processing | O.Reliability | O.Secured_Data_Exchange | O.Design |
| T.Access | X | | X | X | | | | | | X |
| T.Identification | | X | X | X | | | | | | |
| T.Faults | | | | | | | | X | | |
| T.Tests | | | | | | | | X | | |
| T.Design | | | | | | | | X | | |
| T.Calibration_Parameters | X | | | X | | | X | | | |
| T.Card_Data_Exchange | | | X | | | | | X | X | |
| T.Clock | X | | | X | | | | | | |
| T.Environment | | | | | | | | X | | |
| T.Fake_Devices | X | | X | X | | | | X | X | |
| T.Hardware | | | X | | | | X | X | | X |
| T.Motion_Data | | | X | X | | | X | X | X | |
| T.Non_Activated | | | | | | | | | | |
| T.Output_Data | | | X | | | X | | | | |
| T.Power_Supply | | | X | | | | | X | | |
| T.Security_Data | X | | | | | | X | X | | |
| T.Software | X | | X | | | X | X | X | | X |
| T.Stored_Data | X | | X | | X | | | X | X | X |

**Table 26: Mapping of threats to objectives**

| Threats | Objectives | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OE.Development | OE.ManufacturingOE.Manufacturing | OE.Delivery | OE.Activation | OE.Sec_Data_Generation | OE.Sec_Data_Transport | OE.Card_Availability | OE.Driver_Card_Uniqueness | OE.Card_Traceability | OE.Approved_Workshops | OE.Regular_Inspections | OE.Faithful_Calibration | OE.Faithful_Drivers | OE.Controls | OE.Software_Upgrade |
| T.Access | | | | X | | | | | | | | | | | |
| T.Identification | | | | | | | X | X | X | | | | X | X | |
| T.Faults | X | | | | | | | | | | | | | | |
| T.Tests | X | X | | | | | | | | | | | | | |
| T.Design | X | X | | | | | | | | | | | | | |
| T.Calibration_Parameters | | | | | | | | | | X | X | X | | X | |
| T.Card_Data_Exchange | | | | | | | | | | | | | | | |
| T.Clock | | | | | | | | | | X | X | X | | X | |
| T.Environment | | | | | | | | | | | | | | X | |
| T.Fake_Devices | | | | | | | | | | | | | | | |
| T.Hardware | | | | | | | | | | | X | | | X | |
| T.Motion_Data | | | | | | | | | | | | | | | |
| T.Non_Activated | | | X | X | | | | | | | | | | X | |
| T.Output_Data | | | | | | | | | | | | | | | |
| T.Power_Supply | | | | | | | | | | | X | | | X | |
| T.Security_Data | | | | | X | X | | | | | | | | X | |
| T.Software | | | | | | | | | | | X | | | X | X |
| T.Stored_Data | | | | | | | | | | | | | | | |

**Table 27: Mapping of threats to objectives for the environment**

In the following, for each TOE threat it will be explained why and how it is addressed by the security objectives listed in the tables above.

### T.Access

The control of user access to functions and data as prescribed by the security objective O.Access counters directly the threat T.Access.

Furthermore, the security objectives O.Design, O.Audit and O.Authentication prevent the possibility that a user gains access to functions and data by adopting a false identity and support thereby the realisation of the objective O.Access.

The security objective for the environment OE.Activation supports the objectives mentioned above by assuring that the security functions of the TOE are active. So, there is no way for the user to circumvent these security functions.

### T.Identification

The combination of the security objectives O.Authentication, O.Accountability and O.Audit as well as the security objectives for the environment OE.Card_Availability, OE.Driver_Card_Uniqueness, OE.Card_Traceability, OE.Faithful_Drivers and OE.Controls counters the threat T.Identification.

First, the security objectives O.Authentication and O.Accountability authenticates the user by its card holder identity. The security objective O.Audit audits attempts to use no identity.

The uniqueness of the mapping between the card holder identity and the identity of the user, e.g. the driver, is guaranteed by the security objectives OE.Faithful_Drivers and OE.Controls.

The uniqueness of the card itself is assured by the objectives OE.Driver_Card_Uniqueness and OE.Card_Traceability. The objective OE.Card_Availability prevents the possibility that a driver has no card.

### T.Faults

The security objective O.Reliability addresses directly the threat by avoiding unforeseen

states of the EFAS-3 in case of faults. The objective OE.Development counters the threat indirectly

by organisational means during the development.

### T.Tests

The threat T.Tests is countered by the combination of security objectives OE.Development, OE.Manufacturing and O.Reliability.

The security objective O.Reliability inhibits the use of test modes after activating the EFAS-3.

The security objectives for the environment OE.Development and OE.Manufacturing guarantee the invalidating of test modes of the EFAS-3 before activation and the non-existence of back doors by organisational means.

### T.Design

The threat T.Design is also countered by the combination of security objectives OE.Development, OE.Manufacturing and O.Reliability.

Here the security objective O.Reliability makes it difficult for the user to gain information about the design of the EFAS-3 by reverse engineering.

The security objectives for the environment OE.Development and OE.Manufacturing prevent the leak of manufacturer’s material about the design of the EFAS-3 by organisational means during design and manufacturing of the EFAS-3.

### T.Calibration_Parameters

The security objectives for the environment OE.Approved_Workshops, OE.Regular_Inspections, OE.Faithful_Calibration and OE.Controls assure by organisational means that the TOEs which are used have been calibrated correctly.

The security objectives O.Access and O.Authentication guarantee that a modification of the calibration data is only possible if the user is in possession of a workshop card and the respective PIN. The security objective O.Processing ensures that the stored calibration parameters are used for an accurate calculation of the motion data.

So the combination of these objectives counters the threat T.Calibration_Parameters.

### T.Card_Data_Exchange

The threat T.Card_Data_Exchange is countered by the combination of the security objectives O.Audit, O.Secured_Data_Exchange and O.Reliability.

The security objective O.Secured_Data_Exchange secures the data exchange between the EFAS-3 and the tachograph card, such that modifications of the data are detected. In this case by the security objective O.Audit modifications of exchanged data are audited by the EFAS-3. With O.Reliability data are exchanged by reliable services.

### T.Clock

The threat T.Clock is countered as follows:

The security objectives for the environment OE.Approved_Workshops, OE.Regular_Inspections, OE.Faithful_Calibration and OE.Controls assure by organisational means that the internal clock of the EFAS-3 have been set to the correct time and is controlled regularly.

The security objectives O.Access and O.Authentication guarantee that a modification of the internal clock is only possible if the user is in possession of a workshop card and the respective PIN.

### T.Environment

The threat T.Environment is countered by the combination of the security objective O.Reliability and the security objective for the environment OE.Controls.

The objective O.Reliability detect such an environmental attack, e.g. if the case is opened, and the objective OE.Controls counter such an attack by organisational means.

### T.Fake_Devices

The threat T.Fake_Devices is countered by the following security objectives:

First, by the objective O.Authentication the EFAS-3 authenticates the connected entities and detects fake devices under them. In this case this event is audited by the objective O.Audit. The objective O.Access protects especially the motion sensor identification data stored in the EFAS-3 and which are used for the authentication. The security objective O.Secured_Data_Exchange secures the data exchange between the EFAS-3 and the tachograph card and Motion Sensor, such that fake devices are detected. Finally the security objective O.Reliability provices reliable services protecting against the connection of faked devices.

### T.Hardware

The threat T.Hardware is countered by the following security objectives:

The security objectives O.Design, O.Reliability and O.Processing detect manipulations of the EFAS-3 hardware which affect the security functionality of the EFAS-3. These manipulations are audited according to the security objective O.Audit. These audits enable organisational means by the security objective for the environment OE.Controls. The modification of hardware is also detected since due to the objective for the environment OE.Regular_Inspections recording equipment is periodically inspected and calibrated.

