INTELLIC

Security Target EFAS-4.0

name of project:	EFAS-4
file name:	1030-100-SEC-EN18_APPR_SecurityTargetEFAS-4.doc
version:	18
number of document:	1030-100-SEC-EN18
rendered by/at:	Dr. Horst Kießling / 25.08.2010
last edited by/at:	Dr. Horst Kießling / 10.11.2011
status:	released
location:	project folder and net file: Z:_EFAS-4_1030\Zulassung\Security\EigeneDokumente\SecurityTarget\ 1030-100-SEC-EN18_APPR_SecurityTargetEFAS-4.doc

	Name (in block letters):	date:	signature:
prepared by:	Dr. Horst Kießling	10.11.2011	
reviewed by:	Bernd Hoeppener	10.11.2011	
approved by:	Simon Veselsky	10.11.2011	

Release notes:

version	date	page	chapter	changes, notes	modified by	number of pages
00	2010-08-25	all	all	Initial version	Dr. Horst Kießling	43
	2010-08-25	all	all	Adapted suggestions from Bernd Hoeppener and Dr. Bernd Rose	Dr. Horst Kießling	42
	2010-08-26	all	9.3.1	added reasoning for SFR-TSF mapping	Dr. Horst Kießling	49
	2010-08-27	all	-	formal corrections	Dr. B. Rose	49
01	2010-08-31	all	all	integrated all pp SFSs with ST, enhanced rationale by SW-Update TSFs, amended reasoning	Dr. Horst Kießling	71
02	2010-09-01	all	all	Made corrections with respect to review comments	Dr. Horst Kießling	72
03	2010-10-28	all	all	Editorial changes, added tables and sections from the PP, added additional assets for SW-update	Dr. Horst Kießling	101
04	2010-11-04	all	all	Some formal corrections after review	Dr. Bernd Rose	101
05	2010-11-09	all	all	Editorial changes and formal amendments	Dr. Horst Kießling	102
06	2010-11-23	all	all	Added reference to SW-Update, editorial changes	Dr. Horst Kießling	102
10	2010-12-02	all	all	SFR operations, Added Statement of Compatibility	Dr. Horst Kießling	110
11	2011-02-24	all	all	Changes on requests of certification body and evaluation facility	Dr. Horst Kießling	127
12	2011-03-01	all	all	Software Update mechanism (AES)	Dr. Horst Kießling	117
13	2011-05-24	88	9.1.8	Integrity Mechanism MAC-storage-location	Dr. Horst Kießling	118
14	2011-10-06	all	all	Changes due to BSI comments	Dr. Horst Kießling	117
15	2011-10-24	all	all	SC-Processor more precisely specified	Dr. Horst Kießling	117
16	2011-11-07	all	all	Minor corrections on SFR operations Minor corrections on SF.UPDATE	Dr. Horst Kießling	117
17	2011-11-07	49, 52	8.1.5.1	SFRs FDP_ACC.1/SW-Upgrade, FDP_ACF.1/SW-Upgrade corrected	Dr. Horst Kießling	117

18	2011-11-10	14	3.2	Bluetooth interface does not exist	Dr. Horst Kießling	118

Table of Contents

1 SCOPE 8

2 ST INTRODUCTION (ASE_INT) 8

2.1 ST REFERENCE 8
2.2 TOE REFERENCE 8
2.3 TOE OVERVIEW 9
2.3.1 TOE Definition and Operational Usage 9
2.3.2 TOE Major Security Features for Operational Use 10
2.3.3 TOE Type 11
2.3.4 Non-TOE hardware/software/firmware 12

3 TOE DESCRIPTION 14

3.1 ARCHITECTURE OVERVIEW 14
3.2 TOE HARDWARE 14
3.3 TOE SOFTWARE 16
3.4 DETAILS OF SECURITY MECHANISMS 16
3.5 TOE PRODUCT SCOPE 17
3.6 TOE ENVIRONMENT 17
3.6.1 Development Environment 17
3.6.2 Manufacturing Environment 17
3.6.3 Fitters and Workshop Environment 18
3.6.4 End User Environment 18

4 CONFORMANCE CLAIMS 19

4.1 CC CONFORMANCE CLAIMS 19
4.2 PP CLAIM 19
4.3 PACKAGE CLAIM 19
4.4 CONFORMANCE RATIONALE 19

5 SECURITY PROBLEM DEFINITION 20

5.1 INTRODUCTION 20
5.2 THREATS 24
5.3 ORGANISATIONAL SECURITY POLICIES 25
5.4 ASSUMPTIONS 27

6 SECURITY OBJECTIVES 29

6.1 SECURITY OBJECTIVES FOR THE TOE 29
6.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 30
6.3 SECURITY OBJECTIVE RATIONALE 33

7 EXTENDED COMPONENTS DEFINITION 37

8 SECURITY REQUIREMENTS 38

8.1 SECURITY FUNCTIONAL REQUIREMENTS 38
8.1.1 Overview 39
8.1.2 Class FAU Security Audit 43
8.1.2.1 FAU_GEN Security audit data generation 43
8.1.2.2 FAU_SAR Security audit review 43
8.1.2.3 FAU_STG Security audit event storage 44
8.1.3 Class FCO Communication 44
8.1.3.1 FCO_NRO Non-repudiation of origin 44
8.1.4 Class FCS Cryptographic Support 45
8.1.4.1 FCS_CKM Cryptographic key management 45
8.1.4.2 FCS_COP Cryptographic operation 48
8.1.5 Class FDP User Data Protection 49
8.1.5.1 FDP_ACC Access control policy 49
8.1.5.2 FDP_ACF Access control functions 51

8.1.5.3 FDP_ETC Export from the TOE 54
8.1.5.4 FDP_ITC Import from outside of the TOE 54
8.1.5.5 FDP_RIP Residual information protection 56
8.1.5.6 FDP_SDI Stored data integrity 57
8.1.6 Class FIA Identification and Authentication 57
8.1.6.1 FIA_AFL Authentication failures 57
8.1.6.2 FIA_ATD User attribute definition 58
8.1.6.3 FIA_UAU User authentication 59
8.1.6.4 FIA_UID User identification 61
8.1.7 Class FPR Privacy 61
8.1.7.1 FPR_UNO Unobservability 61
'To observe the cryptographic operations' means here 'using any TOE external interface in order to gain the values of cryptographic keys which shall be kept secret'. 61
8.1.8 Class FPT Protection of the TSF 62
8.1.8.1 FPT_FLS Fail secure 62
8.1.8.2 FPT_PHP TSF physical protection 62
8.1.8.3 FPT_STM Time stamps 63
8.1.8.4 FPT_TDC Inter-TSF TSF Data Consistency 63
8.1.8.5 FPT_TST TSF self test 63
8.1.9 Class FRU Resource Utilisation 64
8.1.9.1 FRU_PRS Priority of service 64
8.1.10 Class FMT Security Management 64
8.1.10.1 FMT_MSA Management of security attributes 64
8.1.10.2 FMT_MOF Management of functions in TSF 66
8.1.10.3 FMT_SMF Specification of Management Functions 66
8.1.10.4 FMT_SMR Security management roles 66
8.2 SECURITY ASSURANCE REQUIREMENTS 67
8.3 SECURITY REQUIREMENTS RATIONALE 68
8.3.1 Security Functional Requirements Rationale 68
8.3.2 Rationale for SFR's Dependencies 71
8.3.3 Security Assurance Requirements Rationale 71
8.3.4 Security Requirements – Internal Consistency 71
8.3.4.1 SFRs 71
8.3.4.2 SARs 71

9 TOE SUMMARY SPECIFICATION 71

9.1 TOE SECURITY FUNCTIONS 71
9.1.1 SF.ACS Security Attribute Based Access Control 71
9.1.2 SF.SECAUDIT Audit 71
9.1.3 SF.EX_CONF Confidentiality of Data Exchange 71
9.1.4 SF.EX_INT Integrity and Authenticity of Data Exchange 71
9.1.5 SF.GEN_SKEYS Generation of Session Keys 71
9.1.6 SF.GEN_DIGSIG Generation of Digital Signatures optionally with Encryption 71
9.1.7 SF.VER_DIGSIG Verification of Digital Signatures optionally with Decryption 71
9.1.8 SF.DATA_INT Stored Data Integrity Monitoring and Action 71
9.1.9 SF.IA_KEY Key Based User / TOE Authentication 71
9.1.10 SF.INF_PROT Residual Information Protection 71
9.1.11 SF.FAIL_PROT Failure and Tampering Protection 71
9.1.12 SF.SELFTEST Self Test 71
9.1.13 SF.UPDATE VU Software Upgrade 71
9.2 ASSURANCE MEASURES 71
9.3 TOE SUMMARY SPECIFICATION RATIONALE 71
9.3.1 Security Functions Rationale 71
9.3.2 Assurance Measures Rationale 71

10 STATEMENT OF COMPATIBILITY 71

10.1 RELEVANCE OF SECURITY CONTROLLER TSF 71
10.2 SECURITY REQUIREMENTS 71
10.2.1 Security Functional Requirements 71
10.2.2 Security Assurance Requirements 71
10.3 SECURITY OBJECTIVES 71

10.4 COMPATIBILITY: TOE SECURITY ENVIRONMENT 71
10.4.1 Assumptions *71*
10.4.2 Threats *71*
10.4.3 Organisational Security Policies *71*
10.5 CONCLUSION 71
11 ANNEX 71
11.1 GLOSSARY AND LIST OF ACRONYMS 71
11.2 BIBLIOGRAPHY 71

Table of Figures

FIGURE 1: SIMPLIFIED DRAWING OF THE VU 10
FIGURE 2: EFAS-4.0 LIFE-CYCLE 11
FIGURE 3: VU OPERATIONAL ENVIRONMENT 12

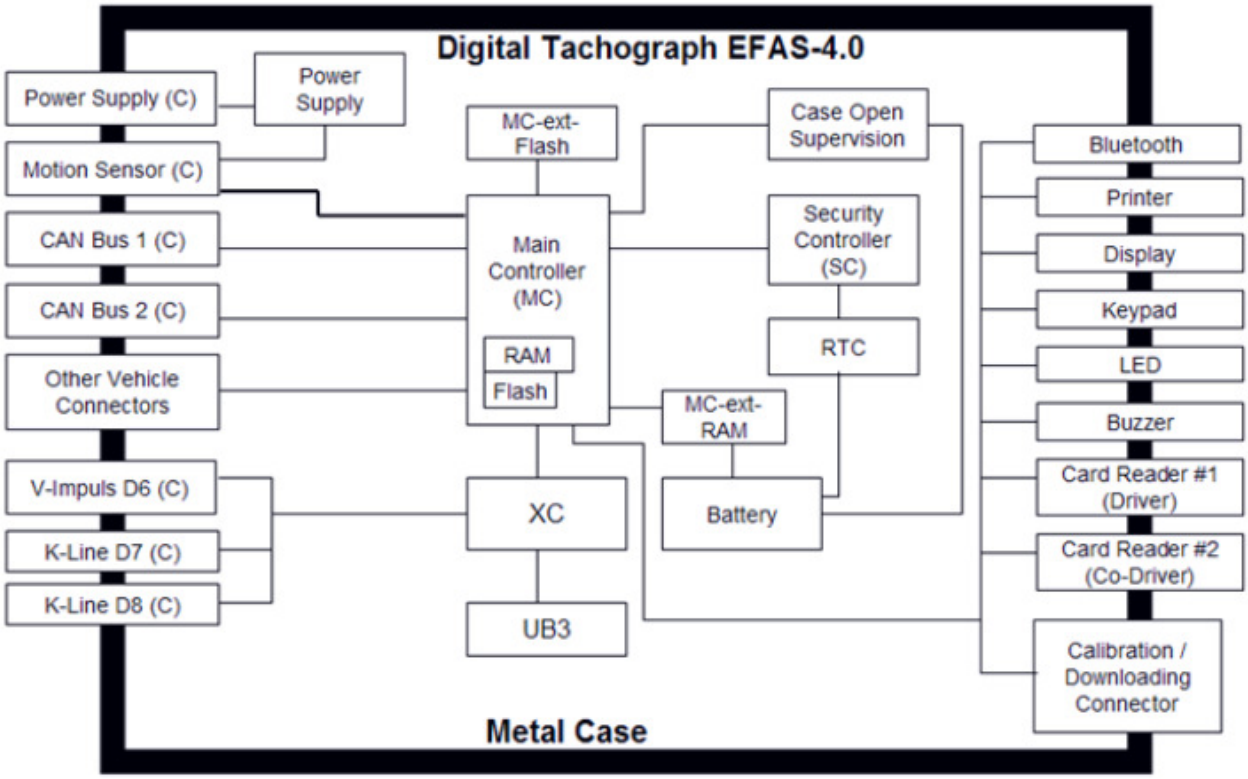

FIGURE 4: EFAS-4.0 V02.00 WITH INTERFACES 14

Table of Tables

TABLE 1: PRIMARY ASSETS 20
TABLE 2: SECONDARY ASSETS 22
TABLE 3: SUBJECTS AND EXTERNAL ENTITIES 23
TABLE 4: SECURITY OBJECTIVES FOR THE TOE 29
TABLE 5: SECURITY OBJECTIVE RATIONALE 34
TABLE 6: SECURITY FUNCTIONAL GROUPS VS. SECURITY FUNCTIONAL REQUIREMENTS 42
TABLE 7: COVERAGE OF SECURITY OBJECTIVES FOR THE TOE BY SFR 70
TABLE 8: SUITABILITY OF THE SFRS 71
TABLE 9: SAR DEPENDENCIES 71
TABLE 10:OVERVIEW OF DEVELOPERS' TOE RELATED DOCUMENTS 71
TABLE 11: COVERAGE OF SECURITY FUNCTIONAL REQUIREMENTS BY TOE SECURITY FUNCTIONALITY 71
TABLE 12: RELEVANCE OF SECURITY CONTROLLER TSF FOR COMPOSITE ST 71
TABLE 13: MAPPING OF SECURITY CONTROLLER OBJECTIVES TO TOE OBJECTIVES 71
TABLE 14: MAPPING OF SECURITY CONTROLLER ASSUMPTIONS TO TOE OBJECTIVES 71
TABLE 15: MAPPING OF SECURITY CONTROLLER THREATS TO TOE THREATS 71
TABLE 16: MAPPING OF SECURITY CONTROLLER OSPS TO TOE OSPS 71

1 Scope

This document specifies the Security Target (ST) for the intellic EFAS-4.0 digital tachograph.

2 ST Introduction (ASE_INT)

2.1 ST Reference

This document is the Security Target (ST) of the EFAS-4.0 (the TOE) provided by intellic Germany GmbH for a Common Criteria evaluation.

Document Title:	Security Target - EFAS-4.0
Document Date:	10.11.2011
Document Version:	18
Editor:	Dr. Horst Kießling
Publisher:	intellic Germany GmbH
CC-Version:	3.1 (Revision 3)
Assurance Level:	The minimum assurance level for this ST is EAL4 augmented.
General Status:	Released
TOE:	EFAS-4.0
TOE Developer:	intellic Germany GmbH
TOE Sponsor:	intellic GmbH (Austria)
Certification ID:	BSI-DSZ-CC-0726
IT Evaluation Scheme:	German CC Evaluation Scheme
Evaluation Body:	SRC Security Research & Consulting GmbH (SRC)

2.2 TOE Reference

The target of evaluation (TOE) is the EFAS-4.0 digital tachograph with SW version 02.00 as developed by intellic Germany GmbH, based on INFINEON M7801 A12 (see [SCST]).

The INFINEON SC is used with the following configuration (Sales name SLE 78 CFX 1600P):

- M7801 A12,
- Chip Identifier Byte = 77h,
- NVM 160 kBytes,
- ROM blocked,
- XRAM 8kBytes,
- with ISO7816(2),
- without I2C,
- with Flash Loader (FL) 3.50.022
- including RMS V8000B0015
- and STS V78.01.07.07
- and SA V1.4 B90
- and Overall-Patch V8013

- with patches for FL, RMS
- and STS
- and SW: RSA2048 V1.02.008

2.3 TOE Overview

2.3.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) addressed by the current security target is a vehicle unit (VU) in the sense of Annex I B [EU1B] intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards.

The physical scope of the TOE is a device to be installed in a vehicle. The TOE consists of a hardware box (includes processing units, data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration/ downloading connector, facilities for entry of user's inputs, embedded software and of related user manuals. It must be connected to a motion sensor (MS) and to a power supply unit; it can temporarily be connected with other devices used for calibration, data export, software upgrade and diagnostics.

The TOE receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all these user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces for download purpose inclusive remote download after corresponding identification and authentication of the company (by means of the company card).

Furthermore, the TOE contains the functionality for secure update of the defined parts of the TOE software.

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

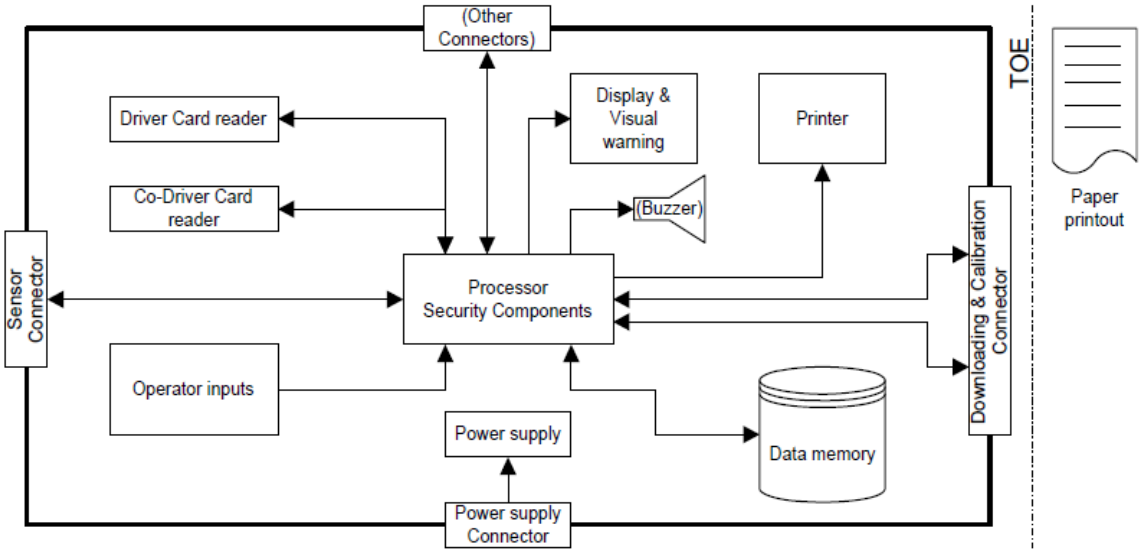

Figure 1: Simplified Drawing of the VU

2.3.2 TOE Major Security Features for Operational Use

The main security feature of the TOE is as specified in [EU1B] (O.VU_Main): The data to be measured (the physical data measurement is performed by the motion sensor which is not part of this TOE) and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

It concretely means that security of the VU aims to protect

a) the data recorded and stored in such a way as to prevent unauthorized access to and manipulation of the data and detecting any such attempts,
b) the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
c) the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and
d) the integrity and authenticity of data downloaded (locally and remotely).

The main security feature stated above is provided by the following major security services
(please refer to [GST], chapter 4):

a) Identification and authentication of motion sensor und tachograph cards,
b) Access control to functions and stored data,
c) Accountability of users,
d) Audit of events and faults,
e) Object reuse for secret data,
f) Accuracy of recorded and stored data,
g) Reliability of services,
h) Data exchange with motion sensor, tachograph cards and external media (download function).

'Identification and Authentication' as well as 'data exchange' directly require cryptographic support according to [GST], sec. 4.9.

2.3.3 TOE Type

The TOE type is the Vehicle Unit EFAS-4.0, a vehicle unit in the sense of Annex I B [EU1B].

The life cycle of the EFAS-4.0 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.

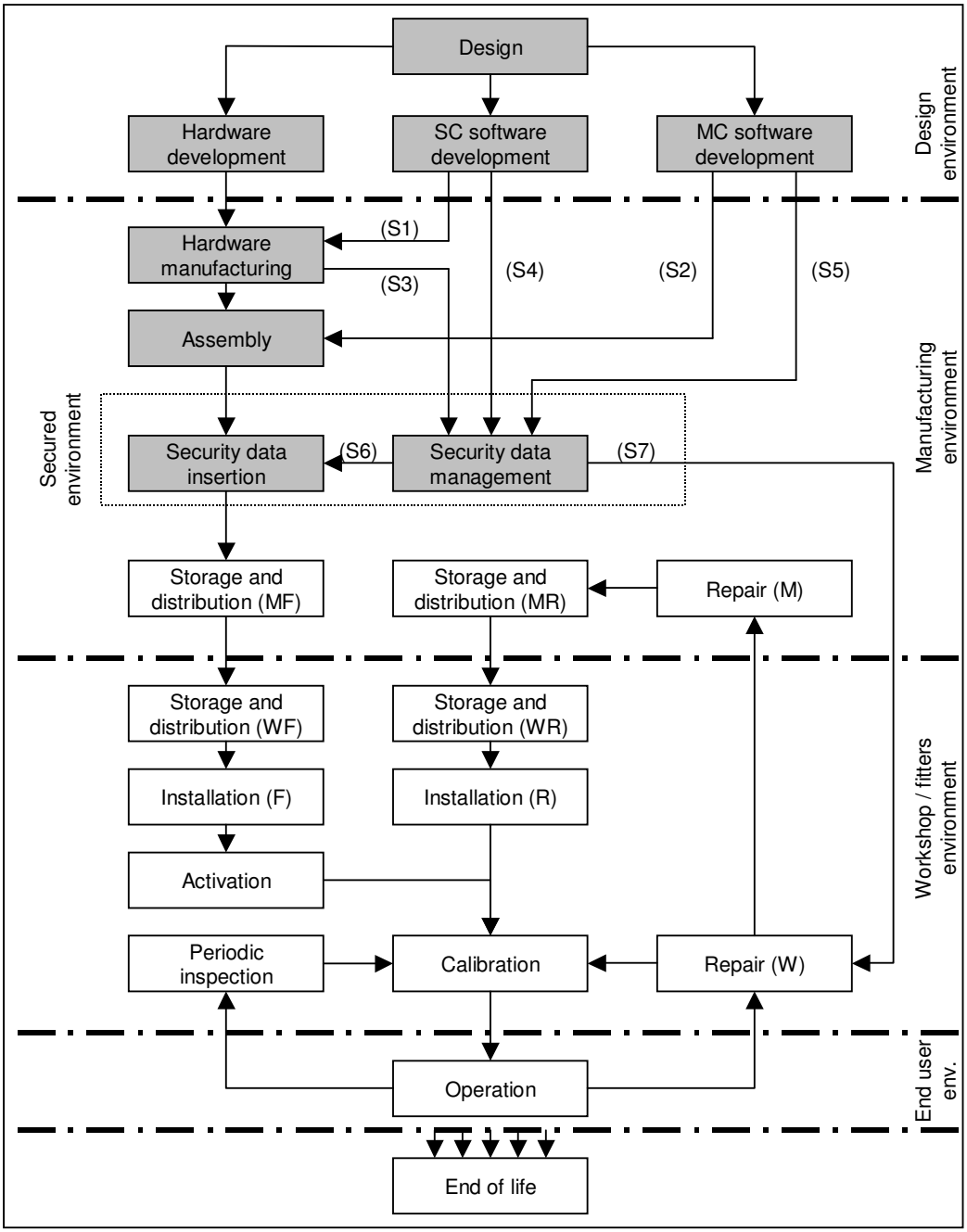

Figure 2: EFAS-4.0 Life-Cycle

The security requirements in section 4 of [GST] limit the scope of the security examination of the TOE to the operational phase in the end user environment. Therefore, the security policy defined by this ST also focuses on the operational phase of the VU in the end user environment. Some single properties of the calibration phase

being significant for the security of the TOE in its operational phase are also considered by the current ST as required by [GST].

The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [EU1B], REQ007 and REQ010: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU (calibration phase comprises all operations within the fitters and workshops environment).

This security target takes all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see section 4.3 'Package Claim' below) and the requirements from the BSI-CC-PP-0057 protection profile (see [PPT]). The TOE delivery from its manufacturer to the first customer (approved workshops) exactly happens at the transition from the manufacturing to the calibration phase, see also [PPT], sec. 8.2 for delivery interfaces.

A software update can be executed by a workshop on the basis of encrypted update data prepared by the Security Server in the manufacturing environment (S7).
The VU enables a software update of defined parts of the software (incl. wireless remote update connection), if the corresponding authentication was successful.

2.3.4 Non-TOE hardware/software/firmware

The vehicle unit's operational environment while installed in a vehicle is depicted in the following figure:

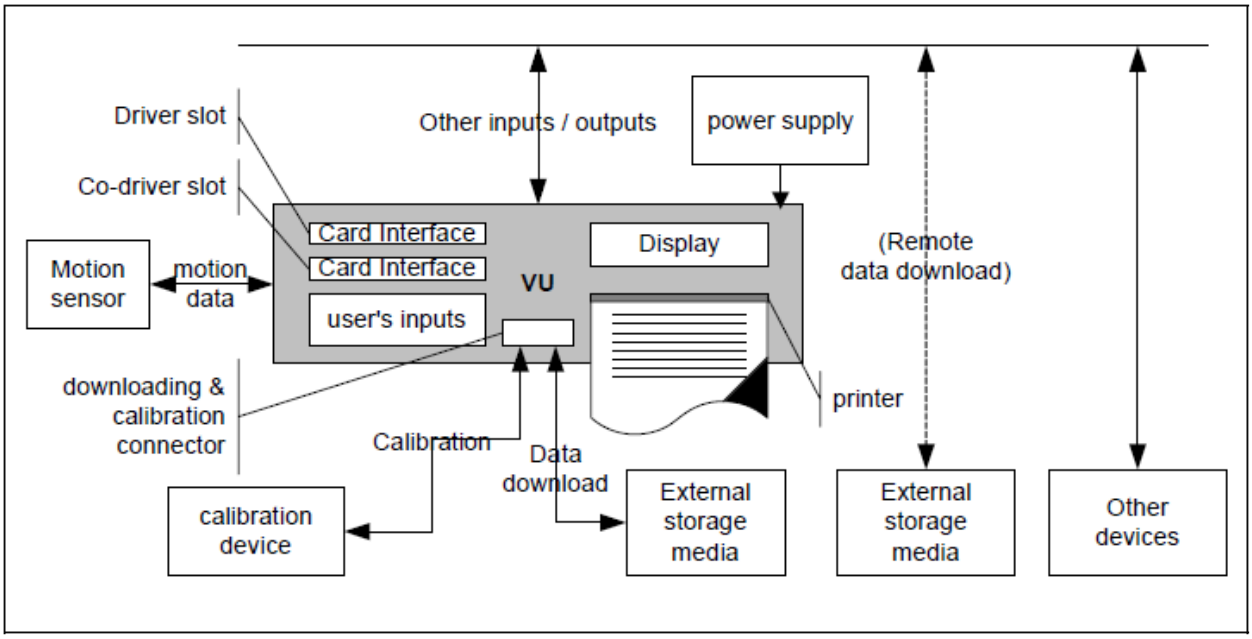

Figure 3: VU Operational Environment

The following TOE-external components are

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

b) functionally necessary for an Annex I B compliant operation:

- calibration device (fitters and workshops environment only)
- tachograph cards (four different types of them)
- printer paper
- external storage media for data download;

c) helpful for a convenient TOE operation:
- connection to the vehicle network e.g. CAN-connection.
- connection to a remote download device

While operating, the TOE will verify, whether the connected motion sensor and tachograph cards possess appropriate credentials showing their belonging to the digital tachograph system. A security certification according to [GST] is a prerequisite for the type approval of a motion sensor and tachograph cards.

The VU “Digital Tachograph EFAS-4.0” contains a separate Extension Controller – XC (see next chapter). The Extension Controller controls external interfaces as an agent for the MC and evaluates the acceleration data from the second motion data source – Acceleration Sensor UB3. The TOE does not include the Extension Controller (hardware and software) and the Acceleration Sensor UB3.

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 "M7801 A12 (sales name SLE 78 CFX 1600P)" provided by INFINEON. The IC is evaluated according to Common Criteria EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5 and is listed under the Certification ID BSI-DSZ-CC-0727-2011. The evaluation of the IC is based on the Protection Profile BSI-PP-0035, Version 1.0 as of June 15th 2007.

3 TOE Description

3.1 Architecture Overview

The Target of Evaluation (TOE) is the Digital Tachograph EFAS-4.0 (EFAS-4.0 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] and summarized in the PP [PPT].

The following figure 4 shows security relevant physical interfaces and internal components of the EFAS-4.0 digital tachograph.

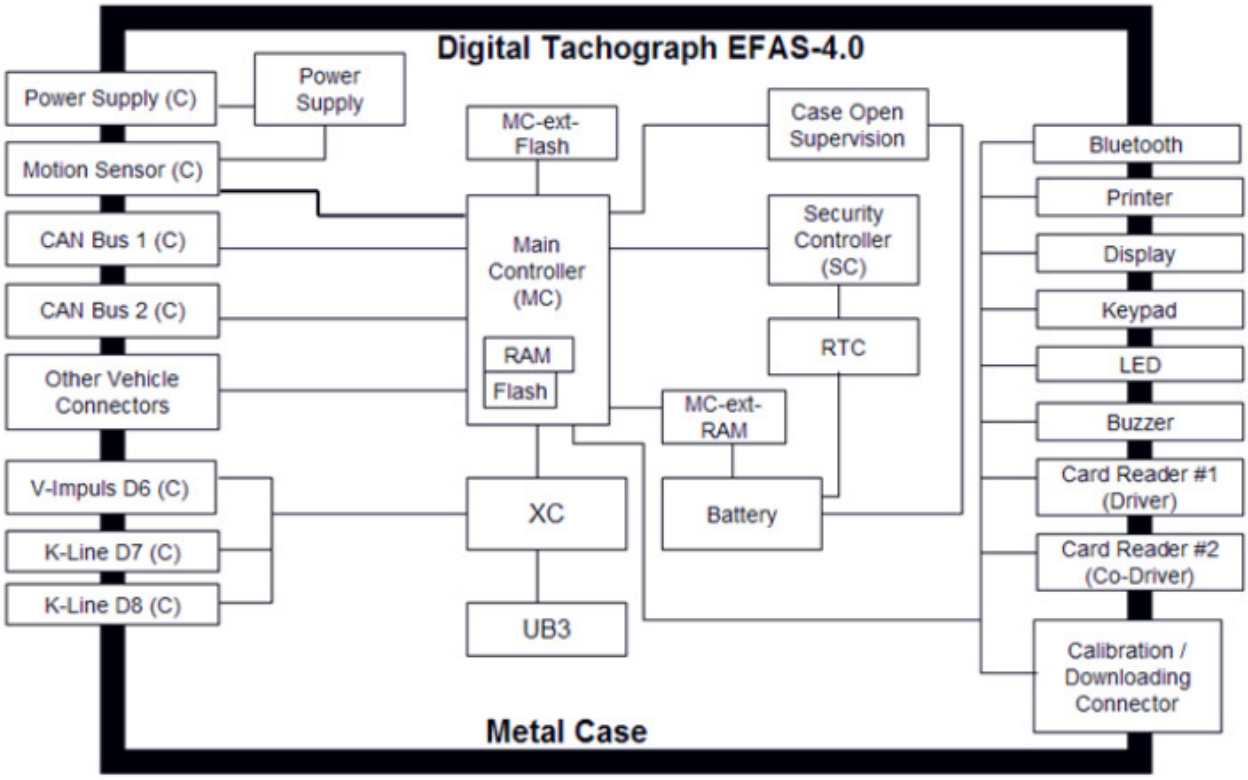

Figure 4: EFAS-4.0 V02.00 with Interfaces

3.2 TOE Hardware

The hardware components are:

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

- Storage of sensitive data (certificates, identities, audit records, …)

- Cryptographic operations.
- Supervision of time/date and motion data.
- Supervision of user data stored in the MC flash.

Main Controller (MC)
The main controller controls all external interfaces - either directly or via XC extension controller - it has exclusive access to the VU onboard flash and RAM.

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

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

Real Time Clock (RTC)
The RTC provides the EFAS-4.0 with a reliable time.

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

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

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

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

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

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

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

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

The following hardware is part of the EFAS-4.0 digital tachograph, but not of the TOE:

Extension Controller (XC)
The extension controller controls external interfaces as an agent for the MC and evaluates the acceleration data from the second motion data source UB3.

UB3 Acceleration Sensor
The acceleration sensor measures acceleration and delivers measurement data to the XC.

3.3 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 Security Server as well as between the VU and a remote company server (with connection to a Company Card). In addition, the SC software supervises the other parts of the VU, especially the time/date handling as well as the code and user data storage in the MC flash.

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

MC Boot Software
The MC boot software starts the MC application software and executes parts of the software update.

The following software is part of the EFAS-4.0 digital tachograph, but not of the TOE:

XC Software
The XC software implements functions necessary for the control of dedicated external interfaces and of the internal motion data source (acceleration sensor.