### T.Motion_Data

The security objective O.Authentication authenticates the motion sensor. The security objective O.Secured_Data_Exchange secures the data exchanges between motion sensor and EFAS-3 based on the authentication of the motion sensor. If the motion data are modified the objective O.Audit audits this event. O.Reliability provides only reliable services. O.Processing supports the protection against an unauthorised modification of VUs motion data.

So, the combination of these objectives counters the threat T.Motion_data.

### T.Non_Activated

This threat is countered by the following security objectives for the environment:

The objective OE.Delivery ensures that the handling of non-activated EFAS-3 is done in a manner which maintains EFAS-3 security. The objective OE.Activation guarantees that EFAS-3 are activated after its installation before the vehicle leaves the premises where installation took place. The objective OE.Controls ensures via regularly and randomly performed law enforcement controls regularly and randomly including security audits that users could not use non activated equipment.

### T.Output_Data

The threat T.Output_Data is countered directly by the security objective O.Output. The objective O.Audit supports O.Output by auditing attempts to manipulate output data.

### T.Power_Supply

The threat T.Power_Supply is countered by the combination of the security objectives O.Audit and O.Reliability and the security objective for the environment OE.Controls.

The objective O.Reliability detects a modification of the power supply and the objectives O.Audit audits such an attempt. By the objective OE.Controls the threat is countered by controlling the audit of this event. Manipulations via power supply are also detected since due to the objective for the environment OE.Regular_Inspections recording equipment is periodically inspected and calibrated.

### T.Security_Data

Since user access to data is controlled by the EFAS-3 and the EFAS-3 provides a reliable service the threat T.Security_Data, i.e. that users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment, is countered by the combination of the security objectives O.Access and O.Reliability. Additionally the security objectives for the environment OE.Sec_Data_Generation enforcing that security data generation algorithms are only accessible to authorised and trusted persons only and OE.Sec_Data_Transport enforcing that security data must be generated, transported, and inserted into the EFAS-3, in such a way to preserve its appropriate confidentiality and integrity ensure that the threat is completely countered. By the security objective for the environment OE.Controls law enforcement controls are performed regularly and randomly including security audits. Finally O.Processing ensures that processing of inputs to derive user data is accurate.

### T.Software

The threat T.Software which consists of the potential modification of EFAS-3 software by users is countered by the combination of the security objectives O.Design, O.Access and O.Reliability and the security objective for the environment OE.Controls. O.Design guarantees secure use of the SC by the software. O.Access controls user access to EFAS-3 software, O.Reliability provides only reliable services and OE.Controls ensure that law enforcement controls including security audits are regularly and randomly performed. Modification of VUs software is also detected since due to the security objective for the environment OE.Regular_Inspections recording equipment is periodically inspected and calibrated. By O.Audit attempts to undermine the system security, based on the EFAS-3 software, are audited. With O.Output and O.Processing software modification is not possible via data output and via data input. With OE.Software_Upgrade the security certification of software revisions protects the software against unauthorised modification.

### T.Stored_Data

The threat T.Stored_Data i.e. that users could try to modify stored data (security or user data) is countered by the combination of the security objectives O.Design (guarantees secure use of the SC by the software), O.Access (which controls user access to EFAS-3), O.Audit (ensuring that EFAS-3 audits attempts to undermine system security and traces theme to associated users) and O.Integrity (maintaining the integrity of stored data).The objective O.Reliability accounts for the protection of sensitive data against modification by providing reliable services. Additionally O.Secured_Data_Exchange protects the unauthorised modification of stored data via sensitive interfaces since the EFAS-3 must secure data exchanges with the motion sensor and with tachograph cards.

### 8.1.2 Assumptions - Security Objectives

The mapping of the assumptions for the environment of the TOE to the relevant security objectives assigns each assumption to the equally named objective.

| **Assumptions** | **Objectives for the environment** |
|---|---|
| A.Development | OE.Development |
| A.Manufacturing | OE.Manufacturing |
| A.Delivery | OE.Delivery |
| A.Activation | OE.Activation |

| | |
|---|---|
| A.Sec_Data_Generation | OE.Sec_Data_Generation |
| A.Sec_Data_Transport | OE.Sec_Data_Transport |
| A.Card_Availability | OE.Card_Availability |
| A.Driver_Card_Uniqueness | OE.Driver_Card_Uniqueness |
| A.Card_Traceability | OE.Card_Traceability |
| A.Approved_Workshops | OE.Approved_Workshops |
| A.Regular_Inspections | OE.Regular_Inspections |
| A.Faithful_Calibration | OE.Faithful_Calibration |
| A.Faithful_Drivers | OE.Faithful_Drivers |
| A.Controls | OE.Controls |
| A.Software_Upgrade | OE.Software_Upgrade |

**Table 28: Mapping of assumptions to objectives for the environment**

### 8.1.3 Organisational Security Policies - Security Objectives

The security objective O.Design requires the developer of the SC software to take into account the requirements of the SC developer as assumed in the Organisational Security Policy P.Design and P.CRYPTO, thus these OSPs are covered by this security objective.

## 8.2 Security Requirements Rationale

According to the requirements of Common Criteria, CC Part 1 [CC1] and CC Part 3 [CC3], the security requirements rationale demonstrates that the set of security requirements of the TOE is suitable to meet the security objectives for the TOE and its environment. In detail, the following will be shown:

- The stated security objectives are met by the combination of the functional and assurance requirements components for the TOE and its IT environment.
- Mutual support and internal consistency are met by the set of security requirements.
- The choice of security requirements is reasoned, whereby any of the following conditions is specifically reasoned:
  - chosen additional requirements not included in Parts 2 or 3,
  - chosen additional assurance requirements not included in EAL 4,
  - non-satisfaction of dependencies.
- The selected strength of function level for the ST is consistent with the security objectives for the TOE.

### 8.2.1 Security Functional Requirements Rationale

The security objectives for the SC of chap. 4 are related to the SARs and SFRs for the TOE defined in chap. 5. The mapping of the security objectives for the SC to the relevant SARs and SFRs is done within the CC evaluation of the IC resp. within the associated Security Target [ATMEL_ST].

This chapter shows that the set and combination of the security assurance requirements (SARs) and the defined security functional requirements (SFRs) for the TOE are suitable to reach the identified security objectives for the TOE and its environment. Additionally this chapter shows that each of these SARs and SFRs contributes to at least one of the security objectives for the TOE and its environment.

The table below gives an overview which SFRs for the TOE contribute to the satisfaction of each TOEs specific security objective.