3.4 Details of Security Mechanisms

EFAS-4.0 provides all security mechanisms required in the BSI-CC-PP-0057 protection profile (see [PPT]), in particular the following:

EFAS-4.0 monitors the case opening, the values of the power supply, the RTC, the flash memory contents and the communication with the motion sensor. The TOE runs

self tests during initial start-up, and during normal operation to verify its correct operation. For events impairing the security, EFAS-4.0 generates audit records with associated data. The EFAS-4.0 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.

3.5 TOE Product Scope

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

- The vehicle unit EFAS-4.0, Hardware/Software
- Operating Manual EFAS-4.0 document in paper / electronic pdf-form (for all kinds of users)
- Service and Installation Manual EFAS-4.0, document in paper / electronic pdf-form (for workshop personnel)

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

3.6 TOE Environment

3.6.1 Development Environment

The EFAS-4.0 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 enforce the usage of guidelines. The complete development of the TOE is well documented. The confidentiality and integrity of development results is protected (usage of file servers with dedicated access rights, version controls, backup strategies, usage of e-mail encryption for communication and firewall protection). The used measures are always documented.

3.6.2 Manufacturing Environment

In the manufacturing environment, responsibilities are assigned in a manner which maintains IT security and the EFAS-4.0 is protected from physical attacks which might compromise IT security. The manufacturing environment is well documented, supported by procedures based on ISO 9001:2000 (see [ISO9001]). Measures are defined to protect security data like cryptographic keys against disclosure and manipulation. Systems which implement security data generation algorithms are accessible to authorised and trusted persons only. Security data are generated, transported, and inserted into the EFAS-4.0, in such a way as to preserve its appropriate confidentiality and integrity.

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

3.6.3 Fitters and Workshop Environment

The EFAS-4.0 fitters and workshop environment is as described in the BSI-CC-PP-0057 protection profile (see [PPT]).

3.6.4 End User Environment

The EFAS-4.0 end user environment is as described in the BSI-CC-PP-0057 protection profile (see [PPT]).

4 Conformance Claims

4.1 CC Conformance Claims

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [CC1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [CC2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [CC3]

as follows

- Part 2 conformant,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [CM] has to be taken into account.

4.2 PP Claim

This security target claims conformance to the protection profile (PP) BSI-CC-PP-0057 “Protection Profile ‘Digital Tachograph – Vehicle Unit (VU PP)’“ as sponsored by “Bundesamt für Sicherheit in der Informationstechnik“, author Dr. Igor Furgel T-Systems GEI GmbH, SC Security Analysis & Testing, version 1.0 as of 13th July 2010.

4.3 Package Claim

This ST claims conformance to the following security requirements package:

- Assurance package E3hCC31_AP as defined in section 9.2 below.

This assurance package is commensurate with JIL [JIL] defining an assurance package called E3hAP. This assurance package declares assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. 3.1) certification (in conjunction with the Digital Tachograph System) as demonstrated in [PPT].

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see section 9.2 below).

4.4 Conformance Rationale

Since this security target (ST) claims strict conformance with the protection profile (PP) BSI-CC-PP-0057 referenced in 4.2 “PP Claim”, no rationale is necessary here.

5 Security Problem Definition

5.1 Introduction

The primary and secondary assets to be secured are as introduced in BSI-CC-PP-0057 (see [PPT] section 3.1), but enhanced as described in the following tables (marked yellow).

1 The **primary assets** to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap. 11.1 for the term definitions)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	user data (recorded or stored in the TOE)	Any data, other than security data (sec. III.12.2 of [EU]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [EU].	Integrity Authenticity
2	user data transferred between the TOE and an external device connected	All user data being transferred from or to the TOE. A TOE communication partner can be: - a motion sensor, - a tachograph card, or - an external medium for data download. Motion data are part of this asset. User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality[1] Integrity Authenticity[2]

Table 1: Primary Assets

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

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

1 Not each data element being transferred represents a secret. Whose data confidentiality shall be protected while transferring them (i) between the TOE and a MS, is specified in [ISO16844], sec. 7.6 (instruction #11); (ii) between the TOE and a tachograph card – in Appendix 2 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Tachograph Cards Specification, chap. 4 (access condition = PRO SM). Confidentiality of data to be downloaded to an external medium is not required to be protected.

[2] Not each data element being transferred shall be protected for its integrity and authenticity. Whose data integrity and authenticity shall be protected while transferring them (i) between the TOE and a MS, is specified in [ISO16844], sec. 7.5 (instruction #80); (ii) between the TOE and a tachograph card – in Appendix 2 of Annex I B of Commission Regulation (EEC) No. 1360/2002, chap. 4 (access condition = AUT). Integrity and authenticity of data to be downloaded to en external medium shall always be protected.

Object No.	Asset	Definition	Property to be maintained by the current security policy
3	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
5	TOE immanent secret security data	Secret security elements used by the TOE in order to enforce its security functionality. There are the following security elements of this category: - equipment private key (EQT.SK), see [EU1B], sec. III.12.2, - vehicle unit part of the symmetric master key for communication with MS (Km_{VU}), see [CSM], sec. 3.1.3, - session key between motion sensor and vehicle unit K_{Sm} (see [ISO16844], sec. 7.4.5 (instruction 42)), - session key between tachograph cards and vehicle unit K_{St} (see [CSM], sec. 3.2) - SW-Update Keys	Confidentiality Integrity
6	TOE immanent non-secret security data	Non-secret security elements used by the TOE in order to enforce its security functionality. There are the following security elements of this category: - European public key (EUR.PK), - Member State certificate (MS.C), - equipment certificate (EQT.C). - Serial Number and Production date see [EU1B], sec. III.12.2.	Integrity Authenticity
7	TOE security relevant software	Updateable security relevant software components of the TOE (inclusive update credentials), in particular SC	Confidentiality Authenticity Integrity

Object No.	Asset	Definition	Property to be maintained by the current security policy
	components (security patch)	software (except the update mechanism).	
8	TOE non-security relevant software components (patch)	Updateable non-security relevant software components of the TOE (inclusive update credentials), such as MC software and other software components.	Confidentiality Authenticity Integrity

Table 2: Secondary assets

The workshop tachograph card requires an additional human user authentication by presenting a correct PIN value to the card. The vehicle unit (i) transmits the PIN verification value input by the user to the card and (ii) receives the card response to this verification attempt. A workshop tachograph card can only be used within the fitters and workshops environment (see A.Card_Availability below), which is presumed to be trustworthy (see A.Approved_Workshops below). Hence, no threat agent is presumed while using a workshop tachograph card.
In this context, the VU is not required to secure a PIN verification value and any card response to a verification attempt, cf. [CSM], chap. 4.

Subjects and external entities

4 This security target considers the following subjects:

External Entity No.	Subject No.	Role	Definition
1	1	User	Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card. There can also be Unknown User of the TOE and malicious user of the TOE – an attacker. User identity is kept by the VU in form of a concatenation of User group and User ID, cf. [GST], UIA_208 representing security attributes of the role 'User'. An attacker is a threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP/ST, especially to change properties of the assets having to be

External Entity No.	Subject No.	Role	Definition
			maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. Due to constraints and definitions in [GST], an attacker is an attribute of the role 'User' in the context of the current PP/ST. Being a legal user is also an attribute of the role User.
2	2	Unknown User	not authenticated user.
3	3	Motion Sensor	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled. A MS possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are MS serial number encrypted with the identification key (Enc(KID|NS)) together with pairing key encrypted with the master key (Enc(KM|KP))
4	-	Tachograph Card	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: driver card, control card, workshop card, company card. A tachograph card possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK.
5	4	Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable. Valid credentials can be either a certified key pair for authentication of a device or MS serial number encrypted with the identification key (Enc(KID|NS)) together with pairing key encrypted with the master key (Enc(KM|KP)).
6	-	Attacker	see item User above.

Table 3: Subjects and external entities

This table defines the subjects in the sense of [CC1] which can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC1]). From this point of view, the TOE itself does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

5.2 Threats

The threats to the security target (ST) are as described in the protection profile BSI-CC-PP-0057 (see [PPT] section 3.2) they are fully cited here for convenience.

Threats averted solely by the TOE:

T.Card_Data_Exchange	Users could try to modify user data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).
T.Faults	Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security[3].
T.Output_Data	Users could try to modify data output (print, display or download)[3].

Threats averted by the TOE and its operational environment:

T.Access	Users could try to access functions[3] not allowed to them (e.g. drivers gaining access to calibration function).
T.Calibration_Parameters	Users could try to use miscalibrated equipment[3] (through calibration data modification, or through organisational weaknesses).
T.Clock	Users could try to modify internal clock[3].
T.Design	Users could try to gain illicit knowledge of design[3] either from manufacturer's material (through theft, bribery …) or from reverse engineering.
T.Environment	Users could compromise the VU security[3] through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).
T.Fake_Devices	Users could try to connect fake devices (motion sensor, smart cards) to the VU[4].

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

T.Hardware	Users could try to modify VU hardware[3].
T.Identification	Users could try to use several identifications or no identification[5].
T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal)[6].
T.Power_Supply	Users could try to defeat the VU security objectives[3] by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data[7] during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify VU software[3] on the VU or during the updates (modification of patches for updates).
T.Stored_Data	Users could try to modify stored data (security[8] or user data).
T.Tests	The use of non invalidated test modes or of existing back doors could compromise the VU security[3].

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

Threats averted solely by the TOE's operational environment:

T.Non_Activated	Users could use non activated equipment[3].

5.3 Organisational Security Policies

The organisational security policies are as described in BSI-CC-PP-0057 (see [PPT] section 3.3) enhanced as described in the following tables (marked yellow).

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

[4] Communication with genuine/known equipment is a prerequisite for a secure data exchange and, hence, represents a partial aspect of the asset 'user data transferred between the TOE and an external device connected'.

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

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

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

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

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

OSPs related to the TOE:

OSP.Accountability	The VU must collect accurate accountability data.
OSP.Audit	The VU must audit attempts to undermine system security and should trace them to associated users.
OSP.Processing	The VU must ensure that processing of inputs to derive user data is accurate.
OSP.Test_Points	All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU must be disabled or removed before the VU activation during the manufacturing process.

OSPs related to the TOE and its operational environment:

OSP.Type_Approved_MS[9]	The VU shall only be operated together with a motion sensor being type approved according to Annex I B.
OSP.SW_Upgrade	The software updates have to be performed in the way that the update process itself and the transport of software parts for update to the VU will be secured to ensure the compliance to the software requirements RLB_204, RLB_205 of [GST].

OSPs related to the TOE's operational environment:

OSP.PKI

1) The European Authority shall establish a PKI according to [CSM], sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of the PKI.
2) The ERCA shall securely generate its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs.
3) The ERCA shall ensure that it issues MSi.C certificates

[9] The identity data of the motion sensor (serial number N_S) will be sent to the VU on request by the MS itself (see instruction #40 in [ISO16844]). The 'certificate' $Enc(K_{ID}|N_S)$ stored in the motion sensor is merely used by it for VU authentication, but not for verifying N_S by the VU (see instruction #41 in [ISO16844]). Therefore, the VU accepts this data (serial number N_S) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved.

	only for the rightful MSCAs.
	4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
	5) MSCAs shall securely generate their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
	6) MSCAs shall ensure that they issue EQTj.C certificates only for the rightful equipment.
OSP.MS_Keys	1) The European Authority shall establish a special key infrastructure for management of the motion sensor keys according to [ISO16844] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure.
	2) The ERCA shall securely generate both parts (K_{mVU} and K_{mWC}) of the master key (K_m).
	3) The ERCA shall ensure that it securely convey this key material only to the rightful MSCAs.
	4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
	5) MSCAs shall securely calculate the motion sensor identification key (K_{ID}) and the motion sensor's credentials: MS individual serial number encrypted with the identification key ($Enc(K_{ID}|N_S)$) and MS individual pairing key encrypted with the master key ($Enc(K_M|K_P)$).
	6) MSCAs shall ensure that they issue these MS credentials[10], K_{mVU}[11] and K_{mWC}[12] only to the rightful equipment.

5.4 Assumptions

The assumptions are as described in BSI-CC-PP-0057 (see [PPT] section 3.4).

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

The GST in [GST] does not define any dedicated assumption, but measures; these measures will be reflected in the current PP in form of the security objectives for the TOE environment below. Hence, it is to define some assumptions in the current PP being sensible and necessary from the formal point of view (to reflect those environmental measures from [GST]).

[10] to the motion sensors

[11] to the vehicle units

[12] to the workshop cards

A.Activation	Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.
A.Approved_Workshops	The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.
A.Card_Availability	Tachograph cards are available to the TOE users and delivered by Member State authorities to authorised persons only.
A.Card_Traceability	Card delivery is traceable (white lists, black lists), and black lists are used during security audits.
A.Controls	Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).
A.Driver_Card_Uniqueness	Drivers possess, at one time, one valid driver card only.
A.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.
A.Faithful_Drivers	Drivers play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …)[13].
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated.

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

6 Security Objectives

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

6.1 Security Objectives for the TOE

The security objectives for the TOE are as described in the protection profile BSI-CC-PP-0057 (see [PPT] section 4.1) enhanced as described in the following table (marked yellow).

The following TOE security objectives address the protection provided by the TOE independent of the TOE environment.

They are derived from the security objectives as defined in [GST], sec. 3.5.

O.Access	The TOE must control user access to functions and data.
O.Accountability	The TOE must collect accurate accountability data.
O.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
O.Authentication	The TOE should authenticate users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The TOE must maintain stored data integrity.
O.Output	The TOE must ensure that data output reflects accurately data measured or stored.
O.Processing	The TOE must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The TOE must provide a reliable service.
O.Secured_Data_Exchange	The TOE must secure data exchanges with the motion sensor and with tachograph cards.
O.Software_Analysis[14]	There shall be no way to analyse or debug software[15] in the field after the TOE activation.
O.Software_Upgrade	The TOE must ensure confidentiality, authenticity and integrity of software to be installed during a software upgrade.

Table 4: Security Objectives for the TOE

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

[15] It is a matter of the decision by the certification body and the evaluation facility involved in a concrete certification process on a classification of the TOE (hard- and software) into security relevant and irrelevant parts.

6.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are as described in BSI-CC-PP-0057 (see [PPT] section 4.2) enhanced as described in the following tables (marked yellow):

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment *independent* of the TOE itself.

They are derived from the security objectives as defined in GST [GST], sec. 3.6, where they are represented as security measures.

a) design environment (cf. the life cycle diagram in Figure 2: EFAS-4.0 Life-Cycle above):

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

b) Manufacturing environment

OE.Manufacturing	VU manufacturers shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.
OE.Sec_Data_Generation	Security data generation algorithms shall be accessible to authorised and trusted persons only.
OE.Sec_Data_Transport	Security data shall be generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.
OE.Delivery	VU manufacturers, vehicle manufacturers and fitters or workshops shall ensure that handling of the TOE is done in a manner which maintains IT security.
OE.Software_Upgrade	Software revisions shall be granted security certification before they can be implemented in the TOE. The software parts for updates have to be secured during the generation and transport to the VU.
OE.Sec_Data_Strong[16]	Security data inserted into the TOE shall be as cryptographically strong as required by [CSM].
OE.Test_Points[17]	All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation by the VU manufacturer during the manufacturing process.

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

[17] This objective is added for the sake of a more clear description of the security policy: In the GST [GST], this aspect is part of O.Reliability, what might be not self-evident: A TOE cannot achieve an objective depending on action of its manufacturer. The special concern here is RLB_201 in [GST].

Please note that the design and the manufacturing environments are not the intended usage environments for the TOE. The security objectives for these environments being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test_Points, OE.Delivery) are the subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing environments do not address any potential *TOE user* and, therefore, cannot be reflected in the documents of the assurance class AGD.
The remaining security objectives for the manufacturing environment (OE.Sec_Data_Generation, OE.Sec_Data_Transport, OE.Sec_Data_Strong and OE.Software_Upgrade) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

c) Workshops environment

OE.Activation	Vehicle manufacturers and fitters or workshops shall activate the TOE after its installation before the vehicle leaves the premises where installation took place.
OE.Approved_Workshops	Installation, calibration and repair of recording equipment shall be carried by trusted and approved fitters or workshops.
OE.Faithful_Calibration	Approved fitters and workshops shall enter proper vehicle parameters in recording equipment during calibration.

d) End-user environment

OE.Card_Availability	Tachograph cards shall be available to TOE users and delivered by Member State Authorities to authorised persons only.
OE.Card_Traceability	Card delivery shall be traceable (white lists, black lists), and black lists must be used during security audits.
OE.Controls	Law enforcement controls shall be performed regularly and randomly, and must include security audits.
OE.Driver_Card_Uniqueness	Drivers shall possess, at one time, one valid driver card only.
OE.Faithful_Drivers[18]	Drivers shall play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …).
OE.Regular_Inspections	Recording equipment shall be periodically inspected and calibrated.
OE.Type_Approved_MS[19]	The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to Annex I B.

[18] The objective OE.Faithful_Drivers taken from the Generic Security Target [GST] seems not to be realistic and enforceable (from *security* point of view), because the driver is the person, who has to be controlled and surveyed (see the Commission Regulation [EU]). This objective is claimed in the current PP only for the sake of compatibility with the GST [GST] and is necessary from *functional* point of view, see also A.Faithful_Drivers.

[19] The identity data of the motion sensor (serial number N_S) will be sent to the VU on request by the MS itself (see instruction #40 in [ISO16844]). The 'certificate' Enc(K_{ID}|N_S) stored in the motion sensor is merely used by it for VU authentication, but not for verifying N_S by the VU (see instruction #41 in [ISO16844]). Therefore, the VU accepts this data (serial number N_S) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved (-> UIA_202).

6.3 Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats (see 5.2) and OSPs (see 5.3) are addressed by the security objectives. It also shows that all assumptions (see 5.4) are addressed by the security objectives for the TOE environment.

This rationale covers the rationale part in [GST], chap. 8 and in its corrigendum 2004 (see [EU]) as described in [PPT]; however, enhanced by the additional rationale for T.Software (partly), OSP.SW_Upgrade, O.Software_Upgrade, OE.Software_Upgrade (partly).

	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.SW_Upgrade	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections
O.Access	x					x		x		x						x		x																	
O.Accountability		x																	x																
O.Audit	x	x					x			x	x	x		x	x		x	x		x															
O.Authentication	x	x				x		x		x		x											x												
O.Integrity						x												x																	
O.Output					x						x			x			x	x																	
O.Processing						x	x	x	x	x	x					x	x				x														
O.Reliability			x	x	x		x		x	x	x	x			x	x	x	x				x													
O.Secured_Data_Echange							x			x		x				x																			
O.Software_Analysis					x																														
O.Software_Upgrade																	x									x									
OE.Development					x												x																		
OE.Software_Upgrade																x	x	x								x									
OE.Delivery													x																						
OE.Manufacturing				x	x																														
OE.Sec_Data_Strong																x								x	x										
OE.Sec_Data_Generation																x								x	x										
OE.Sec_Data_Transport																x								x	x										
OE.Test.Points																						x													
OE.Activation	x												x														x								
OE.Approved_Workshops						x		x					x															x					x		
OE.Card_Availability		x																											x						
OE.Card_Traceability		x																												x					
OE.Controls						x		x	x	x	x		x		x	x	x	x													x				
OE.Driver_Card_Uniqueness		x																														x			

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

Table 5: Security Objective Rationale

A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below (as taken from the protection profile [PPT], no amendmends necessary).

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

T.Identification is addressed by O.Authentication to ensure the identification of the user, O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address this threat by storing all activity carried (even without an identification) with the VU. The OE.Driver_Card_Uniqueness, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.

T.Faults is addressed by O.Reliability for fault tolerance. Indeed, if the TOE provides a reliable service as required by O.Reliability, the TOE cannot experience uncontrollable internal states. Hence, also each possible fault of the TOE will be controllable, i.e. the TOE will be in a well-known state at any time. Therefore, threats grounding in faults of the TOE will be eliminated.

T.Tests is addressed by O.Reliability and OE.Manufacturing. Indeed, if the TOE provides a reliable service as required by O.Reliability and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the TOE can neither enter any invalidated test mode nor have any back door. Hence, the related threat will be eliminated.

T.Design is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Software_Analysis to prevent reverse engineering and by O.Output (RLB_206) to ensure that data output reflects accurately data measured or store and O.Reliability (RLB_201, 204, 206).

T.Calibration_Parameters is addressed by O.Access to ensure that the calibration function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive calibration data is accurate, by O.Integrity to maintain the integrity of calibration parameters stored. Workshops are approved by Member States authorities and are therefore trusted to calibrate properly the equipment (OE.Approved_Workshops, OE.Faithful_Calibration). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections), contribute to address the threat.

Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the VU, which helps addressing the threat.

T.Card_Data_Exchange is addressed by O.Secured_Data_Exchange. O.Audit contributes to address the threat by recording events related to card data exchange integrity or authenticity errors. O.Reliability (ACR_201, 201a), O.Processing (ACR_201a).

T.Clock is addressed by O.Access to ensure that the full time adjustment function is accessible to workshops only and by O.Authentication to ensure the identification of the workshop and by O.Processing to ensure that processing of inputs made by the workshop to derive time adjustment data is accurate. Workshops are approved by Member States authorities and are therefore trusted to properly set the clock (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Faithful_Calibration), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.

T.Environment: is addressed by O.Processing to ensure that processing of inputs to derive user data is accurate.and by O.Reliability to ensure that physical attacks are countered. OE.Controls includes controls by law enforcement officers of time adjustment data records held in the VU, which helps addressing the threat.

T.Fake_Devices is addressed by O.Access (ACC_205) O.Authentication (UIA_201 – 205, 207 – 211, 213, UIA_221 – 223), O.Audit (UIA_206, 214, 220), O.Processing (ACR_201a), O.Reliability (ACR_201, 201a), O.Secured_Data_Exchange (CSP_201 - 205). OE.Type_Approved_MS ensures that only motion sensors with correct identification data have the credentials that are required to successfully authenticate themselves. OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the whole installation.

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

T.Motion_Data is addressed by O.Authentication, O.Reliability (UIA_206, ACR_201, 201a), O.Secured_Data_Exchange and OE.Regular_Inspections , OE.Type_Approved_MS. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

T.Non_Activated is addressed by the OE.Activation and OE.Delivery. Workshops are approved by Member States authorities and are therefore trusted to activate properly the equipment (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Controls), also contribute to address the threat.

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

T.Power_Supply is mainly addressed by O.Reliability to ensure appropriate behaviour of the VU against the attack. O.Audit contributes to address the threat by keeping records of attempts to tamper with power supply. OE.Controls includes controls by law enforcement officers of power supply interruption records held in the VU, which helps addressing the threat. OE.Regular_Inspections helps addressing the threat through installations, calibrations, checks, inspections , repairs tcarried out by trusted fitters and workshops.

T.Security_Data is addressed by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport, OE.Software_Upgrade, OE.Controls. It is addressed by the O.Access, O.Processing, O.Secured_Data_Exchange to ensure appropriate protection while stored in the VU. O.Reliability (REU_201, RLB_206).

T.Software is addressed in the user environment by the O.Output, O.Processing, O.Reliability and O.Software_Upgrade as well as OE.Software_Upgrade to ensure the confidentiality, authenticity and integrity of the code. O.Audit contributes to address the threat by recording events related to integrity errors. During design and manufacture, the threat is addressed by the OE.Development objectives. OE.Controls, OE.Regular_Inspections (checking for the audit records related).

T.Stored_Data is addressed mainly by O.Integrity, O.Access, O.Output and O.Reliability to ensure that no illicit access to data is possible. The O.Audit contributes to address the threat by recording data integrity errors. OE.Sofware_Upgrade included that software revisions shall be security certified before they can be implemented in the TOE to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU helping in addressing the threat.

OSP.Accountability is fulfilled by O.Accountability.

OSP.Audit is fulfilled by O.Audit.

OSP.SW_Upgrade is fulfilled by O.Software_Upgrade and OE.Software_Upgrade,

OSP.Processing is fulfilled by O.Processing.

OSP.Test_Points is fulfilled by O.Reliability and OE.Test_Points.

OSP.Type_Approved_MS is fulfilled by O.Authentication and OE.Type_Approved_MS.

OSP.PKI is fulfilled by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport.

OSP.MS_Keys is fulfilled by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport.

A.Activation is upheld by OE.Activation.

A.Approved_Workshops is upheld by OE.Approved_Workshops.

A.Card_Availability is upheld by OE.Card_Availability.

A.Card_Traceability is upheld by OE.Card_Traceability.

A.Controls is upheld by OE.Controls.

A.Driver_Card_Uniqueness is upheld by OE.Driver_Card_Uniqueness.

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

A.Faithful_Drivers is upheld by OE.Faithful_Drivers.

A.Regular_Inspections is upheld by OE.Regular_Inspections.

7 Extended Components Definition

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

8 Security Requirements

This security target (ST) clarifies and adapts the security requirements as given in the protection profile BSI-CC-PP-0057([PPT] chapter 6).

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

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [CC1] of the CC. These operations are used in the protection profile BSI-CC-PP-0057 [PPT] and in this ST, respectively.

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

The **selection** operation is used to select one or more options provided by [PPT] or CC in stating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted by showing as underlined text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier. In order to trace elements belonging to a component, the same slash “/” with iteration indicator is used behind the elements of a component.

For the sake of a better readability, an additional notation is used in order to indicate belonging of some SFRs to same functional cluster, namely a double slash “//” with the related functional group indicator after the component identifier. In order to trace elements belonging to a component, the same double slash “//” with functional cluster indicator is used behind the elements of a component.

Whenever an element in [PPT] contains an operation that the PP author left uncompleted, the ST author has to complete that operation and the operation within the ST is shown with yellow background.

8.1 Security Functional Requirements

The security functional requirements are as derived in the protection profile BSI-CC-PP-0057 ([PPT] chapter 6.1) which covers the SEFs from the generic security target (see [GST] chapter 4) as demonstrated in ([PPT] chapter 6.1) and documented in ([PPT] Annex A chapter 9).

In the following the necessary assignments as foreseen by [PPT] for the SFRs in the protection profile and the necessary enhancements for software-update functionality and remote download access are processed. For the remote download functionality, the corresponding application notes are considered as recommended in the [PPT]. For the software-update functionality, some new SFRs are included. Hereby, the security functionality defined in the PP is not constricted.

SFRs below include – if adequate - in curly braces {…} a list of SEFs related. This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from [GST]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

The complete coverage of the SEF(s) from [GST] is documented in the protection profile [PPT] Annex A, chap. 9.

8.1.1 Overview

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the ST defined the security functional groups as given in the [PPT] and allocated the functional requirements described in the following sections to them. For better comparison, the security functional groups are copied from [PPT] and the additional functional requirements are shown with yellow background.

Security Functional Groups	Security Functional Requirements concerned
Identification and authentication of motion sensor, tachograph cards (according to [GST], sec. 4.1)	– FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_AFL.1/MS: Authentication failure: motion sensor – FIA_AFL.1/TC: Authentication failure: tachograph cards – (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE Supported by: – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards

Security Functional Groups	Security Functional Requirements concerned
	– (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1/PP) – FIA_AFL.1/Remote: remote TC authentication failure handling
Access control to functions and stored data (according to [GST], sec. 4.2)	– (FDP_ACC.1/FIL, FDP_ACF.1/FIL): file structures – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): functions – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): stored data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): user data export – (FDP_ACC.1/IS, FDP_ACF.1/IS): input sources – FDP_ACC.1/SW-Upgrade: authenticate the software upgrades as destined for a particular TOE – FDP_ACF.1/SW-Upgrade: capability to control access to the TSF software upgrade function Supported by: – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT – FMT_MSA.3/UDE – FMT_MSA.3/IS – (FMT_MSA.1, FMT_SMF.1/PP, FMT_SMR.1//TC)
Accountability of users (according to [GST], sec. 4.3)	– FAU_GEN.1: Audit records: Generation – FAU_STG.1: Audit records: Protection against modification – FAU_STG.4: Audit records: Prevention of loss – FDP_ETC.2: Export of user data with security attributes Supported by: – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): VU identification data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): Data update on the TC – FPT_STM.1: time stamps

Security Functional Groups	Security Functional Requirements concerned
	– FCS_COP.1/TDES: for the motion sensor and the tachograph cards
Audit of events and faults (according to [GST], sec. 4.4)	– FAU_GEN.1: Audit records: Generation – FAU_SAR.1: Audit records: Capability of reviewing Supported by: – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): Storing motion sensor's audit records – FDP_ETC.2 Export of user data with security attributes: Related audit records to the TC.
Object reuse for secret data (according to [GST], sec. 4.5)	– FDP_RIP.1 Subset residual information protection Supported by: – FCS_CKM.4: Cryptographic key destruction
Accuracy of recorded and stored data (according to [GST], sec. 4.6) and of SW-upgrade data	– FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC) – FDP_ITC.2/IS: right input sources with sec. attributes (MS and TC) – FPT_TDC.1/IS: Inter-TSF basic TSF data consistency (MS and TC) – FDP_SDI.2: Stored data integrity Supported by: – (FDP_ACC.1/IS, FDP_ACF.1/IS): right input sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): limited manual entry – FAU_GEN.1: Audit records: Generation – FPT_STM.1: Reliable time stamps – FPT_TDC.1/SW-Upgrade: capability to ensure the consistency of data for the update – FCS_COP.1/AES: for decryption and CMAC verification of the software update data – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards
Reliability of services (according to [GST], sec. 4.7)	– FDP_ITC.2/IS: no executable code from external sources – FDP_ITC.2/SW-Upgrade: definition of conditions for update acceptance – FPR_UNO.1: Unobserveability of leaked data

Security Functional Groups	Security Functional Requirements concerned
	– FPT_FLS.1: Failure with preservation of secure state – FPT_PHP.2//Power_Deviation: Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services Supported by: – FAU_GEN.1: Audit records: Generation – (FDP_ACC.1/IS, FDP_ACF.1/IS): no executable code from external sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): Tachograph Card withdrawal – FMT_MOF.1: No test entry points
Data exchange with motion sensor, tachograph cards and external media (download function) (according to [GST], sec. 4.8)	– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media – FDP_ETC.2 Export of user data with security attributes: to the TC and to external media – FDP_ITC.2/IS Import of user data with security attributes: from the MS and the TC Supported by: – FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) – FCS_COP.1/RSA: for data downloading to external media (signing) – (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media – (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC – FAU_GEN.1: Audit records: Generation
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification/authentication

Table 6: Security Functional Groups vs. Security Functional Requirements

Note that in the following all additional SFRs and all completed operations compared to [PPT] are shown with yellow background.

8.1.2 Class FAU Security Audit

8.1.2.1 FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation {UIA_206, UIA_214, ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_202, AUD_203, ACR_205, RLB_203, RLB_206, RLB_210, RLB_214, DEX_202, DEX_204}

Hierarchical to: -

Dependencies: FPT_STM.1 Reliable time stamps: is fulfilled by FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) the activities and auditable events specified in REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, and 105a[20] and {UIA_206, UIA_214, AUD_202, ACR_205, RLB_203, RLB_206, RLB_210, RLB_214[21], DEX_202, DEX_204};
RLB_208, UIA_220.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the information specified in {REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, 105a[22]};
none.

8.1.2.2 FAU_SAR Security audit review

FAU_SAR.1 Audit review {AUD_205}

Hierarchical to: -

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

[21] Last card session not correctly closed

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

Dependencies:	FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1
FAU_SAR.1.1	The TSF shall provide everybody with the capability to read the recorded information according to REQ011 from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

8.1.2.3 FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage {ACT_206}[23]

Hierarchical to:	-
Dependencies:	FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to detect unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss {ACT_206}[24]

Hierarchical to:	FAU_STG.3
Dependencies:	FAU_STG.1 Protected audit trail storage: is fulfilled by FAU_STG.1
FAU_STG.4.1	The TSF shall overwrite the oldest stored audit records and behave according to REQ 083, 086, 089, 092 and 105b, if the audit trail is full.

8.1.3 Class FCO Communication

8.1.3.1 FCO_NRO Non-repudiation of origin

FCO_NRO.1 Selective proof of origin {DEX_206, DEX_207}

Hierarchical to:	-
Dependencies:	FIA_UID.1 Timing of identification: not fulfilled, but **justified** the components FIA_UID.2/MS, FIA_UID.2/TC being present in the PP do not fulfil this dependency, because they are not affine to DEX_206, DEX_207 (data download). The sense of the current dependency would be to attach the VU identity (ACT_202) to the data to be downloaded; the VU identification data are permanently stored in the VU, so that

[23] REQ081 to 093 and REQ102 to 105a

[24] REQ 083, 086, 089, 092, 105b; REQ105b is completely covered by ACT_206.

the VU always 'knows' its own identity.

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted data to be downloaded to external media at the request of the originator.

FCO_NRO.1.2 The TSF shall be able to relate the VU identity ~~of the originator~~ of the information, and the data to be downloaded to external media ~~of the information~~ to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to the recipient given
- according to specification [CSM], sec. 6.1,
limited to the scope as required in {DEX 207} and {DEX 208}.

8.1.4 Class FCS Cryptographic Support

8.1.4.1 FCS_CKM Cryptographic key management

FCS_CKM.1 Cryptographic key generation {CSP_202}

Hierarchical to: -

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

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

a) K_m, K_P, K_{ID} and K_{SM}: two-keys TDES as specified in [ISO16844];

b) K_{ST}: two-keys TDES as specified in [CSM].