| **Security Functional Requirements** | **Objectives** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | O.Access | O.Accountability | O.Audit | O.Authentication | O.Integrity | O.Output | O.Processing | O.Reliability | O.Secured_Data _Exchange |
| FAU_GEN.1 | | | X | | | | | | |
| FAU_SAA.1 | | | X | | | X | | X | |
| FCO_NRO.1 | | | | | | X | | | |
| FCS_CKM.1 | | | | | | | | X | X |
| FCS_CKM.2/Session_key | | | | | | | | X | X |
| FCS_CKM.2/RSA_cert | | | | | | | | X | X |
| FCS_CKM.3/RSA_private_sig | | | | | | | | X | X |
| FCS_CKM.3/RSA_public_sig | | | | | | | | X | X |
| FCS_CKM.3/RSA_private_enc | | | | | | | | X | X |
| FCS_CKM.3/RSA_public_dec | | | | | | | | X | X |
| FCS_CKM.3/Session_key | | | | | | | | X | X |
| FCS_CKM.3/Key_motion_sensor | | | | | | | | X | X |
| FCS_CKM.3/RSA_private_IDD | | | | | | | | X | X |
| FCS_CKM.3/Ext_device | | | | | | | | X | X |
| FCS_CKM.4 | | | | | | | | X | X |
| FCS_COP.1/RSA_card_cert | | | | | | | | X | X |
| FCS_COP.1/RSA_Signature | | | | | | | | X | X |
| FCS_COP.1/RSA_enc_dec | | | | | | | | X | X |
| FCS_COP.1/3-DES | | | | | | | | X | X |
| FCS_COP.1/MAC | | | | | | | | X | X |
| FCS_COP.1/3-DES_motion_sensor | | | | | | | | X | X |
| FCS_COP.1/RSA_IDD | | | | | | | | X | X |
| FCS_COP.1/Ext_device | | | | | | | | X | X |
| FDP_ACC.2 | X | | | | | | X | X | |
| FDP_ACF.1 | X | X | X | | X | | | X | |
| FDP_ITC.1 | X | | | | | | | | |
| FDP_RIP.1 | | | | | | | X | X | |
| FDP_SDI.2 | | | X | | X | | | X | |
| FIA_AFL.1/Motion_sensor | | | X | | | | | X | |
| FIA_AFL.1/Card | | | X | | | | | X | |
| FIA_AFL.1/Company | | | X | | | | | X | |
| FIA_UAU.1 | X | | | X | | | | | X |
| FIA_UAU.3 | X | | | X | | | | | |
| FIA_UAU.6 | X | | | X | | | | | X |
| FIA_UID.1 | X | | | X | | | | | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| FPT_FLS.1 | | | X | | | | | X | |
| FPT_ITA.1 | | | X | | | | X | X | |
| FPT_PHP.1 | | | X | | | X | | X | |
| FPT_SEP.1 | | | | | | X | X | X | |
| FPT_STM.1 | | X | X | | | | | X | |
| FPT_TST.1 | | | X | | | | | X | |
| FTP_ITC.1/Motion_sensor | | | X | | | | | X | X |
| FTP_ITC.1/Card | | | X | | | | | X | X |
| FTP_ITC.1/Ext_device | | | X | | | | | X | X |

**Table 29: Mapping of security objectives to security functional requirements**

In the following, for each TOE specific security objective it will be explained why and how it is satisfied by the SFRs listed in the preceding table.

### O.Access

According to the security objective O.Access the TOE enforces the access rules defined in the security functional policy AC_SFP by the security functional requirements FDP_ACC.2, FDP_ACF.1 and FDP_ITC.1.

The components FIA_UAU.1, FIA_UAU.3, FIA_UAU.6 and FIA_UID.1 supply a successful identification and authentication of the user before getting access to data or functions of the EFAS-3 and therefore support the enforcing of the access rules.

### O.Accountability

According to the security objective O.Accountability the TOE collects accurate accountability data by the functional requirement FDP_ACF.1. This functionality is supported by a reliable time stamp supplied by the component FPT_STM.1.

### O.Audit

According to the security objective O.Audit the TOE audits attempts to undermine system security and trace them back to associated users.

The audit records are generated by the components FAU_GEN.1 according to the rules defined by the component FAU_SAA.1.

These attempts to undermine the system security are detected by the components FDP_ACF.1, FDP_SDI.2, FIA_AFL.1/Motion_sensor, FIA_AFL.1/Card, FIA_AFL.1/Company, FPT_FLS.1, FPT_ITA.1, FPT_PHP.1, FPT_STM.1, FPT_TST.1, , FTP_ITC.1/Motion_sensor, FTP_ITC.1/Card and FTP_ITC.1/Ext_device.

### O.Authentication

According to the security objective O.Authentication the TOE authenticates users and connected entities.

The authentication is accomplished by the components FIA_UAU.1, FIA_UAU.3 and FIA_UAU.6. The authentication is supported by the identification of the users and connected entities as required by the component FIA_UID.1.

### O.Integrity

According to the security objective O.Integrity the TOE maintains the integrity of stored data.

The TOE monitors the stored data for integrity errors by the component FDP_SDI.2. Furthermore the access to modify the stored data is restricted by the component FDP_ACF.1.

### O.Output

According to the security objective O.Output the TOE ensures that the data output reflects accurately data measured or stored.

The component FCO_NRO.1 provides an evidence of origin in form of a digital signature of the data output. FAU_SAA.1 supports this security objective since the recognition of violations are reflected in the data output.

The components FPT_PHP.1 and FPT_SEP.1 support this functionality by detecting of physical tampering and refusing input from external sources as executable code.

#### O.Processing

According to the security objective O.Processing the TOE ensures that processing of inputs to derive user data is accurate.

First, the user data are only processed from the right input sources by component FDP_ACC.2. By the component FPT_ITA.1 the EFAS-3 ensures that the access to the input data is obtained when required. The component FDP_RIP.1 ensures that temporary storage objects can be re-used without involving inadmissible information flow.

Finally by the component FPT_SEP.1 the TOE refuses input from external sources as executable code.

#### O.Reliability

According to the security objective O.Reliability the TOE provides a reliable service.

This is accomplished by the functional components FDP_ACC.2, FDP_ACF.1, FDP_RIP.1 and FDP_SDI.2 referring to protection of the data and by the components FPT_FLS.1, FPT_ITA.1, FPT_PHP.1, FPT_SEP.1, FPT_STM.1, FPT_TST.1 and FTP_ITC.1/*referring the protection of the TOE itself. Furthermore, the components FIA_AFL.1/* handle authentication failures.

FAU_SAA.1 supports this security objective since potential violations are recognised by the VU which is a necessary assumption to provide reliable services.

Finally the components FCS_CKM.1, FCS_CKM.2/*, FCS_CKM.3/*, FCS_CKM.4 and FCS_COP.1/* support the functionality by providing cryptographic means.

#### O.Secured_Data_Exchange

According to the security objective O.Secured_Data_Exchange the TOE secures data exchanges with the motion sensor and with tachograph cards.

The securing of the data exchange is accomplished by the components FTP_ITC.1/*.

To this functionality support cryptographical methods defined by the components FCS_CKM.1, FCS_CKM.2/*, FCS_CKM.3/*, FCS_CKM.4and FCS_COP.1/*. Furthermore, the identification and authentication of the connected entities is done by the components FIA_UAU.1, FIA_UAU.6 and FIA_UID.1.

#### O.Design

The design of the SC software in such a manner, that the requirements from the SC developer, i. e. from all relevant guidance documents are met, is covered by the SARs for the whole TOE. In particular, the components of the class ADV with its design documentation and implementation representation contribute to the fulfilment of the security objective O.Design.

### 8.2.2 Security Functional Requirements Dependencies

The dependencies under the SFRs for the SC of chap. 5 are considered in the scope of the CC evaluation of the SC resp. within the associated Security Target [ATMEL_ST].

The following section demonstrates that all dependencies between the identified security functional requirements included in this ST are satisfied.

The following table includes an overview of all SFRs and their dependencies. For each SFR information are provided about the relevance of the dependency and about the satisfaction of dependencies by other SFRs of this ST. If - according to the definitions in CC Part 2 [CC2] - alternative dependencies exist, only the chosen one is referred. Furthermore, only direct dependencies are considered. The table does not include the FMT-components in the dependencies column since the TOE´s functionality as defined in the Tachograph specification [EU], Annex 1B does not require functionality regarding the management of TOE Security Functions, security attributes, roles or TSF Data. Since the SFRs are analysed in alphabetic order SFRs may occur as dependencies before being analysed.

| Number | SFR | Dependencies | Support or comment |
|---|---|---|---|
| 1. | FAU_GEN.1<br>Audit Data Generation | FPT_STM.1 Reliable time stamps | FPT_STM.1 |
| 2. | FAU_SAA.1<br>Potential Violation Analysis | FAU_GEN.1 Audit data generation | FAU_GEN.1 |
| 3. | FCO_NRO.1<br>Selective Proof of Origin | FIA_UID.1 Timing of identification | FIA_UID.1 |
| 4. | FCS_CKM.1<br>Cryptographic Key Generation | [FCS_CKM.2 Cryptographic key distribution or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.2/Session_key<br>FCS_CKM.4<br>**Not applicable** |
| 5. | FCS_CKM.2/Session_key<br>Cryptographic Key Distribution | [FDP_ITC.1 Import of user data without security attributes<br>or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 6. | FCS_CKM.2/RSA_cert<br>Cryptographic Key Distribution | [FDP_ITC.1 Import of user data without security attributes<br>or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FDP_ITC.1<br>-<br>**Not applicable** |
| 7. | FCS_CKM.3/RSA_private_sig<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 8. | FCS_CKM.3/RSA_public_sig<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |

| Num ber | SFR | Dependencies | Support or comment |
|---|---|---|---|
| 9. | FCS_CKM.3/RSA_private _enc<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 10. | FCS_CKM.3/RSA_public_ dec<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 11. | FCS_CKM.3/Session_key<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 12. | FCS_CKM.3/Key_motion _sensor<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 13. | FCS_CKM.3/RSA_private _IDD<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 14. | FCS_CKM.3/Ext_device<br>Cryptographic Key Access | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 15. | FCS_CKM.4<br>Cryptographic Key Destruction | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>**Not applicable** |

| Number | SFR | Dependencies | Support or comment |
|---|---|---|---|
| 16. | FCS_COP.1/RSA_card_cert<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 17. | FCS_COP.1/RSA_Signature<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 18. | FCS_COP.1/RSA_enc_dec<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 19. | FCS_COP.1/3-DES<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 20. | FCS_COP.1/MAC<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 21. | FCS_COP.1/3-DES_motion_sensor<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1<br>FCS_CKM.4<br>**Not applicable** |
| 22. | FCS_COP.1/RSA_IDD<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |

| Num ber | SFR | Dependencies | Support or comment |
|---|---|---|---|
| 23. | FCS_COP.1/Ext_device<br>Cryptographic Operation | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | **Not applicable (see below)** |
| 24. | FDP_ACC.2<br>Complete Access Control | FDP_ACF.1 Security attribute based access control | FDP_ACF.1 |
| 25. | FDP_ACF.1<br>Security Attribute Based Access Control | FDP_ACC.1 Subset access control required | FDP_ACC.2 |
| 26 | FDP_ITC.1<br>Import of User Data without Security Attributes | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.2<br>**Not applicable** |
| 27 | FDP_RIP.1<br>Subset Residual Information Protection | No dependencies | No dependencies |
| 28. | FDP_SDI.2<br>Stored Data Integrity Monitoring and Action | No dependencies | No dependencies |
| 29. | FIA_AFL.1/Motion_sensor<br>Authentication Failure Handling | FIA_UAU.1 Timing of authentication | FIA_UAU.1 |
| 30. | FIA_AFL.1/Card<br>Authentication Failure Handling | FIA_UAU.1 Timing of authentication | FIA_UAU.1 |
| 31. | FIA_AFL.1/Company<br>Authentication Failure Handling | FIA_UAU.1 Timing of authentication | FIA_UAU.1 |
| 32. | FIA_UAU.1<br>Timing of Authentication | FIA_UID.1 Timing of identification | FIA_UID.1 |
| 33. | FIA_UAU.3<br>Unforgeable Authentication | No dependencies | No dependencies |
| 34. | FIA_UAU.6<br>Re-authenticating | No dependencies | No dependencies |
| 35. | FIA_UID.1<br>Timing of Identification | No dependencies | No dependencies |
| 36. | FMT_MSA.1<br>Management of Security Attributes | | **SFR not applicable (see below)** |
| 37. | FMT_MSA.2<br>Secure Security Attributes | | **SFR not applicable (see below)** |
| 38. | FMT_MSA.3<br>Static Attribute Initialisation | | **SFR not applicable (see below)** |

| Num ber | SFR | Dependencies | Support or comment |
|---|---|---|---|
| 39. | FMT_MTD.1<br>Management of TSF Data | | **SFR not applicable (see below)** |
| 40. | FMT_SMR.1<br>Security Roles | | **SFR not applicable (see below)** |
| 41. | FPT_FLS.1<br>Failure with Preservation of Secure State | ADV_SPM.1 Informal TOE security policy model | ADV_SPM.1 |
| 42. | FPT_ITA.1<br>Inter-TSF availability within a defined availability metric | No dependencies | No dependencies |
| 43. | FPT_PHP.1<br>Passive detection of physical attack | No dependencies | No dependencies |
| 44. | FPT_SEP.1<br>TSF Domain Separation | No dependencies | No dependencies |
| 45. | FPT_STM.1<br>Reliable Time Stamps | No dependencies | No dependencies |
| 46. | FPT_TST.1<br>TSF Testing | FPT_AMT.1 Abstract machine testing | **Not applicable (see below)** |
| 47. | FTP_ITC.1/Motion_sensor<br>Inter-TSF trusted channel | No dependencies | No dependencies |
| 48. | FTP_ITC.1/Card<br>Inter-TSF trusted channel | No dependencies | No dependencies |
| 49. | FTP_ITC.1/Ext_device<br>Inter-TSF trusted channel | No dependencies | No dependencies |

**Table 30: Security Functional Requirements Dependencies**

Except for the components stated in the right column in bold characters and the FMT-components the table above shows that the functional component dependencies are satisfied by any functional component defined in this ST. This is explained in the following:

- The dependency of FPT_TST.1 with FPT_AMT.1 (Abstract Machine Testing) is not relevant for the EFAS-3. FPT_TST.1 is self-consistent for the TOE (hardware and software) and does not require the FPT_AMT.1 function. The TOE software is not tested inside the scope of FPT_TST.1. FPT_TST.1 is-self consistent, and FPT_AMT.1 is not applicable.
- The dependency of FCS_CKM.3/x (except /Session key and /Motion_sensor) with 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 and FCS_CKM.4 Cryptographic key destruction is not applicable as the SFRs contain the access to private/public RSAkeys all stored in the EFAS-3. Neither import nor generation nor key destruction are relevant for these public and private keys.
- The dependency of FCS_COP.1/RSA_x with 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 and FCS_CKM.4 Cryptographic key destruction is not applicable as the SFRs contain the access to private/public RSAkeys all stored in the EFAS-3. Neither import nor generation nor key destruction are relevant for this public key.

- Security attributes, roles or TSF Data, all FMT-components / are not applicable for the TOE since the TOE´s functionality as defined in the Tachograph specification [EU], Annex 1B does not require any functionality regarding the management of TOE Security Functions.

### 8.2.3 Strength of Function Level Rationale

Based on the requirements in the Tachograph specification [EU], Annex 1B main body and Appendix 10 (Vehicle Unit Generic Security Target), and under consideration of the JIL interpretations [JIL], the level for the strength of the TOE´s security functional requirements is claimed as SOF-high. Successful attack is judged beside normal feasibility. Only attackers possessing a high level of expertise, opportunity and resources may defeat the critical security mechanisms of the TOE.

### 8.2.4 Security Assurance Requirements Rationale

The assurance requirements of this ST defined in chapter 5.1.3 are summarized in the following table:

| **Assurance Requirements** | **Name** | **Type** |
|---|---|---|
| EAL4 | Methodically designed, tested and reviewed | Assurance Level / Class |
| ADO_IGS.2 | Generation Log | Higher hierarchical component |
| ADV_IMP.2 | Implementation of the TSF | Higher hierarchical component |
| ATE_DPT.2 | Testing: Low-Level Design | Higher hierarchical component |
| AVA_VLA.4 | Highly Resistant | Higher hierarchical component |

**Table 31: Security Assurance Requirements Rationale**

#### 8.2.4.1 Evaluation Assurance Level Rationale

The assurance level for the TOE is chosen as EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4. This is caused by the requirements of the Tachograph specification Tachograph specification [EU], Annex 1B main body and Appendix 10 (Vehicle Unit Generic Security Target) regarding the TOE evaluation level and under consideration of the JIL interpretations [JIL], chapter 2.2 and Annex A.