FCS_CKM.2 Cryptographic key distribution {CSP_203}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: is fulfilled by FCS_CKM.1
FCS_CKM.4: is fulfilled by FCS_CKM.4

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

a) K_{SM}: as specified in [ISO16844], sec. 7.4.5;

b) K_{ST}: as specified in [CSM], CSM_020.

FCS_CKM.3 Cryptographic key access {CSP_204}

Hierarchical to: -

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

a) fulfilled by FCS_CKM.1 for the session keys K_{SM} and K_{ST} as well as for the temporarily stored keys K_m, K_P and K_{ID};

b) fulfilled by FDP_ITC.2/IS for the temporarily stored key Km_{wc} (entry DEX_203); fulfilled by FDP_ITC.2/SW-Upgrade for the temporarily stored keys KAuth, $K_{Firmware}$-SC and $K_{Firmware}$-MC;

c) not fulfilled, but **justified** for EUR.PK, EQT.SK, Km_{vu}, $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$: The persistently stored keys (EUR.PK, EQT_j.SK, Km_{vu}, $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$) will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

FCS_CKM.4: is fulfilled by FCS_CKM.4

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

a) Km_{wc}: part of the Master key read out from the workshop card and temporarily stored in the TOE (calibration phase);

b) K_m: temporarily reconstructed from part of the Master key Km_{vu} and part of the Master key Km_{wc} as specified in [ISO16844], sec. 7.2 and in [CSM], sec. 3.1.3, CSM_036, CSM_037 (calibration phase);

c) K_{ID}: temporarily reconstructed from the Master key K_m as specified in [ISO16844], sec. 7.2, 7.4.3 (calibration phase);

d) K_P: temporarily reconstructed from Enc(K_m|K_P) as specified in [ISO16844], sec. 7.2, 7.4.3 (calibration phase);

e) K_{SM}: internally generated and temporarily stored during a session between the TOE and the motion sensor connected (calibration and operational phases);

f) K_{ST}: internally generated and temporarily stored during a session between the TOE and the tachograph card connected (calibration and operational phases);

g) EUR.PK: stored during manufacturing of the TOE (calibration and operational phases);

h) EQT_j.SK: stored during manufacturing of the TOE (calibration and operational phases);

i) part of the Master key Km_{vu}: stored during manufacturing of the TOE (calibration and operational phases);

j) SW-Update Keys - $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$: stored during manufacturing of the TOE; KAuth, $K_{Firmware}$-SC and $K_{Firmware}$-MC: stored during the software update process.

FCS_CKM.4 Cryptographic key destruction {CSP_205}

Hierarchical to: -

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

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

a) Km_{wc}: delete after use (at most by the end of the calibration phase);

b) K_m: delete after use (at most by the end of the calibration phase);

c) K_{ID}: delete after use (at most by the end of the calibration phase);

d) K_P: delete after use (at most by the end of the calibration phase);

e) K_{SM}: delete by replacement (by closing a motion sensor communication session during the next pairing process);

f) K_{ST}: delete by replacement (by closing a card communication session);

g) EUR.PK: this public key does not represent any secret and, hence, needn't to be deleted;

h) EQT_j.SK: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational;

i) part of the Master key Km_{vu}: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx and must not be destroyed as long as the TOE is operational;

j) SW-Update Keys - $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$:

will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx, and must not be destroyed as long as the TOE is operational; KAuth, $K_{Firmware}$-SC and $K_{Firmware}$-MC: delete after use (at the end of the software update process);

k) Each deletion denoted above means value overwriting with "FF".

The component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of *temporary* or *permanent* nature. In contrast, the component FDP_RIP.1 concerns in this PP only the temporarily stored instantiations of objects in question.
The permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} must not be destroyed as long as the TOE is operational. Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} unavailable at decommissioning the TOE is a matter of the related organisational policy.

8.1.4.2 FCS_COP Cryptographic operation

FCS_COP.1/TDES Cryptographic operation {CSP_201}

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: is fulfilled by FCS_CKM.1 FCS_CKM.4: is fulfilled by FCS_CKM.4
FCS_COP.1.1/TDES	The TSF shall perform the cryptographic operations (encryption, decryption, Retail-MAC) in accordance with a specified cryptographic algorithm Triple DES in CBC and ECB modes and cryptographic key size 112 bits that meet the following:[ISO16844] for the Motion Sensor and [CSM] for the Tachograph Cards.

FCS_COP.1/AES Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: a) fulfilled by FDP_ITC.2/SW-Upgrade for the temporarily stored keys KAuth, $K_{Firmware}$-SC and $K_{Firmware}$-MC; b) not fulfilled, but **justified** for $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$: The persistently stored keys $KENC_{UpdateVu}$ and $KAUTH_{UpdateVu}$ will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx. FCS_CKM.4: is fulfilled by FCS_CKM.4
FCS_COP.1.1/AES	The TSF shall perform the cryptographic operations (decryption and data integrity protection) in accordance

with a specified cryptographic algorithm AES in CBC mode and CMAC and cryptographic key size 128 bits that meet the following: [FIPS 197] (AES), [NIST SP800-38A] (AES CBC mode) and [NIST SP800-38B] (AES CMAC).

FCS_COP.1/RSA Cryptographic operation {CSP_201}

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: not fulfilled, but **justified** It is a matter of RSA decrypting and verifying in the context of CSM_020 (VU<->TC authentication) and of RSA signing according to CSM_034 using static keys imported outside of the VU's operational phase (OE.Sec_Data_xx). FCS_CKM.4: is fulfilled by FCS_CKM.4
FCS_COP.1.1/RSA	The TSF shall perform the cryptographic operations (decryption, verifying for the Tachograph Cards authentication and signing for downloading to external media) in accordance with a specified cryptographic algorithm RSA and cryptographic key size 1024 bits that meet the following: [CSM], CSM_020 for the Tachograph Cards authentication and [CSM], CSM_034 for downloading to external media, respectively.

8.1.5 Class FDP User Data Protection

8.1.5.1 FDP_ACC Access control policy

FDP_ACC.1/FIL Subset access control {ACC_211}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/FIL
FDP_ACC.1.1/FIL	The TSF shall enforce the File Structure SFP on tachograph application and data files structure as required by ACC_211.

FDP_ACC.1/FUN Subset access control {ACC_201}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/FUN
FDP_ACC.1.1/FUN	The TSF shall enforce the SFP FUNCTION on subjects, objects, and operations as referred to in - operational modes {ACC_202} and the related

restrictions on access rights {ACC_203},
- calibration functions {ACC_206} and time adjustment {ACC_208},
- limited manual entry {ACR_201a}, and
- Tachograph Card withdrawal {RLB_213}
as required by ACC_201.

FDP_ACC.1/DAT Subset access control {ACC_201}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/DAT
FDP_ACC.1.1/DAT	The TSF shall enforce the SFP DATA on subjects, objects, and operations as referred to in: - VU identification data: REQ075 (structure) {ACT_202} and REQ076 (once recorded) {ACC_204}, - MS identification data: REQ079 (Manufacturing-ID) and REQ155 (pairing) {ACC_205}, - Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209}, - Security Data: REQ080 {ACC_210}, - MS Audit Records: {AUD_204} as required by ACC_201.

FDP_ACC.1/SW-Upgrade Subset access control {ACC_201}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/SW-Upgrade
FDP_ACC.1.1/ SW-Upgrade	The TSF shall enforce the SFP SW_Upgrade on updateable software components and User with identity UNKNOWN for updates of MC software components and User with identity WORKSHOP for updates of SC software components.

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

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/UDE
FDP_ACC.1.1/UDE	The TSF shall enforce the SFP User Data Export on subjects, objects, and operations as required by REQ 109 and 109a.

FDP_ACC.1/IS Subset access control {ACR_201, RLB_205}

Hierarchical to:	-
Dependencies:	FDP_ACF.1: is fulfilled by FDP_ACF.1/IS
FDP_ACC.1.1/IS	The TSF shall enforce the SFP_Input_Sources on subjects, objects, and operations as required by ACR_201 (right input sources) and RLB_205 (no external executable code).

8.1.5.2 FDP_ACF Access control functions

FDP_ACF.1/FIL Security attribute based access control {ACR_211}

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/FIL FMT_MSA.3: is fulfilled by FMT_MSA.3/FIL
FDP_ACF.1.1/FIL	The TSF shall enforce the File_Structure_SFP to objects based on the following: the entire files structure of the TOE-application as required by {ACC_211}.
FDP_ACF.1.2/FIL	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: none.
FDP_ACF.1.3/FIL	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/FIL	The TSF shall explicitly deny access of subjects to objects based on the following additional rules as required by {ACC_211}.

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/FUN FMT_MSA.3: is fulfilled by FMT_MSA.3/FUN
FDP_ACF.1.1/FUN	The TSF shall enforce the SFP_FUNCTION to objects based on the following: subjects, objects, and their attributes as referred to in: - operational modes {ACC_202} and the related restrictions on access rights {ACC_203}, - calibration functions {ACC_206} and time adjustment {ACC_208}, - limited manual entry {ACR_201a}, and - Tachograph Card withdrawal {RLB_213}.
FDP_ACF.1.2/FUN	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in {ACC_202, ACC_203, ACC_206, ACC_208, ACR_201a, RLB_213}.
FDP_ACF.1.3/FUN	The TSF shall explicitly authorise access of subjects to

objects based on the following additional rules: none.

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

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

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/DAT
FMT_MSA.3: is fulfilled by FMT_MSA.3/DAT

FDP_ACF.1.1/DAT The TSF shall enforce the SFP DATA to objects based on the following: subjects, objects, and their attributes as referred to in:
- VU identification data: REQ075 (structure) {ACT_202} and REQ076 (once recorded) {ACC_204},
- MS identification data: REQ079 (Manufacturing-ID) and REQ155 (pairing) {ACC_205},
- Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209},
- Security Data: REQ080 {ACC_210},
- MS Audit Records: {AUD_204}.

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

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

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

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

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/UDE
FMT_MSA.3: is fulfilled by FMT_MSA.3/UDE

FDP_ACF.1.1/UDE The TSF shall enforce the SFP User Data Export to objects based on the following: subjects, objects, and their attributes as required by REQ 109 and 109a.

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

FDP_ACF.1.3/UDE The TSF shall explicitly authorise access of subjects to

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

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/IS FMT_MSA.3: is fulfilled by FMT_MSA.3/IS
FDP_ACF.1.1/IS	The TSF shall enforce SFP Input Sources to objects based on the following: subjects, objects, and their attributes as required by ACR 201 (right input sources) and RLB 205 (no external executable code).
FDP_ACF.1.2/IS	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in {ACR 201[25]}.
FDP_ACF.1.3/IS	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/IS	The TSF shall explicitly deny access of subjects to objects based on the following additional rules as required by {RLB 205}.

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

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/SW-Upgrade FMT_MSA.3: not fulfilled but **justified**: For an update, the patch data are accepted only together with the corresponding credentials, which contain all information needed for verification. So, it is not necessary to initialise any static attributes.
FDP_ACF.1.1/SW-Upgrade	The TSF shall enforce SFP SW Upgrade to objects based on the following: updateable software components may be exchanged if the integrity and the authenticity of the patch data is confirmed with help of the update credentials.
FDP_ACF.1.2/SW-Upgrade	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - update of SC software components is only possible after workshop card authentication, - update of software components is only possible if the

[25] Especially for MS and TC

	integrity and the authenticity of the patch data were confirmed with help of the update credentials.
FDP_ACF.1.3/SW-Upgrade	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SW-Upgrade	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

8.1.5.3 FDP_ETC Export from the TOE

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

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/UDE
FDP_ETC.2.1	The TSF shall enforce the SFP User Data Export when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: REQ110, DEX_205, DEX_208.

8.1.5.4 FDP_ITC Import from outside of the TOE

FDP_ITC.1 Import of user data without security attributes {ACR_201}

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS FMT_MSA.3: is fulfilled by FMT_MSA.3/IS
FDP_ITC.1.1	The TSF shall enforce the SFP Input Sources when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: as required by {ACR_201} for recording equipment calibration parameters and user's inputs.

FDP_ITC.2/IS Import of user data with security attributes {ACR_201, RLB_205, DEX_201, DEX_202, DEX_203, DEX_204}

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS [FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but **justified**: Indeed, trusted channels VU<->MS and VU<->TC will be established. Since the component FTP_ITC.1 represents just a higher abstraction level integrative description of this property and does not define any additional properties comparing to {FDP_ITC.2/IS + FDP_ETC.2 + FIA_UAU.1/TC (and /MS)}, it can be dispensed with this dependency in the current context of the PP. FPT_TDC.1: is fulfilled by FPT_TDC.1/IS
FDP_ITC.2.1/IS	The TSF shall enforce the SFP_Input_Sources when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/IS	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/IS	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/IS	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/IS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE as required by: - [ISO16844] for the Motion Sensor {ACR_201, DEX_201}, - DEX_202 (audit record and continue to use imported data), - [CSM] for the Tachograph Cards {ACR_201, DEX_203}, - DEX_204 (audit record and not using of the data), - RLB_205 (no executable code from external sources).

FDP_ITC.2/SW-Upgrade Import of user data[26] with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/SW-Upgrade [FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but **justified**: For an update, the patch data are accepted only together with the corresponding credentials, which contain all information needed for verification. So, it is not necessary to establish trusted channel or trusted path. FPT_TDC.1: is fulfilled by FPT_TDC.1/SW-Upgrade

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

FDP_ITC.2.1/SW-Upgrade	The TSF shall enforce the SFP SW_Upgrade when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/SW-Upgrade	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/SW-Upgrade	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/SW-Upgrade	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/SW-Upgrade	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: update of the indicated software components only if the integrity and the authenticity of the patch data is confirmed with help of the update credentials.

8.1.5.5 FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {REU_201}

Hierarchical to: -

Dependencies: -

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a **temporarily stored** resource is made unavailable upon the allocation of the resource to the following objects:

a) Km_{wc}: workshop card part of the motion sensor master key (at most by the end of the calibration phase);

b) K_m: motion sensor master key (at most by the end of the calibration phase);

c) K_{ID}: motion sensor identification key (at most by the end of the calibration phase);

d) K_P: motion sensor pairing key (at most by the end of the calibration phase);

e) K_{SM}: session key between motion sensor and vehicle unit (when its temporarily stored value shall not be used any more);

f) K_{ST}: session key between tachograph cards and vehicle unit (by closing a card communication session);

g) $EQT_j.SK$: equipment private key (when its temporarily stored value shall not be used any more);

h) Km_{vu}: VU part of the motion sensor master key (when

its temporarily stored value shall not be used any more);

i) PIN: the verification value of the workshop card PIN temporarily stored in the TOE during its calibration (at most by the end of the calibration phase);

j) SW-Update Keys - $KENC_{UpdateVu}$, $KAUTH_{UpdateVu}$, KAuth, $K_{Firmware}$-SC and $K_{Firmware}$-MC (when the temporarily stored values shall not be used any more, at most by the end of the software update).

The component FDP_RIP.1 concerns in this ST only the temporarily stored (e.g. in RAM) instantiations of objects in question. In contrast, the component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of *temporary* or *permanent* nature.
Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} unavailable at decommissioning the TOE is a matter of the related organisational policy.

The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

8.1.5.6 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action {ACR_204, ACR_205}

Hierarchical to:	-
Dependencies:	-
FDP_SDI.2.1	The TSF shall monitor user data stored in **the TOE's data memory** ~~containers controlled by the TSF~~ for integrity errors ~~on all objects, based on the following attributes: [assignment: *user data attributes*~~].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall generate an audit record.

The context for the current SFR is built by the related requirements ACR_204, ACR_205 (sec. 4.6.3 of [GST] 'Stored data integrity'). This context gives a clue for interpretation that it is not a matter of temporarily, but of permanently stored user data[27].

8.1.6 Class FIA Identification and Authentication

8.1.6.1 FIA_AFL Authentication failures

FIA_AFL.1/MS Authentication failure handling {UIA_206}

[27] see definition in glossary

Hierarchical to:	-
Dependencies:	FIA_UAU.1: is fulfilled by FIA_UAU.2//MS
FIA_AFL.1.1/MS	The TSF shall detect when 20 unsuccessful authentication attempts occur related to motion sensor authentication.
FIA_AFL.1.2/MS	When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall - generate an audit record of the event, - warn the user, - continue to accept and use non secured motion data sent by the motion sensor.

FIA_AFL.1/TC Authentication failure handling {UIA_214}

Hierarchical to:	-
Dependencies:	FIA_UAU.1: is fulfilled by FIA_UAU.1/TC
FIA_AFL.1.1/TC	The TSF shall detect when 5 unsuccessful authentication attempts occur related to tachograph card authentication.
FIA_AFL.1.2/TC	When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall - generate an audit record of the event, - warn the user, - assume the user as Unknown User and the card as non valid[28] (definition (z) and REQ007).