Within this evaluation all assurance components will be used as defined in CC Part 2 [CC2] and CC Part 3 [CC3] with the refinements as referred in the JIL interpretations [JIL], Annex A.3 and A.5 (refer to chapter 5.1.4 of this ST). An assurance level comparable to the evaluation level ITSEC E3 high is provided by the chosen CC assurance components for the TOE inclusive the chosen augmentations and refinements.

The evaluation assurance level of EAL4 augmented is selected for the TOE since this level provides a suitable and reasonable level of assurance for the TOE, with regard to the TOE´s security and resistance against attacks with high attack potential in its operational use as well as to the security of the development process of the TOE. To guarantee for a sufficiently secure product, the evaluators have access to the low level design, hardware design documents and source code. The chosen assurance level admits the developer to reach maximum assurance from security analysis based on best commercial practices. Thereby a sufficiently high practical level of assurance expected for the security product is reached.

#### 8.2.4.2 Assurance Augmentations Rationale

Since the assurance components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4 are chosen with respect to the requirements in the JIL interpretations [JIL], Annex A.3 and A.5 in order to achieve a CC assurance level comparable to ITSEC E3 high as required in the Tachograph specification [EU], Annex 1B main body and Appendix 10 (Vehicle Unit Generic Security Target) no additional rationale is given in this Security Target.

### 8.2.5 Security Assurance Requirements Dependencies

The security assurance requirements specified by this Security Target are drawn from the assurance class EAL4 with its augmentation by the higher hierarchical components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4.

EAL4 is a set of assurance components for which all dependencies are satisfied. For the components of the augmentation in the following it is shown that all further dependencies resulting from the augmentation are satisfied:

- ADO_IGS.2 has a dependency with AGD_ADM.1. This dependency is satisfied by EAL4.
- ADV_IMP.2 has dependencies with ADV_LLD.1, ADV_RCR.1, ALC_TAT.1. These components are included in EAL4, and so these dependencies are satisfied.
- ATE_DPT.2 has dependencies with ADV_HLD.2, ADV_LLD.1 and ATE_FUN.1. All these dependencies are satisfied by EAL4.
- AVA_VLA.4 has dependencies with ADV_FSP.1, ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, AGD_ADM.1 and AGD_USR.1. All these dependencies are satisfied by EAL4.

### 8.2.6 Security Requirements - Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security assurance requirements (SARs) and the security functional requirements (SFRs) is consistent and that requirements support each other if necessary. Regarding consistency and mutual support the analysis of the TOE´s security requirements shows:

- The assurance class EAL4 is an established set of assurance requirements meeting mutual support and consistency.
- The dependency analysis for the additional assurance components in chapter 8.2.5 shows that the assurance requirements meet consistency and mutual support since no inconsistencies appear and all (additional) dependencies are met.
- The dependency analysis in chapter 0 for the security functional requirements of the TOE resulting from the EU Tachograph Specification [EU], Annex 1B, Appendix 10 (Vehicle Unit Generic Security Target) shows that between all defined functional requirements mutual support and internal consistency is met. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are suitably explained. The SFRs do not lead to any inconsistency or any weakness as can be seen from the explanations in chapter 8.2.1.
- The mutual support and internal consistency of the functional requirements is shown for the TOE relevant SFRs in chapter 8.2.1.
- All operations conducted on the CC functional components lead to a consistent and reasonable ensemble. The following has to be noted:
  - All operations on the chosen SFRs are performed considering the requirements in the Tachograph specification [EU], Annex 1B, Appendix 10 (Vehicle Unit Generic Security Target).
  - For the SC relevant SFRs the evidence is done within the scope of the CC evaluation of the SC resp. in the correlated ST [ATMEL_ST].
  - Iteration operations: The iteration of the functional components for cryptographic support, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 and FCS_COP.1, are necessary to differentiate between the different cryptographic algorithms and mechanisms of the TOE. The iteration of the functional component FIA_AFL.1 is necessary to differentiate between the different authentication mechanisms of the TOE. The iteration of the functional component FTP_ITC.1 is necessary to differentiate between the different remote trusted products motion sensor, tachograph card and external device.
  - Assignment and selection operations: All assignment and selection operations are conducted in such a way that they build an internally consistent security system and do

not contradict each other reflecting the security requirements of the Tachograph system as specified in the Tachograph specification [EU], Annex 1B. This concerns in particular the defined access control policy AC_SFP.

- Refinement operations are not conducted.

- Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies which are not met. In chapter 0 it is shown that this does not arise. Additionally as discussed in chapter 8.2.4, the chosen assurance components are suitable for the TOE functionality. Therefore there are not inconsistencies between security functional requirements the assurance requirements and these two sets support each other.

## 8.3 TOE Summary Specification Rationale

According to the requirements of Common Criteria, CC Part 1 [CC1] and CC Part 3 [CC3], the TOE summary specification rationale shows that the TOE security functions (TSFs) and assurance measures are suitable to meet the TOE security requirements. The following will be shown:

- The strength of the TOE function claims are valid, or assertions that such claims are unnecessary are valid.
- The combination of the specified TOE´s IT security functions cooperate whereby TOE security functional requirements are met.
- The claim that the stated assurance measures are compliant with the assurance requirements is reasoned.

### 8.3.1 Security Functions Rationale

The SFRs for the SC of chap. 5 are related to the TSFs of the SC refered in chap. 6. The mapping of the SFRs for the SC to the relevant TSFs is done within the CC evaluation of the SC resp. within the associated Security Target [ATMEL_ST].

The following section demonstrates that the set and combination of the defined TOE security functions (TSFs) is suitable to satisfy the identified TOE security functional requirements (SFRs). Furthermore, this section shows that each of the TSFs is related to at least one security functional requirement.

The SFRs for the TOE of chapter 5.1.1 are related to the TSFs of the TOE defined in chapter 6.1. The mapping of the SFRs for the TOE to the relevant TSFs is done in the following (compare the compliance with the generic security target, chapter 6.4).

The tables below give an overview of which TSFs of the TOE contribute to the satisfaction of the SFRs for the TOE.

| **Security Functional Requirements** | **TOE Security Functions** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | F.ACS | F.SECAUDIT | F.IA_KEY | F.DATA_INT | F.EX_CONF | F.EX_INT | F.INF_PROT | F.FAIL_PROT | F.SELFTEST | F.GEN_SKEYS | F.GEN_DIGSIG | F.VER_DIGSIG |
| FAU_GEN.1 | | X | | | | | | | | | | |
| FAU_SAA.1 | | X | | | | | | | | | | |
| FCO_NRO.1 | X | | | | | | | | | | X | |
| FCS_CKM.1 | | | X | | | | | | | X | | |
| FCS_CKM.2/Session_key | X | | X | | | | | | | X | X | X |

| **Security Functional Requirements** | **TOE Security Functions** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | F.ACS | F.SECAUDIT | F.IA_KEY | F.DATA_INT | F.EX_CONF | F.EX_INT | F.INF_PROT | F.FAIL_PROT | F.SELFTEST | F.GEN_SKEYS | F.GEN_DIGSIG | F.VER_DIGSIG |
| FCS_CKM.2/RSA_cert | X | | X | | | | | | | | | X |
| FCS_CKM.3/RSA_private_sig | X | | | | | | | | | | | |
| FCS_CKM.3/RSA_public_sig | X | | | | | | | | | | | |
| FCS_CKM.3/RSA_private_enc | X | | | | | | | | | | | |
| FCS_CKM.3/RSA_public_dec | X | | | | | | | | | | | |
| FCS_CKM.3/Session_key | X | | | | | | | | | | | |
| FCS_CKM.3/Key_motion_sensor | X | | | | | | | | | | | |
| FCS_CKM.3/RSA_private_IDD | X | | | | | | | | | | | |
| FCS_CKM.3/Ext_device | X | | | | | | | | | | | |
| FCS_CKM.4 | | | | | | | X | | | | | |
| FCS_COP.1/RSA_card_cert | X | | | | | | | | | | | X |
| FCS_COP.1/RSA_Signature | X | | | | | | | | | | X | X |
| FCS_COP.1/RSA_enc_dec | X | | | | | | | | | | X | X |
| FCS_COP.1/3-DES | X | | | | X | | | | | | | |
| FCS_COP.1/MAC | X | | | | | X | | | | | | |
| FCS_COP.1/3-DES_motion_sensor | X | | | | X | X | | | | | | |
| FCS_COP.1/RSA_IDD | X | | | | | X | | | | | | |
| FCS_COP.1/Ext_device | X | | | | | X | | | | | | |
| FDP_ACC.2 | X | | | | | | | | | | | |
| FDP_ACF.1 | X | | | | | | | | | | | |
| FDP_ITC.1 | X | | | | X | X | | | | | | |
| FDP_RIP.1 | | | | | | | X | | | | | |
| FDP_SDI.2 | X | | | X | | | | | | | | |
| FIA_AFL.1/Motion_sensor | | | X | | | | | | | | | |
| FIA_AFL.1/Card | | | X | | | | | | | | | |
| FIA_AFL.1/Company | | | X | | | | | | | | | |
| FIA_UAU.1 | | | X | | | | | | | | | |
| FIA_UAU.3 | | | X | | | | | | | | | |
| FIA_UAU.6 | | | X | | | | | | | | | |
| FIA_UID.1 | | | X | | | | | | | | | |
| FPT_FLS.1 | | | | | | | | X | | | | |
| FPT_ITA.1 | X | | | | | | | | | | | |
| FPT_PHP.1 | | | | | | | | X | | | | |
| FPT_SEP.1 | X | | | | | | | | | | | |

| Security Functional Requirements | TOE Security Functions | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | F.ACS | F.SECAUDIT | F.IA_KEY | F.DATA_INT | F.EX_CONF | F.EX_INT | F.INF_PROT | F.FAIL_PROT | F.SELFTEST | F.GEN_SKEYS | F.GEN_DIGSIG | F.VER_DIGSIG |
| FPT_STM.1 | | X | | | | | | | | | | |
| FPT_TST.1 | | | | | | | | | X | | | |
| FTP_ITC.1/Motion_sensor | | | X | | | X | | | | | | |
| FTP_ITC.1/Card | | | X | | | X | | | | | | |
| FTP_ITC.1/Ext_device | | | X | | X | X | | | | | | |

**Table 32: Security Functions Rationale**

In the following, for each SFR of the TOE it will be explained why and how the TSFs listed in the preceding tables meet the respective SFR.

### FAU_GEN.1

The TSF F.SECAUDIT meets FAU_GEN.1 as it implements exactly the SFR. In particular the TSF generates audit records as specified by the SFR.

### FAU_SAA.1

The TSF F.SECAUDIT meets FAU_SAA.1 as it implements exactly the SFR. In particular the TSF applies the set of rules in monitoring the audited events, based upon these rules indicates a potential violation of the TSF and enforces the rules specified in the SFR for monitoring audited events.

### FCO_NRO.1

The TSF F.GEN_DIGSIG realizes the generation of evidence of origin of the respective data as required in the SFR FCO_NRO.1. Hereby, the TSF F.ACS, which implements the security function policy AC_SFP, ensures the connection and access to the required unique private signature key.

### FCS_CKM.1

The generation of session keys used for securing the following data exchange is part of the TSFs F.IA_KEY and F.GEN_SKEYS and is carried out according to the requirements of the SFR FCS_CKM.1. In particular these TSF implement the generation of session keys for the communication with the tachograph card as for the communication with the motion sensor.

### FCS_CKM.2/Session_key

The distribution of session keys within the mutual authentication process between the TOE and the tachograph card, between the TOE and the motion sensor resp. between the TOE and external device is in the responsibility of the TSF F.IA_KEY and is carried out according to the requirements of the SFR FCS_CKM.2/Session_key. For the mutual authentication process between the tachograph card and the EFAS-3, the TSFs F.GEN_DIGSIG, F.VER_DIGSIG and F.GEN_SKEYS perform the basic cryptographic operations within the mutual authentication process including the export of cryptographic certificates. The import of cryptographic certificates is implemented by the TSF F.VER_DIG. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP.

### FCS_CKM.2/RSA_cert

The distribution of public keys within the mutual authentication process between EFAS-3 and the tachograph card is realised by the TSF F.IA_KEY and is carried out according to the requirements of the SFR FCS_CKM.2/RSA_cert. Public keys are imported respective exported via certificates requiring the verification of the certificates during the mutual authentication process. The verification of certificates by EFAS-3 during the import of public keys is supported by F.VER_DIGSIG.

**FCS_CKM.3/***

The TSF F.ACS meets the SFRs FCS_CKM.3/* as it implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_CKM.4**

The TSF F.INF_PROT meets the SFR FCS_CKM.4 as it implements the memory preparation upon the allocation of resources whereby it ensures that any previous information content is no longer available. This concerns in particular the erasing of all volatile and non-volatile memories used for processing cryptographic keys or key related material.

**FCS_COP.1/RSA_card_cert**

The TSFs F F.VER_DIGSIG responsible for the verification of digital signatures of certificates realise the SFR FCS_COP.1/RSA_card_cert . The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policy AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/RSA_Signature**

The TSFs F.GEN_DIGSIG and F.VER_DIGSIG responsible for the generation respective verification of digital signatures realise the SFR FCS_COP.1/RSA_Signature. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/RSA_enc_dec**

The TSFs F.GEN_DIGSIG and F.VER_DIGSIG providing the additional functionality for asymmetric decryption respective encryption realise the SFR FCS_COP.1/RSA_enc_dec. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/3-DES**

The TSF F.EX_CONF responsible for securing the data exchange between tachograph card an EFAS-3 with respect to confidentiality realises the SFR FCS_COP.1/3-DES. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/MAC**

The TSF F.EX_INT responsible for securing the data exchange between tachograph card and EFAS-3 with respect to integrity realises the SFR FCS_COP.1/MAC. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/3-DES_motion_sensor**

The TSFs F.EX_CONF and F.EX_INT responsible for securing the data exchange between motion sensor and EFAS-3 with respect to confidentiality and integrity realise the SFR FCS_COP.1/3-DES_motion_sensor. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

**FCS_COP.1/RSA_IDD**

The TSF F.EX_INT responsible for securing the data exchange from EFAS-3 to a dedicated intelligent equipment with respect to authenticity and integrity realises the SFR FCS_COP.1/RSA_IDD. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

### FCS_COP.1/Ext_device

The TSF F.EX_INT responsible for securing the data exchange from management device to EFAS-3 with respect to authenticity and integrity realises the SFR FCS_COP.1/Ext_device. The access to the relevant keys is regulated by the TSF F.ACS which implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

### FDP_ACC.2, FDP_ACF.1

The TSF F.ACS contributes directly to the SFRs FDP_ACC.2 and FDP_ACF.1 as it implements the security function policies AC_SFP as defined in chapter 5.1.1.1.

### FDP_ITC.1

The TSFs F.ACS, F.EX_INT and F.EX_CONF implements the SFR FDP_ITC.1 as they implement the security function policies AC_SFP as defined in chapter 5.1.1.1 and realise the requirement of data import.

### FDP_RIP.1

The TSF F.INF_PROT contributes directly to the SFR FDP_RIP.1 as it implements the memory preparation upon the allocation of the respective resource whereby it ensures that any previous information content is no longer available. This concerns all volatile and non-volatile memories used for processing security relevant material.