FIA_AFL.1/Remote Authentication failure handling {UIA_214, UIA_220}

Hierarchical to:	-
Dependencies:	FIA_UAU.1: is fulfilled by FIA_UAU.1/TC
FIA_AFL.1.1/Remote	The TSF shall detect when 5 unsuccessful authentication attempts occur related to tachograph card authentication.
FIA_AFL.1.2/Remote	When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall - generate an audit record of the event, - warn the user, - assume the user as Unknown User and the card as non valid[29] (definition (z) and REQ007). - warn the remote station about having 5 unsuccessful authentication attempts.

8.1.6.2 FIA_ATD User attribute definition

FIA_ATD.1//TC User attribute definition {UIA_208}

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

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

Hierarchical to:	-
Dependencies:	-
FIA_ATD.1.1//TC	The TSF shall maintain the following list of security attributes belonging to individual users: as defined in {UIA_208, UIA_216}.

8.1.6.3 FIA_UAU User authentication

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

Hierarchical to:	-
Dependencies:	FIA_UID.1: is fulfilled by FIA_UID.2/TC
FIA_UAU.1.1/TC	The TSF shall allow (i) TC identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by FAU_SAR.1 on behalf of the user to be performed before the user is authenticated[30].
FIA_UAU.1.2/TC	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PIN Timing of authentication {UIA_212}

Hierarchical to:	-
Dependencies:	FIA_UID.1: is fulfilled by FIA_UID.2/TC[31]
FIA_UAU.1.1/PIN	The TSF shall allow (i) TC (Workshop Card) identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by FAU_SAR.1 on behalf of the user to be performed before the user is authenticated[32].
FIA_UAU.1.2/PIN	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2//MS User authentication before any action {UIA_203}[33].

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

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

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

[33] Though MS identification happens before the MS authentication, they will be done within same command (80 or 11); hence, it is also plausible to choose here the functional component FIA_UAU.2.

Hierarchical to:	FIA_UAU.1
Dependencies:	FIA_UID.1: is fulfilled by FIA_UID.2/MS
FIA_UAU.2.1//MS	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.3/MS Unforgeable authentication {UIA_205}.

Hierarchical to:	-
Dependencies:	-
FIA_UAU.3.1/MS	The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2/MS	The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.3/TC Unforgeable authentication {UIA_213} and {UIA_219}.

Hierarchical to:	-
Dependencies:	-
FIA_UAU.3.1/TC	The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2/TC	The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.5//TC Multiple authentication mechanisms {UIA_211} and {UIA_218}.

Hierarchical to:	-
Dependencies:	-
FIA_UAU.5.1//TC	The TSF shall provide multiple authentication mechanisms according to CSM_20 in [CSM] to support user authentication.
FIA_UAU.5.2//TC	The TSF shall authenticate any user's claimed identity according to the CSM_20 in [CSM].

FIA_UAU.6/MS Re-authenticating {UIA_204}.

Hierarchical to:	-
Dependencies:	-
FIA_UAU.6.1/M	The TSF shall re-authenticate the user under the conditions:

S more frequently than once per hour, cf. UIA_204 in [GST].

FIA_UAU.6/TC Re-authenticating {UIA_210}.

Hierarchical to: -
Dependencies: -
FIA_UAU.6.1/TC The TSF shall re-authenticate the user under the conditions: more frequently than once per day, cf. UIA_210 in [GST].

8.1.6.4 FIA_UID User identification

FIA_UID.2/MS User identification before any action {UIA_201}

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

FIA_UID.2/TC User identification before any action {UIA_207} and {UIA_215}

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

8.1.7 Class FPR Privacy

8.1.7.1 FPR_UNO Unobservability

FPR_UNO.1 Unobservability {RLB_204 for leaked data}

Hierarchical to: -
Dependencies: -
FPR_UNO.1.1 The TSF shall ensure that all users are unable to observe the **cryptographic** operation**s** as required by FCS_COP.1/AES, FCS_COP.1/TDES and FCS_COP.1/RSA on cryptographic keys being to keep secret (as listed in FCS_CKM.3 excepting EUR.PK) by **the TSF** [~~assignment: *list of protected users and/or subjects*~~].

'To observe the cryptographic operations' means here 'using any TOE external

interface in order to gain the values of cryptographic keys which shall be kept secret'.

8.1.8 Class FPT Protection of the TSF

8.1.8.1 FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	-
Dependencies:	-
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}.

8.1.8.2 FPT_PHP TSF physical protection

FPT_PHP.2//Power_Deviation Notification of physical attack {RLB_209}

Hierarchical to:	FPT_PHP.1
Dependencies:	FMT_MOF.1: not fulfilled, but **justified:** It is a matter of RLB_209: this function (detection of deviation) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a not applicable way for RLB_209
FPT_PHP.2.1//Power_Deviation	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2//Power_Deviation	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3//Power_Deviation	For the devices/elements for which active detection is required in {RLB_209}, the TSF shall monitor the devices and elements and notify the user and audit record generation when physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack {RLB_204 for stored data}

Hierarchical to:	-
Dependencies:	-
FPT_PHP.3.1	The TSF shall resist physical tampering attacks to the TOE security enforcing part of the software in the field after the TOE activation by responding automatically such that the SFRs are always enforced.

8.1.8.3 FPT_STM Time stamps

FPT_STM.1 Reliable time stamps {ACR_201}

Hierarchical to:	-
Dependencies:	-
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

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

8.1.8.4 FPT_TDC Inter-TSF TSF Data Consistency

FPT_TDC.1/IS Inter-TSF basic TSF data consistency {ACR_201}

Hierarchical to:	-
Dependencies:	-
FPT_TDC.1.1/IS	The TSF shall provide the capability to consistently interpret secure messaging attributes as defined by [ISO16844] for the Motion Sensor and by [CSM] for the Tachograph Cards when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/IS	The TSF shall use the interpretation rules (communication protocols) as defined by [ISO16844] for the Motion Sensor and by [CSM] for the Tachograph Cards when interpreting the TSF data from another trusted IT product.

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

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

8.1.8.5 FPT_TST TSF self test

FPT_TST.1 TSF testing {RLB_202}

Hierarchical to:	-
Dependencies:	-
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate the **integrity of security data and the integrity of stored**

executable code (if not in ROM) ~~the correct operation of [selection: *[assignment: parts of TSF], the TSF*~~].

FPT_TST.1.2 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of security data.

FPT_TST.1.3 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of stored TSF executable code.

8.1.9 Class FRU Resource Utilisation

8.1.9.1 FRU_PRS Priority of service

FRU_PRS.1 Limited priority of service {RLB_212}

Hierarchical to: -

Dependencies: -

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to functions and data covered by the current set of SFRs shall be mediated on the basis of the subjects' assigned priority.

8.1.10 Class FMT Security Management

8.1.10.1 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes {UIA_208}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/FUN
FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
FMT_SMF.1: is fulfilled by FMT_SMF.1/PP

FMT_MSA.1.1 The TSF shall enforce the SFP_FUNCTION to restrict the ability to change_default the security attributes User Group, User ID[34] to nobody.

FMT_MSA.3/FUN Static attribute initialisation

Hierarchical to: -

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

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

FMT_MSA.3.2/F The TSF shall allow nobody to specify alternative initial

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

UN	values to override the default values when an object or information is created.

FMT_MSA.3/FIL Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1: is fulfilled by FMT_MSA.1 FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
FMT_MSA.3.1/FIL	The TSF shall enforce the File Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/FIL	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/DAT Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1: is fulfilled by FMT_MSA.1 FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
FMT_MSA.3.1/DAT	The TSF shall enforce the SFP_DATA to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/DAT	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/UDE Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1: is fulfilled by FMT_MSA.1 FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
FMT_MSA.3.1/UDE	The TSF shall enforce the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/UDE	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/IS Static attribute initialisation

Hierarchical to:	-

Dependencies:	FMT_MSA.1: is fulfilled by FMT_MSA.1 FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
FMT_MSA.3.1/IS	The TSF shall enforce the SFP_Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/IS	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

8.1.10.2 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour {RLB_201}

Hierarchical to:	-
Dependencies:	FMT_SMR.1: is fulfilled by FMT_SMR.1//TC FMT_SMF.1: is fulfilled by FMT_SMF.1/PP
FMT_MOF.1.1	The TSF shall restrict the ability to enable the functions specified in {RLB_201} to nobody.

8.1.10.3 FMT_SMF Specification of Management Functions

FMT_SMF.1/PP Specification of Management Functions {UIA_208}

Hierarchical to:	-
Dependencies:	-
FMT_SMF.1.1/PP	The TSF shall be capable of performing the following management functions: all operations being allowed only in the calibration mode as specified in REQ010.

FMT_SMF.1/SW-Upgrade Specification of Management Functions

Hierarchical to:	-
Dependencies:	-
FMT_SMF.1.1/SW-Upgrade	The TSF shall be capable of performing the following management functions: update of updateable software components if the rights and conditions are fulfilled as specified in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade.

8.1.10.4 FMT_SMR Security management roles

FMT_SMR.1//TC Security roles {UIA_208}

Hierarchical to:	-
Dependencies:	FIA_UID.1: is fulfilled by FIA_UID.2/TC

FMT_SMR.1.1// TC	The TSF shall maintain the roles as defined in {UIA_208} as User Groups: - DRIVER (driver card), - CONTROLLER (control card), - WORKSHOP (workshop card), - COMPANY (company card), - UNKNOWN (no card inserted), - Motion Sensor, - Unknown equipment.
FMT_SMR.1.2// TC	The TSF shall be able to associate users with roles.

8.2 Security Assurance Requirements

The security assurance requirements are as derived in BSI-CC-PP-0057 (see [PPT] section 6.2).

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

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

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

The CC community acts on the presumption that the assurance components of CCv3.1 and CCv2.x are equivalent to each other.

Due to this fact, the ST includes the appropriate assurance package **E3hCC31_AP** compiled and defined in the PP [PPT] as shown below (validity of this proposal is confined to the Digital Tachograph System):

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

Assurance Classes	Assurance Family	E3hCC31_AP (based on EAL4)
Life Cycle Support	ALC_CMC	4
	ALC_CMS	4
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	ATE_FUN	1
	ATE_IND	2
AVA Vulnerability Assessment	AVA_VAN	5

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

The requirement {RLB_215} is covered by ADV_ARC (security domain separation); the requirement {RLB_204} is partially covered by ADV_ARC (self-protection).

8.3 Security Requirements Rationale

8.3.1 Security Functional Requirements Rationale

The SFR rationale is taken from BSI-CC-PP-0057 ([PPT] sections 6.3.1, 6.3.2 and 6.3.4) and enhanced by necessary rationale for SW upgrade and remote download.

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Excha	O.Software_Analysis	O.Software_Upgrade
FAU_GEN.1	Audit data generation		x	x								
FAU_SAR.1	Audit review		x	x								
FAU_STG.1	Protected audit trail storage		x	x		x						
FAU_STG.4	Prevention of audit data loss		x	x								
FCO_NRO.1	Selective proof of origin						x			x		
FCS_CKM.1	Cryptographic key generation									x		
FCS_CKM.2	Cryptographic key distribution									x		

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Excha	O.Software_Analysis	O.Software_Upgrade
FCS_CKM.3	Cryptographic key access									x		
FCS_CKM.4	Cryptographic key destruction									x		
FCS_COP.1/TDES	Cryptographic operation									x		
FCS_COP.1/AES	Cryptographic operation											x
FCS_COP.1/RSA	Cryptographic operation									x		
FDP_ACC.1/FIL	Subset access control	x										
FDP_ACC.1/FUN	Subset access control	x						x	x	x	x	
FDP_ACC.1/DAT	Subset access control	x										
FDP_ACC.1/UDE	Subset access control	x										
FDP_ACC.1/IS	Subset access control	x						x	x			
FDP_ACC.1/SW-Upgrade	Subset access control	x							x			x
FDP_ACF.1/FIL	Security attribute based access control	x										
FDP_ACF.1/FUN	Security attribute based access control	x						x	x	x	x	
FDP_ACF.1/DAT	Security attribute based access control	x										
FDP_ACF.1/UDE	Security attribute based access control	x										
FDP_ACF.1/IS	Security attribute based access control	x						x	x			
FDP_ACF.1/SW-Upgrade	Security attribute based access control	x							x			x
FDP_ETC.2	Export of user data with security attributes		x			x	x			x		
FDP_ITC.1	Import of user data without security attributes							x	x			
FDP_ITC.2/IS	Import of user data with security attributes							x	x	x		
FDP_ITC.2/SW-Upgrade	Import of user data with security attributes								x			x
FDP_RIP.1	Subset residual information protection	x						x	x			
FDP_SDI.2	Stored data integrity monitoring and action			x		x	x		x			
FIA_AFL.1/MS	Authentication failure handling			x	x				x			
FIA_AFL.1/TC	Authentication failure handling			x	x				x			
FIA_AFL.1/Remote	Authentication failure handling			x	x				x			
FIA_ATD.1//TC	User attribute definition			x						x		
FIA_UAU.1/TC	Timing of authentication				x					x		
FIA_UAU.1/PIN	Timing of authentication				x							
FIA_UAU.2//MS	User authentication before any action				x					x		
FIA_UAU.3/MS	Unforgeable authentication				x							
FIA_UAU.3/TC	Unforgeable authentication				x							
FIA_UAU.5//TC	Multiple authentication mechanisms	x			x					x		
FIA_UAU.6/MS	Re-authenticating				x					x		

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Excha	O.Software_Analysis	O.Software_Upgrade
FIA_UAU.6/TC	Re-authenticating				x					x		
FIA_UID.2/MS	User identification before any action	x	x	x	x					x		
FIA_UID.2/TC	User identification before any action	x	x	x	x					x		
FMT_MSA.1	Management of security attributes	x								x		
FMT_MSA.3/FUN	Static attribute initialisation	x						x	x	x	x	
FMT_MSA.3/FIL	Static attribute initialisation	x										
FMT_MSA.3/DAT	Static attribute initialisation	x										
FMT_MSA.3/IS	Static attribute initialisation	x						x	x			
FMT_MSA.3/UDE	Static attribute initialisation	x										
FMT_MOF.1	Management of security functions	x							x			
FMT_SMF.1/PP	Specification of Management Functions	x								x		
FMT_SMF.1/SW-Upgrade	Specification of Management Functions											x
FMT_SMR.1//TC	Security roles	x								x		
FPR_UNO.1	Unobservability	x					x	x	x		x	
FPT_FLS.1	Failure with preservation of secure state.			x					x			
FPT_PHP.2//Power_Deviation	Notification of physical attack								x			
FPT_PHP.3	Resistance to physical attack						x	x	x		x	
FPT_STM.1	Reliable time stamps		x	x				x	x			
FPT_TDC.1/IS	Inter-TSF basic TSF data consistency							x	x			
FPT_TDC.1/SW-Upgrade	Inter-TSF basic TSF data consistency								x			x
FPT_TST.1	TSF testing			x					x			
FRU_PRS.1	Limited priority of service								x			

Table 7: Coverage of Security Objectives for the TOE by SFR

A detailed justification required for *suitability* of most of the aforementioned security functional requirements to achieve the security objectives is given in [PPT] section 6.3.1 in the table “Suitability of the SFRs”. The following table argues for the suitability of all SFRs and particularly marks those which are not already covered by the table “Suitability of the SFRs” in [PPT] section 6.3.1.