### FDP_SDI.2

The TSF F.DATA_INT contributes directly to the SFR FDP_SDI.2 as it realizes the monitoring of stored data for integrity errors. Additionally F.ACS supports the monitoring of stored data for integrity errors if the data is security with a cryptographic signature.

### FIA_AFL.1/Motion_sensor, FIA_AFL.1/Card, FIA_AFL.1/Company

The TSF F.IA_KEY realises the key based authentication mechanisms of the TOE and is particularly responsible for the handling of authentication failures as required in the SFRs FIA_AFL1/Motion_sensor, FIA_AFL.1/Card and FIA_AFL.1/Company.

### FIA_UAU.1

The TSF F.IA_KEY meets directly the SFR FIA_UAU.1 as it implements directly the SFRs.

### FIA_UAU.3

The TSF F.IA_KEY meets the SFR FIA_UAU.3 since it implements the key based authentication mechanism of the TOE which operates particularly authentication data as required in the SFR FIA_UAU.3.

### FIA_UAU.6

The TSF F.IA_KEY meets the SFR FIA_UAU.6 since it implements the re-identification and re-authentication as required in the SFR FIA_UAU.6.

### FIA_UID.1

The TSF F.IA_KEY meets the SFR FIA_UID.1 since it implements the management of identity as required in the SFR FIA_UID.1.

### FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1

Not applicable.

### FPT_FLS.1

The TSF F.FAIL_PROT implements features to preserve a secure operation state of the TOE in case of induced failures or tampering. It satisfies directly the requirements of the SFR FPT_FLS.1-1.

**FPT_ITA.1**

The TSF F.ACS meets the SFR FPT_ITA.1 since it implements the data availability requirements as required in the SFR FPT_ITA.1.

**FPT_PHP.1**

The TSF F.FAIL_PROT meets the SFR FPT_PHP.1 since it implements the physical protection as required in the SFR FPT_PHP.1.

**FPT_SEP.1**

The TSF F.ACS meets the SFR FPT_SEP.1 since it implements the reliability of software and multiple application requirements as required in the SFR FPT_SEP.1.

**FPT_STM.1**

The TSF F.SECAUDIT meets the SFR FPT_STM.1.1 since it implements the time stamp as required in the SFR FPT_STM.1.

**FPT_TST.1**

The TSF F.SELFTEST meets the SFR FPT_TST.1 since it implements the self test as required in the SFR FPT_TST.1.

**FTP_ITC.1/Motion_sensor**

The TSF F.EX_INT meets the SFR FTP_ITC.1/Motion_sensor since it implements the data import and export for motion sensor with help of the TSF F.IA_KEY as required in the SFR FTP_ITC.1/Motion_sensor.

**FTP_ITC.1/Card**

The TSF F.EX_INT meets the SFR FTP_ITC.1/Card since it implements the data import and export for tachograph card with help of the TSF F.IA_KEY as required in the SFR FTP_ITC.1/Card.

**FTP_ITC.1/Ext_device**

The TSF F.EX_INT meets the SFR FTP_ITC.1/Ext_device since it implements the secure data import and export for external device with help of the TSF F.IA_KEY as required in the SFR FTP_ITC.1/Ext_device.

### 8.3.2 Assurance Measures Rationale

The assurance measures of the developer as referred in chapter 6.3 are suitable and sufficient to meet the CC assurance level EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4 as claimed in chapter 5.1.3. In particular the deliverables listed in chapter 6.3 are suitable and sufficient to document that the assurance requirements are met.

### 8.3.3 TOE Security Functions - Mutual Support and Internal Consistency

The detailed specification and analysis of the TOE Security Functions in chapter 6.1 demonstrate how the defined functions cooperate and support each other. Furthermore, this description shows that no inconsistencies exist. This result is supported by chapter 8.3.1.

### 8.3.4 Strength of Functions

As the TOE is considered as a security product with critical security mechanisms which shall be resistant against attacks with high attack potential, the chosen SOF level for the TOE´s security functions of SOF-high is consistent with the security objectives for the TOE.

# 9 Annex

## 9.1 Glossary and list of acronyms

| | |
|---|---|
| A.x | Assumption |
| CC | Common Criteria |
| EAL | Evaluation Assurance Level |
| EEPROM | Multiple programmable ROM memory with byte erase. |
| F.x | Security Function |
| Flash | Multiple programmable ROM memory with sector erase. |
| ITSEC | Information Technology Security Evaluation Criteria |
| JIL | Joint Interpretation Library |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| MC | Main Controller |
| O.x | Security Objective of the TOE |
| OE.x | Security Objective of the Environment |
| OS | Operating System |
| PIN | Personal Identification Number |
| RAM | Random Access Memory (loses data if detached from a power supply) |
| ROM | Read Only Memory (stores data independent of a power supply) |
| RSA | Rivest-Shamir-Adleman AlgorithmSAR Security Assurance Requirement |
| RTC | Real time clock |
| SC | Security Controller |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SOF | Strength of Functions |
| SPM | TOE Security Policy Model |
| ST | Security Target |
| T.x | Threat |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |
| VU | Vehicle Unit |

## 9.2 Bibliography

[EU] Annex 1B of Commission Regulation (EC) No.1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, L 207 / 1 ff.), Commission of the European Communities, 05.08.2002.
*corrected by*
Corrigendum in Official Journal of the European Communities L 77, 13.3.2004, p.71–86 (EN):
Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport (Official Journal of the European Communities L 207 of 5 August 2002)

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

[CM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005

[CC1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model, Version 2.3, August 2005

[CC2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements, Version 2.3, August 2005

[CC3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements, Version 2.3, August 2005

[ATMEL_ST] Longbow Security Target, Version 1.3, ATMEL, 3.8.2006

## 9.3 Extracts from the EU Commission Regulation

This chapter contains some statements from the EU Commission Regulation which are referenced in this ST.

050a Upon driver (or workshop) card insertion, and only at this time, the recording equipment shall:

> - remind the cardholder the date and time of his last card withdrawal, and
>
> - ask the cardholder to identify if the current insertion of the card represents a continuation of the current daily work period.

The recording equipment shall allow the cardholder to disregard the question without answering, or to answer positively, or to answer negatively:

- in the case where the cardholder disregards the question, the recording equipment shall prompt the cardholder for a place where the daily work period begins.. The recording equipment shall allow this request to be disregarded. If a location is entered, then it shall be recorded, in the data memory and in the tachograph card, and related to the card insertion time,

- in the case of a negative or positive answer, the recording equipment shall invite the cardholder to enter activities manually, with their dates and times of beginning and end, among WORK, AVAILABILITY, or BREAK/REST only, strictly included within the period last card withdrawal . current insertion only, and without allowing such activities to overlap mutually. This shall be done in accordance with the following procedures:

> - in the case where the cardholder answers positively to the question, the recording equipment shall invite the cardholder to enter activities manually, in chronological order, for the period last

card withdrawal - current insertion. The process shall end when the end time of a manually entered activity equals the card insertion time.