security objectives	Security functional requirement	
O.Access	FDP_ACC.1/FIL	File structure SFP on application and data files structure
	FDP_ACC.1/FUN	SFP FUNCTION on the functions of the TOE
	FDP_ACC.1/DAT	SFP DATA on user data of the TOE
	FDP_ACC.1/UDE	SFP User_Data_Export for the export of user data
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACC.1/SW-Upgrade	Ensure the rights for software updates
	FDP_ACF.1/FIL	Entire files structure of the TOE-application
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/DAT	Defines security attributes for SFP DATA on user
	FDP_ACF.1/UDE	Defines security attributes for SFP User_Data_Export
	FDP_ACF.1/IS	Defines security attributes for SFP Input Sources.
	FDP_ACF.1/SW-Upgrade	Ensure the conditions for software updates
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [CSM] to support user authentication.
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FMT_MSA.1	Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody.
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative

security objectives	Security functional requirement	
		initial values to override the default values when an object or information is created.
	FMT_MSA.3/FIL	Provides the File_Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/DAT	Provides the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/UDE	Provides the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MOF.1	Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, prevents an unintended access to data in the operational phase.
	FMT_SMF.1/PP	Performing all operations being allowed only in the calibration mode.
	FMT_SMR.1//TC	Maintain the roles as defined in {UIA_208} as User Groups.
O.Accountability	FAU_GEN.1	Generates correct audit records
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified

security objectives	Security functional requirement	
		before allowing any other action
	FPT_STM.1	Provides accurate time
O.Audit	FAU_GEN.1	Generates correct audit records
	FAU_SAR.1	Allows users to read accountability audit records
	FAU_STG.1	Protect the stored audit records from unauthorised deletion.
	FAU_STG.4	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	FDP_SDI.2	monitors user data stored for integrity error
	FIA_AFL.1/MS	Detects and records authentication failure events for the motion sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FIA_AFL.1/Remote	Authentication failure handling, additionally to normal failure handling the remote station is warned about having 5 unsuccessful authentication attempts
	FIA_ATD.1//TC	Defines user attributes for tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FPT_FLS.1	Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}
	FPT_STM.1	Provides accurate time
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
O.Authentication	FIA_AFL.1/MS	Detects and records authentication failure events for the motion sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FIA_AFL.1/Remote	Authentication failure handling, additionally to normal failure handling the remote station is warned about having 5 unsuccessful authentication attempts
	FIA_UAU.1/TC	Allows TC identification before authentication
	FIA_UAU.1/PIN	Allows TC (Workshop Card) identification before authentication
	FIA_UAU.2//MS	Motion sensor has to be successfully authenticated before allowing any action

security objectives	Security functional requirement	
	FIA_UAU.3/MS	Provides unforgeable authentication for the motion sensor
	FIA_UAU.3/TC	Provides unforgeable authentication for the tachograph cards
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [CSM] to support user authentication.
	FIA_UAU.6/MS	Periodically re-authenticate the motion sensor
	FIA_UAU.6/TC	Periodically re-authenticate the tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
O.Integrity	FAU_STG.1	Protect the stored audit records from unauthorised deletion
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_SDI.2	monitors user data stored for integrity error
O.Output	FCO_NRO.1	Generates an evidence of origin for the data to be downloaded to external media.
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_SDI.2	monitors user data stored for integrity error
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_PHP.3	Ensures resistance to physical attack to the TOE software in the field after the TOE activation
O.Processing	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/IS	Defines security attributes for SFP User_Data_Export
	FDP_ITC.1	Provides import of user data from outside of the TOE using the SFP Input Sources
	FDP_ITC.2/IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards

security objectives	Security functional requirement	
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_PHP.3	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1/IS	Provides the capability to consistently interpret secure messaging attributes as defined by [ISO16844] for the Motion Sensor and by [CSM] for the Tachograph Cards.
O.Reliability	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACC.1/IS	SFP Input Sources to ensure the right input sources
	FDP_ACC.1/SW-Upgrade	Ensure the rights for software updates
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/IS	Defines security attributes for SFP User_Data_Export
	FDP_ACF.1/SW-Upgrade	Ensure the conditions for software updates
	FDP_ITC.1	Provides import of user data from outside of the TOE using the SFP Input Sources
	FDP_ITC.2/IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards
	FDP_ITC.2/SW-Upgrade	Provides import of SW upgrade data from outside of the TOE, using the defined

security objectives	Security functional requirement	
		conditions for the update acceptance
	FDP_RIP.1	Any previous information content of a resource is made unavailable upon allocation or deallocation of resource
	FDP_SDI.2	monitors user data stored for integrity error
	FIA_AFL.1/MS	Detects and records authentication failure events for the motion sensor
	FIA_AFL.1/TC	Detects and records authentication failure events for the tachograph cards
	FIA_AFL.1/Remote	Authentication failure handling, additionally to normal failure handling the remote station is warned about having 5 unsuccessful authentication attempts.
	FMT_MOF.1	Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, increases TOE reliability in the operational phase.
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3/IS	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FPR_UNO.1	Ensures unobservability of secrets
	FPT_FLS.1	Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}
	FPT_PHP.2//Power_Deviation	Detection of physical tampering (Power_Deviation) and generation of an audit record
	FPT_PHP.3	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	FPT_STM.1	Provides accurate time
	FPT_TDC.1/IS	Provides the capability to consistently interpret secure messaging attributes as defined by [ISO16844] for the Motion Sensor and by [CSM] for the Tachograph Cards.
	FPT_TDC.1/SW-Upgrade	Provides the capability to consistently interpret the patch data and the corresponding credentials.

security objectives	Security functional requirement	
	FPT_TST.1	Detects integrity failure events for security data and stored executable code
	FRU_PRS.1	Ensures that resources will be available when needed
O.Secured_Data_Exchange	FCO_NRO.1	Generates an evidence of origin for the data to be downloaded to external media.
	FCS_CKM.1	Generates of session keys for the motion sensor and the tachograph cards
	FCS_CKM.2	Controls distribution of cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the table below that meets the following list of standards.
	FCS_CKM.3	Controls cryptographic key access and storage in the TOE
	FCS_CKM.4	Destroys cryptographic keys in the TOE
	FCS_COP.1/TDES	Provides the cryptographic operation TDES
	FCS_COP.1/RSA	Provides the cryptographic operation RSA
	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ETC.2	Provides export of user data with security attributes using the SFP User_Data_Export
	FDP_ITC.2/IS	Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards
	FIA_ATD.1//TC	Defines user attributes for tachograph cards
	FIA_UAU.1/TC	Allows TC identification before authentication
	FIA_UAU.2//MS	Motion sensor has to be successfully authenticated before allowing any action
	FIA_UAU.5//TC	Multiple authentication mechanisms according to CSM_20 in [CSM] to support user authentication.
	FIA_UAU.6/MS	Periodically re-authenticate the motion sensor
	FIA_UAU.6/TC	Periodically re-authenticate the tachograph cards
	FIA_UID.2/MS	A motion sensor is successfully identified before allowing any other action
	FIA_UID.2/TC	A tachograph card is successfully identified before allowing any other action
	FMT_MSA.1	Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody

security objectives	Security functional requirement	
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1/PP	Performing all operations being allowed only in the calibration mode
	FMT_SMR.1//TC	Maintain the roles as defined in {UIA_208} as User Groups
O.Software_Analysis	FPT_PHP.3	Ensures resistance to physical attack to the TOE software in the field after the TOE activation
	FPR_UNO.1	Ensures unobservability of secrets
	FDP_ACC.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FDP_ACF.1/FUN	Defines security attributes for SFP FUNCTION according to the modes of operation
	FMT_MSA.3/FUN	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
O.Software_Upgrade	FDP_ACC.1/SW-Upgrade	Ensure the rights for software updates
	FDP_ACF.1/SW-Upgrade	Ensure the conditions for software updates
	FDP_ITC.2/SW-Upgrade	Provides import of SW upgrade data inclusive the corresponding credentials from outside of the TOE.
	FPT_TDC.1/SW-Upgrade	Provides the capability to consistently interpret the patch data and the corresponding credentials.
	FCS_COP.1/AES	Provides the cryptographic operation AES decryption and CMAC.
	FMT_SMF.1/SW-Upgrade	Performs the update if the rights and conditions allow it.

Table 8: Suitability of the SFRs

8.3.2 Rationale for SFR's Dependencies

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

The dependency analysis has directly been made within the description of each SFR in sec. 8.1 above. All dependencies being expected by [CC2] are either fulfilled or their non-fulfilment is justified.

8.3.3 Security Assurance Requirements Rationale

The security assurance requirements rationale is as derived in the protection profile BSI-CC-PP-0057 ([PPT] sections 6.3.3 and 6.3.4)

The current protection profile/ST is claimed to be conformant with the assurance package E3hCC31_AP (cf. sec. 4.3 above). As already noticed there in sec.8.2, the assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

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

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This decision represents a part of the conscious security policy for the recording equipment required by the legislative [EU] and reflected by the current PP and ST.

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

The augmentation of EAL4 chosen comprises the following assurance components:

– ATE_DPT.2 and

– AVA_VAN.5.

For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL4)		
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1

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

Table 9: SAR Dependencies

8.3.4 Security Requirements – Internal Consistency

The argumentation in [PPT] section 6.3.4 applies, in particular:

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

8.3.4.1 SFRs

The dependency analysis in section 8.3.1 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section 8.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current ST accurately and completely reflects the Generic Security Target [GST] and Protection Profile [PPT]. Since the GST [GST] is part of the related legislation, it is assumed to be internally consistent.

Therefore, due to conformity between the current PP and [GST] (see [PPT] section 6.3.4) and the conformity between [PPT] and this ST, also subjects and objects being used in the current ST are used in a consistent way.

8.3.4.2 SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 8.3.3 "Security Assurance Requirements Rationale" shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 8.3.2 "Rationale for SFR's Dependencies" and 8.3.3 "Security Assurance Requirements Rationale". Furthermore, as also discussed in

section 8.3.3 “Security Assurance Requirements Rationale”, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

9 TOE Summary Specification

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

9.1 TOE Security Functions

For the definition of the Security Functions (SF_xxx) related to the SC, it is referred to the Security Target [SCST], chapter 7. Security Functions of the SC are relevant for the EFAS-4.0. The following sections provide a survey of the Security Functions of the TOE under consideration of the requirements in the protection profile [PPT] including all extensions and operations made in chapter 8.1.

9.1.1 SF.ACS Security Attribute Based Access Control

SF.ACS controls the access to the data and functions and enforces the File_Structure SFP, SFP FUNCTION, SFP DATA, SFP User_Data_Export, SFP Input_Sources, SFP SW-Upgrade (see 8.1.5.1) as required by FDP_ACC.1/*, FDP_ACF.1/* and FDP_ITC.1, FDP_ITC.2/IS and FMT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE.

SF.ACS implements the File_Structure SFP for tachograph application and data files structure as required by ACC_211 (FDP_ACC.1/FIL, FDP_ACF.1/FIL) and enforces the SFP FUNCTION, SFP DATA, SFP User_Data_Export on subjects, objects, and operations as required in 4 of [GST] and described in 8.1.5 (FDP_ACC.1/DAT, FDP_ACF.1/DAT, FDP_ACC.1/UDE, FDP_ACF.1/UDE) .

In particular, SF.ACS ensures that access to resources is obtained when required and that resources are neither requested nor retained unnecessarily as required by FRU_PRS.1, furthermore, it preserves the audit trail as required by FAU_STG.1 and protects keys as required by FPR_UNO.1. SF.ACS ensures that cards cannot be released before relevant data have been stored to them:

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

SF.ACS ensures that user data 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, as required by FPT_TDC.1/IS
- VU's real time clock, as required in FPT_STM.1
- recording equipment calibration parameters, as required in FDP_ITC.1
- tachograph cards, as required by FPT_TDC.1/IS, supported by
- users' inputs

in accordance with the requirements FDP_ACC.1/IS, FDP_ACF.1/IS, FPT_STM.1, FDP_ITC.1,FDP_ITC.2/IS, FPT_TDC.1/IS.

SF.ACS ensures that user data (entered manually) related to requirement 109a ([EU], Annex 1B) may only be entered for the period last card withdrawal — current insertion (requirement 050a) in accordance with the requirements FDP_ACC.1/UDE, FDP_ACF.1/UDE.

SF.ACS controls the access to the data and functions of the TOE and prevents the possibility to analyse or debug TOE's software (inclusive the cryptographic keys) in the field after the EFAS-4.0 activation (ADV_ARC, FPR_UNO.1). This includes that SF.ACS allows the calibration functions only in calibration mode (as specified in REQ 010) in accordance with FMT_SMF.1/PP.

Inputs from external sources are not accepted as executable code (as required in FDP_ITC.2/IS, FDP_ACC.1/IS, FDP_ACF.1/IS). Software update of the security and non-security relevant software components is only possible after the corresponding authentication and verification with help of credentials as required in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade,.

SF.ACS contributes audit data through logging of events which deviate from the admissible FDP_ACC.1 in accordance with FAU_GEN.1.

Nobody may change the public/private keys and the KM_{VU} after their insertion during the production process. Nobody may read the private keys and the KM_{VU} after their insertion during the production process in full compliance with FMT_MSA.1, FMT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE (see 8.1.10.1).

In doing so, SF.ACS directly supports FCS_CKM.3 and FCS_COP.1/RSA.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.2 SF.SECAUDIT Audit

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

SF.SECAUDIT, for events impairing the security of the EFAS-4.0, records those events with associated data ([EU], Annex 1B (requirements 094, 096 and 109) as required in FAU_GEN.1.

In particular, for the activities and auditable events specified in REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, and 105a[35] and UIA_206, UIA_214, AUD_202,

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

ACR_205, RLB_203, RLB_206, RLB_210, RLB_214[36], DEX_202, DEX_204, RLB_208, UIA_220 the following information will be stored: date, time and type of the event, subject identity, and the outcome (success or failure) of the event and the information specified in REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, 105a.

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

SF.SECAUDIT enforces audit records storage rules [EU], Annex 1B (requirement 094) and (requirement 096) in a way as required in FDP_ETC.2. In particular, SF.SECAUDIT supports the enforcing the SFP User_Data_Export and provides the capability to read recorded information possibly secured with help of associated security attributes.

SF.SECAUDIT stores audit records generated by the motion sensor in its data memory as required by FAU_GEN.1.

SF.SECAUDIT makes it possible to print, display and download audit records except for the events listed in REQ 011 as required by FAU_SAR.1.

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

- security breach attempts like
  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorized change of motion sensor,
  - card data input integrity error,
  - stored user data integrity error,
  - internal data transfer error,
  - unauthorised case opening,
  - hardware manipulation,
- last card session not correctly closed,
- motion data error event,
- power supply interruption event,
- EFAS-4.0 internal fault.

in a way which covers FAU_GEN.1.

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

[36] Last card session not correctly closed

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

SF.SECAUDIT overwrites the oldest stored audit records and behaves according to [EU] requirements 083, 086, 089, 092 and 105b, if the audit trail is full as required in FAU_STG.4.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.3 SF.EX_CONF Confidentiality of Data Exchange

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

- tachograph card
- motion sensor
- external device and
- Security Server

For this purpose, encryption based on symmetric Triple DES cryptography is used. The data transfer between the EFAS-4.0 and

- tachograph cards is secured according to ISO/IEC 7816-4 (see [ISO7816]) to the extent as defined in [GST] CSM_021 - TDES in CBC mode with key length 112 bits as required in FCS_COP.1/TDES
- the motion sensor is secured according to ISO/DIS 16844-3 (see [ISO16844]) - TDES in ECB mode with key length 112 bits as required in FCS_COP.1/TDES

The communication with the remote external device is secured with TDES-cryptographic mechanisms with calculation of a session key based on secrets stored in the SC and external device and dynamic data portions provided by both components at connection time (mutual authentication mechanism) - TDES in CBC mode with key length 112 bits as required in FCS_COP.1/TDES

The SW-upgrade data inclusive credentials are secured with AES-cryptographic mechanisms based on VU-specific keys according to the BSI recommendations in [TR-02102] - AES in CBC mode with key length 128 bits as required in FCS_COP.1/AES and FDP_ITC.2/SW-Upgrade. The software update patch contains two files. The firmware image file is encrypted by the Security Server with AES keys $K_{Firmware}$-SC and $K_{Firmware}$-MC. The credentials file is encrypted with the unique keys of the associated VUs ($\underline{KENC}_{\underline{UpdateVu}}$).

The cryptographic keys used for securing the data transfer as session keys are generated during the preceding mutual authentication process between the EFAS-4.0 and the external subject (see SF.IA_KEY and SF.GEN_SKEYS).

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.4 SF.EX_INT Integrity and Authenticity of Data Exchange

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

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

The data transfer between the EFAS-4.0 and

- tachograph cards is secured according to ISO/IEC 7816-4 (see [ISO7816]) to the extent as defined in [GST] CSM_021 – Retail-MAC as required in FCS_COP.1/TDES. SF.EX_INT verifies the integrity and authenticity of data imported from tachograph cards. Upon detection of card data integrity or authenticity error, SF.EX_INT generates an audit record compliant with FAU_GEN.1 and does not use the data as required in FDP_ITC.2/IS. SF.EX_INT exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity as required in FDP_ETC.2.
- the motion sensor is secured according to ISO/DIS 16844-3 (see [ISO16844]) and as required in FCS_COP.1/TDES and after proper authentication as required in FIA_UAU.2//MS, FIA_UAU.6/MS, FIA_UID.2/MS. SF.EX_INT verifies the integrity and authenticity of motion data imported from the motion sensor. Upon detection of a motion data integrity or authenticity error, SF.EX_INT generates an audit record and continues to use imported data as required in FDP_ITC.2/IS. .
- the external device is secured according to ISO/IEC 7816-4 (see [ISO7816]) to the extent as defined in [GST] CSM_021 – Retail-MAC as required in FCS_COP.1/TDES after mutual authentication between the VU and the external device.
- downloading equipment are secured according to PKCS#1 V2.0 and with hash algorithm SHA-1 as required in FCS_COP.1/RSA.
  (Note: The source equipment (EFAS-4.0) identification and its security certification (Member state and equipment) are also downloaded. The verifier of the data must possess a trusted European public key to verify the certificate chain.)