- in the case where the cardholder answers negatively to the question, the recording equipment shall:

  - invite the card holder to enter manually activities in chronological order from the card withdrawal time up to the time of end of the related daily work period (or of the activities related to that vehicle in the case where the daily work period continues on a record sheet). The recording equipment shall therefore, before allowing the cardholder to enter manually each activity, invite the cardholder to identify if the time of end of the last recorded activity represents the end of a previous work period (see note below),

  Notes: in the case where the cardholder fails to declare when the previous work period ended, and manually enters an activity of which end time equals the card insertion time, the recording equipment shall:

    - assume that the daily work period ended at the start of the first REST (or remaining UNKNOWN) period after card withdrawal or at the time of card withdrawal if no rest period has been entered (and if no period remains UNKNOWN),

    - assume that the start time (see below) equals the card insertion time,

    - proceed through the steps below;

  - then, if the time of end of the related work period is different from the time of card withdrawal, or if no place of end of daily work period had been entered at that time, prompt the cardholder to .confirm or enter the place where the daily work period ended. (the recording equipment shall allow this request to be disregarded). If a location is entered, it shall be recorded in the tachograph card only and only if different from the one entered at card withdrawal (if one was entered), and related to the time of end of the work period,

  - then invite the cardholder to .enter a start time. of the current daily work period (or of the activities related to the current vehicle in the case where the card holder previously used a record sheet during this period), and prompt the cardholder for a .place where the daily work period begins. (the recording equipment shall allow this request to be disregarded). If a location is entered, it shall be recorded in the tachograph card and related to this start time. If this start time is equal to the card insertion time, the location shall also be recorded in the data memory,

  - then, if this start time is different from the card insertion time, invite the cardholder to enter manually activities in chronological order from this start time up to the time of card insertion. The process shall end when the end time of a manually entered activity equals the card insertion time,

- the recording equipment shall then allow the card holder to modify any activity manually entered, until validation by selection of a specific command, and thereafter forbid any such modification,

- such answers to the initial question followed by no activity entries, shall be interpreted by the recording equipment as if the cardholder had disregarded the question.

During this whole process, the recording equipment shall wait for entries no longer than the following time-outs:

- if no interaction with the equipment's human machine interface is happening during one minute (with a visual, and possibly audible, warning after 30 seconds) or,

- if the card is withdrawn or another driver (or workshop) card is inserted or,

- as soon as the vehicle is moving,

in this case the recording equipment shall validate any entries already made.

081 For each insertion and withdrawal cycle of a driver or workshop card in the equipment, the recording equipment shall record and store in its data memory:

- the card holder's surname and first name(s) as stored in the card,
- the card's number, issuing Member State and expiry date as stored in the card,
- the insertion date and time,
- the vehicle odometer value at card insertion,
- the slot in which the card is inserted,
- the withdrawal date and time,
- the vehicle odometer value at card withdrawal,
- the following information about the previous vehicle used by the driver, as stored in the card:
    - VRN and registering Member State,
    - card withdrawal date and time,
- a flag indicating whether, at card insertion, the card holder has manually entered activities or not.

082 The data memory shall be able to hold these data for at least 365 days.

083 When storage capacity is exhausted, new data shall replace oldest data.

084 The recording equipment shall record and store in its data memory whenever there is a change of activity for the driver and/or the co-driver, and/or whenever there is a change of driving status, and/or whenever there is an insertion or withdrawal of a driver or workshop card:

- the driving status (CREW, SINGLE),
- the slot (DRIVER, CO-DRIVER),
- the card status in the relevant slot (INSERTED, NOT INSERTED) (see Note),
- the activity (DRIVING, AVAILABILITY, WORK, BREAK/REST),
- the date and time of the change.

Note: INSERTED means that a valid driver or workshop card is inserted in the slot. NOT INSERTED means the opposite, i.e. no valid driver or workshop card is inserted in the slot (e.g. a company card is inserted or no card is inserted).

Note: Activity data manually entered by a driver are not recorded in the data memory.

085 The data memory shall be able to hold driver activity data for at least 365 days.

086 When storage capacity is exhausted, new data shall replace oldest data.

087 The recording equipment shall record and store in its data memory whenever a (co-)driver enters the place where a daily work period begins and/or ends:

- if applicable, the (co-)driver card number and card issuing Member State,
- the date and time of the entry (or the date/time related to the entry when the entry is made during the manual entry procedure),
- the type of entry (begin or end, condition of entry),
- the country and region entered,
- the vehicle odometer value.

088 The data memory shall be able to hold daily work periods start and/or end data for at least 365 days (with the assumption that one driver enters two records per day).

089 When storage capacity is exhausted, new data shall replace oldest data.

090 The recording equipment shall record in its data memory the vehicle odometer value and the corresponding date at midnight every calendar day.

091 The data memory shall be able to store midnight odometer values for at least 365 calendar days.

092 When storage capacity is exhausted, new data shall replace oldest data.

093 The recording equipment shall record and store in its data memory the instantaneous speed of the vehicle and the corresponding date and time at every second of at least the last 24 hours that the vehicle has been moving.

094 The recording equipment shall record and store in its data memory the following data for each event detected according to the following storage rules:

| Event | Storage rules | Data to be recorded per event |
|---|---|---|
| Card conflict | - the 10 most recent events. | - date and time of beginning of event,<br>- date and time of end of event,<br>- cards' type, number and issuing Member State of the two cards creating the conflict. |
| Driving without an appropriate card | - the longest event for each of the 10 last days of occurrence,<br>- the five longest events over the last 365 days. | - date and time of beginning of event,<br>- date and time of end of event,<br>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,<br>- number of similar events that day. |
| Card insertion while driving | - the last event for each of the 10 last days of occurrence. | - date and time of the event,<br>- card's type, number and issuing Member State,<br>- number of similar events that day. |
| Last card session not correctly closed | - the 10 most recent events. | - date and time of card insertion,<br>- card's type, number and issuing Member State,<br>- last session data as read from the card:<br>- date and time of card insertion,<br>- VRN and Member State of registration. |
| Over speeding | - the most serious event foreach of the 10 last days of occurrence (i.e. the one with the highest average speed),<br>- the five most serious events over the last 365 days.<br>- the first event having occurred | - date and time of beginning of event,<br>- date and time of end of event,<br>- maximum speed measured during the event,<br>- arithmetic average speed |

| | | |
|---|---|---|
| | after the last calibration. | measured during the event,<br>- card's type, number and issuing Member State of the driver (if applicable),<br>- number of similar events that day. |
| Power supply interruption | - the longest event for each of the 10 last days of occurrence,<br>-  the five longest events over the last 365 days. | - date and time of beginning of event,<br>- date and time of end of event,<br>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,<br>- number of similar events that day. |
| Motion data error | - the longest event for each of the 10 last days of occurrence,<br>- the five longest events over the last 365 days. | - date and time of beginning of event,<br>- date and time of end of event,<br>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,<br>- number of similar events that day. |
| Security breach attempt | - the 10 most recent events per type of event. | - date and time of beginning of event,<br>- date and time of end of event (if relevant),<br>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,<br>- type of event. |

096 The recording equipment shall attempt to record and store in its data memory the following data for each fault detected according to the following storage rules:

| Fault | Storage rules | Data to be recorded per fault |
|---|---|---|
| Card fault | - the 10 most recent driver card faults.. | - date and time of beginning of fault,<br>- date and time of end of fault,<br>- card's type number and issuing Member State. |
| Recording equipment faults | - the 10 most recent faults for each type of fault,<br>- the first fault after the last calibration. | - date and time of beginning of fault,<br>- date and time of end of fault,<br>- type of fault,<br>- cards' type, number and |

| | | |
|---|---|---|
| | | issuing Member State of any card inserted at beginning and/or end of the fault. |

102 The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent control activities:

- date and time of the control,

- control card number and card issuing Member State,

- type of the control (displaying and/or printing and/or VU downloading and/or card downloading).

103 In case of downloading, the dates of the oldest and of the most recent days downloaded shall also be recorded.

104 The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent company locks:

- lock-in date and time,

- lock-out date and time,

- company card number and card issuing Member State,

- company name and address.

105 The recording equipment shall record and store in its data memory the following data relevant to the last data memory downloading to external media while in company or in calibration mode:

- date and time of downloading,

- company or workshop card number and card issuing Member State,

- company or workshop name.

105a The recording equipment shall record in its data memory the following data relevant to specific conditions:

-date and time of the entry,

- type of specific condition.

105b The data memory shall be able to hold specific conditions data for at least 365 days (with the assumption that on average, one condition is opened and closed per day). When storage capacity is exhausted, new data shall replace oldest data.

109 The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder.

109a The recording equipment shall update driver activity and location data stored on valid driver and/or workshop cards, with activity and location data manually entered by the cardholder.