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

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

update patch contains two files. The firmware image file is encrypted by the Security Server (see SF.EX_CONF above) and secured additionally (AES CMAC) with an AES key KAuth. The credentials file is encrypted (see SF.EX_CONF above) and secured additionally (AES CMAC) with the unique key of the associated VUs ($KAUTH_{UpdateVu}$).

The cryptographic keys used for securing the data transfer for tachograph cards are session keys which are generated during the preceding mutual authentication process between the EFAS-4.0 and the tachograph card (see SF.IA_KEY, FCS_COP.1/RSA and SF.GEN_SKEYS).

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.5 SF.GEN_SKEYS Generation of Session Keys

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

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

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

- random numbers generated by the EFAS-4.0 and used in the key generation process have a high quality and
- symmetric keys generated by the TOE are checked by the TSF with regard to their cryptographic strength, and only cryptographically strong keys (with the required key length) will be accepted by the TSF.
- Calculation of a session key based on secrets stored in the TSF and in the external device and based on dynamic data portions provided by both components at connection time.

SF.GEN_SKEYS generates and managed session keys (TDES keys) in accordance with the cryptographic key derivation algorithms as specified in [ISO16844] and [CSM]. as required in FCS_CKM.1, FCS_CKM.2 and FCS_CKM.4. The deletion of keys takes place due value overwriting with “FF”.

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

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

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.6 SF.GEN_DIGSIG Generation of Digital Signatures optionally with Encryption

SF.GEN_DIGSIG provides a digital signature generation functionality based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024 bit as required in FCS_COP.1/RSA.
The digital signature function will be used for several purposes with different signature keys and different formats for the digital signature input:

- Explicit generation of digital signatures of data using the signature scheme with appendix (signature generation operation) according to the standard PKCS#1 V2.0 and with hash algorithm SHA-1.
- Within authentication processes between the EFAS-4.0 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 (see [ISO9796]) and with hash algorithm SHA-1.

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

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

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

- Within the authentication process between the EFAS-4.0 and the tachograph card for the generation of authentication tokens using the decryption primitive according to the standard PKCS#1 V2.0.

Signatures are generated and verified in compliance with FCS_COP.1/RSA, key access and its storage are compliant with FCS_CKM.3.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.7 SF.VER_DIGSIG Verification of Digital Signatures optionally with Decryption

SF.VER_DIGSIG provides a functionality to verify digital signatures based on asymmetric cryptography, particularly the RSA algorithm with a key length of 1024 bit.
The SF to verify a digital signature will be used for several purposes with different keys and different formats for the digital signature input:

- Explicit verification of digital signatures of data using the signature scheme with appendix (signature verification operation) according to the standard PKCS#1 V2.0 and with hash algorithm SHA-1.
- Within authentication processes between EFAS-4.0 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 (see [ISO9796]) 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 (see [ISO9796]) and with hash algorithm SHA-1.

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

- Within the authentication processes between EFAS-4.0 and tachograph card for the verification of authentication tokens using the decryption primitive according to the standard PKCS#1 V2.0.

Signatures are verified in compliance with FCS_COP.1/RSA, key access to EU.PK and its storage are compliant with FCS_CKM.3.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.8 SF.DATA_INT Stored Data Integrity Monitoring and Action

SF.DATA_INT 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

SF.DATA_INT includes hardware mechanisms of the SC which protect user data against manipulation. Such hardware mechanisms are features within the design and construction which make reverse-engineering and tamper attacks more difficult. These features comprise dedicated shielding techniques and different scrambling features for the memory blocks.
SF.DATA_INT protects the user data stored in the data memory of the MC by AES CMAC values which are calculated about the data and stored in the MC together with the data. The CMAC-key is stored in the SC, also CMAC-verification of stored data is done in the SC (FCS_COP.1/AES).

SF.DATA_INT protects the user data stored in the SC by checksums and/or double storage.
The integrity of the user data is checked regularly and before data download.
SF.DATA_INT is implemented with ensuring the fulfilment of the SFRs FDP_SDI.2 and FAU_STG.1. Upon detection of a stored user data integrity error, SF.DATA_INT generates an audit record in accordance with FAU_GEN.1 and FAU_STG.1.
SF.DATA_INT overwrites the oldest stored audit records, if the audit trail is full.

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

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.9 SF.IA_KEY Key Based User / TOE Authentication

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

a) **Initial motion sensor identification and authentication (pairing, calibration)**:
The EFAS-4.0 authenticates the motion sensor it is connected to:

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

Authentication is mutual and triggered by the EFAS-4.0 before allowing any other TSF-mediated actions in accordance with FIA_UAU.2//MS (the identification as required in FIA_UID.2/MS takes place too). I.e. the TOE itself is also authenticated towards the motion sensor by means of a challenge-response procedure. Hereby, SF.IA_KEY detects and prevents use of authentication data that has been forged by or copied from any other user of the TSF (FIA_UAU.3/MS) and supports enforcing the SFP FUNCTION and SFP Input Sources to avoid value changes of security attributes (FMT_MSA.1, FMT_MSA.3/FUN and FMT_MSA.3/IS).

b) **User identification and authentication via tachograph card:**
The EFAS-4.0 identifies and authenticates its users at card insertion before allowing any other TSF-mediated actions in accordance with FIA_UID.2/TC, FIA_UAU.1/TC and FIA_UAU.5//TC as well as FIA_UAU.1/PIN. The authentication is mutual and triggered by the EFAS-4.0. I.e. the TOE itself is also authenticated towards the tachograph card by means of a challenge-response procedure. Hereby, SF.IA_KEY detects and prevents use of authentication data that has been forged by or copied from any other user of the TSF (FIA_UAU.3/TC), maintains the list of security attributes belonging to individual users as required by FIA_ATD.1//TC and supports enforcing the SFP FUNCTION to avoid value changes of security attributes (FMT_MSA.1). Authentication is performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. After this the EFAS-4.0 maintains the following roles DRIVER (driver card), CONTROLLER (control card), WORKSHOP (workshop card), COMPANY (company card) and UNKNOWN (no card inserted) as required by FMT_SMR.1//TC.

Note: The external authentication of the EFAS-4.0 corresponds to the internal authentication of the tachograph card and vice versa.

c) **External device identification and authentication:**
Before allowing any further interaction, the EFAS-4.0 shall successfully authenticate the external device. Authentication shall be mutual. I.e. the TOE itself is also authenticated towards the external device by means of a challenge-response procedure.

Cryptography:
In the cases

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

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

c) SF.IA_KEY makes use of symmetric cryptography for mutual authentication between the VU and the external device as well as for data integrity during data exchange between the EFAS-4.0 and the external device.

Cryptographic Protocol:

In the case a):
SF.IA_KEY applies the **initial identification and authentication** as described in chapter 7.4 of ISO/DIS 16844-3 (see [ISO16844]).
The extended serial-number N_S of the motion sensor is sent to the EFAS-4.0. The EFAS-4.0 encrypts the extended serial number N_S of the motion sensor, using the "identification key" K_{ID}. The motion sensor transmits a pairing key K_P which is encrypted with the "master key" K_M to the EFAS-4.0.

The "session key" K_S is transmitted from the EFAS-4.0 to the motion sensor encrypted with the "pairing key" K_P. Pairing information is transmitted from the EFAS-4.0 to the motion sensor encrypted with the "pairing key" in a way as required in FCS_CKM.2 and FDP_ETC.2.
The initial identification and authentication leads to the generation of a "session key" K_S which secures a challenge response mechanism for the following communication between the EFAS-4.0 and the motion sensor.

In the case b):
SF.IA_KEY operates as described in [EU], Appendix 11 ("Get Challenge Operation", "Generation of a digital signature" and "Encryption" for the internal authentication, "Random generation of the EFAS-4.0", "Decryption" and "Verification of a digital signature" for the external authentication.
The private key necessary on the EFAS-4.0´s side for authentication purposes is stored on the EFAS-4.0 and is implicitly connected with the corresponding commands. The access to the keys is controlled by the SFP FUNCTION, which is realised by SF.ACS.

The combination of a successful internal authentication process followed by a successful external authentication process leads to the generation of a new session key (with sequence counter sent) which will be used to secure the following data transfer. The generation of session keys is task of SF.GEN_SKEYS.
For the tachograph card type "Workshop Card" the mutual authentication process described above is only possible after a successful preceding PIN based user authentication between user and Workshop Card. Since EFAS-4.0 only transfers the PIN from the keypad to the Workshop Card this belongs not to the TSF of EFAS-4.0.
Case c):
SF.IA_KEY uses a challenge response protocol with TDES-cryptographic mechanisms for calculation of a session key based on secrets stored in the SC and in the external device and based on dynamic data portions provided by both components at connection time (mutual authentication mechanism). Correct calculation and usage of the session key – shown in further communication - serves as proof of authenticity. Without proper authentication, communications will be aborted.

Unsuccessful authentication:

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

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

as required by FIA_AFL.1/MS.

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

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

as required by FIA_AFL.1/TC.

Case c)
In case of unsuccessful authentication the user will be informed as required by FIA_AFL.1/Remote.

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

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

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

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.10 SF.INF_PROT Residual Information Protection

SF.INF_PROT ensures that any previous information content of a resource used for operations in which security relevant material is involved in volatile memory in the SC of the EFAS-4.0, is explicitly erased (overwriting with “FF”) upon the allocation of a new resource as required in FDP_RIP.1. Furthermore temporarily active keys are distributed in accordance with FCS_CKM.3 and destroyed in accordance with FCS_CKM.4 as implemented by SF.GEN_SKEYS. The deletion of keys takes place due value overwriting with “FF”.

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

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.11 SF.FAIL_PROT Failure and Tampering Protection

SF.FAIL_PROT preserves a secure state when the following types of failures occur:

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

In the case described above, SF.FAIL_PROT

- generates an audit record (except when in calibration mode) compliant with FAU_GEN.1,
- preserve the secure state of the EFAS-4.0,
- maintain the security functions, related to components or processes still operational,
- preserve the stored data integrity

in compliance with FPT_FLS.1.

In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, SF.FAIL_PROT resets the EFAS-4.0 clearly as required by FPT_PHP.2//Power_Deviation.

SF.FAIL_PROT provides the capability to determine whether **physical tampering** has occurred in compliance with FPT_PHP.3. The EFAS-4.0 is designed such that the case open supervision circuit detects any “regular” case opening while the external supply voltage is connected or not and a corresponding audit record is generated (the audit record is generated and stored after power supply reconnection as required by FAU_GEN.1). All other physical tampering attempts can be easily detected by visual inspection.

After its activation, the EFAS-4.0 detects specified hardware manipulation (specified in the assurance class development, e.g. manipulation of the real time clock generating time stamps). In the case of sabotage of the real time clock, SF.FAIL_PROT generates an audit record as required by FAU_GEN.1 and the EFAS-4.0 will be blocked (other cases are specified in the assurance class development).

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.12 SF.SELFTEST Self Test

SF.SELFTEST provides the capability of running self tests during initial start-up, and during normal operation to verify its correct operation (FPT_TST.1).
The EFAS-4.0 self tests include the verification of the integrity of security data and the verification of stored executable code.
Security data are stored

- in the data memory of the SC

Executable code is stored

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

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

SF.SELFTEST ensures that only allowed tests are available (FMT_MOF.1) and preserves a secure state in the case that failures specified in RLB_203, RLB_210, RLB_211 take place (FPT_FLS.1).

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

- Class 0: Fatal error, main processor, SC, ROM, Flash defect. EFAS-4.0 operation and data logging not possible.
- Class 1: Serious faults in non-essential components of the EFAS-4.0. Restricted EFAS-4.0 operation possible (data logging not possible or only possible in an un-secured way).
- Class 2: Warning. Single components of the EFAS-4.0 are (temporarily) not available. EFAS-4.0 operation is possible (with data logging).
- Class 3: No error.

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

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

All commands, actions or test points, specific to the testing needs of the manufacturing phase of the EFAS-4.0 are disabled or removed before the EFAS-4.0 is activated in accordance with FMT_MOF.1. It is not possible to restore them for later use.
The SF is supported by SF.DATA_INT.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.1.13 SF.UPDATE VU Software Upgrade

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

The software update mechanism which is implemented in accordance with the SFR FMT_SMF.1/SW-Upgrade ensures that the update is performed only if the integrity and the authenticity of the patch data is confirmed by means of update credentials (FDP_ACF.1/SW-Upgrade, FPT_TDC.1/SW-Upgrade and FDP_ITC.2/SW-Upgrade). SF.UPDATE decrypts the loaded software components (FCS_COP.1/AES) and exchanges the corresponding parts of the software. In particular, the VU Software Upgrade takes place in the following manner:
The software update patch contains two files.
-The firmware image file is encrypted (AES in CBC mode) with a AES key KFirmware.
-The credentials file is encrypted with the unique key of the associated VUs ($KENC_{UpdateVu}$) using AES in CBC mode. Only one unique VU which contains this key is able to encrypt and to verify the credentials which contain among others the keys for further steps KAuth, $\underline{K_{Firmware}}$-SC and $\underline{K_{Firmware}}$-MC.
$\underline{K_{Firmware}}$-SC and $\underline{K_{Firmware}}$-MC
In the first step, after decryption of the credentials file ($KENC_{UpdateVu}$) the integrity and authenticity of the credentials ($KAUTH_{UpdateVu}$) are verified. If all checks are positive the firmware images are decrypted (for SC and MC separately with $\underline{K_{Firmware}}$-SC and $\underline{K_{Firmware}}$-MC) and the integrity (and the authenticity indirectly) of the firmware image parts (KAuth) is verified. Only if all checks are positive, the update will take place.

The SF is effective only with support of the Security Functions of the SC, see 10.

9.2 Assurance Measures

To satisfy the security assurance requirements defined in section 8.2, suitable assurance measures are employed by the developer of the TOE. For the evaluation of the TOE, the developer provides suitable documents. The documents describe the measures and include further information supporting the verification of the conformance of these measures against the claimed assurance requirements.
The following table includes a mapping between the assurance requirements and the documents including the relevant information for the correspondent requirement. The developer of the TOE provides these documents.

Assurance Class	Family	Document(s) containing the relevant information
ADV Development	ADV_ARC.1	Security architecture description: 1030-120-SEC-DExx (Sicherheitsarchitektur)
	ADV_FSP.4	Complete functional specification: 1030-121-SEC-DExx (Funktionale Spezifikation)
	ADV_IMP.1	Implementation representation of the TSF: 1030-123-SEC-DExx (Darstellung der Implementierung)
	ADV_TDS.3	Basic modular design: 1030-122-SEC-DExx (TOE Design)
AGD Guidance Documents	AGD_OPE.1	Part of the Operating manual EFAS-4.0
	AGD_PRE.1	Operating manual EFAS-4.0 Service and installation manual EFAS-4.0
ALC Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation: 1030-110-SEC-DExx (Leistungsfähigkeit des Konfigurationsmanagements)
	ALC_CMS.4	Problem tracking CM coverage: 1030-111-SEC-DExx (Geltungsbereich des Konfigurationsmanagements)
	ALC_DEL.1	Delivery procedures: 1030-112-SEC-DExx (Auslieferung)
	ALC_DVS.1	Identification of security measures: 1030-113-SEC-DExx (Sicherheit in der Entwicklungsumgebung)
	ALC_LCD.1	Developer defined life-cycle model: Part of 1030-114-SEC-DExx (Lebenszyklus-Beschreibung und Werkzeuge und Techniken)
	ALC_TAT.1	Well-defined development tools: Part of 1030-114-SEC-DExx (Lebenszyklus-Beschreibung und Werkzeuge und Techniken)
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction

Assurance Class	Family	Document(s) containing the relevant information
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE Tests	ATE_COV.2	Analysis of coverage: Part of 1030-140-SEC-DExx (Testdokumentation)
	ATE_DPT.2	Testing: basic design: Part of 1030-140-SEC-DExx (Testdokumentation)
	ATE_FUN.1	Functional testing: Test specification and test records
	ATE_IND.2	Independent testing - sample: Samples of the TOE Source Code and Hardware
AVA Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis: Document Vulnerability Analysis

Table 10:Overview of Developers' TOE related Documents

9.3 TOE Summary Specification Rationale

9.3.1 Security Functions Rationale

The SF is effective only with support of the Security Functions of the SC see 10. The following section demonstrates that the set and combination of the defined TOE Security Functions is suitable to satisfy the identified TOE security functional requirements (SFRs). Furthermore, this section shows that each of the Security Functions is related to at least one security functional requirement.

The SFRs for the TOE of section 8.1 are related to the Security Functions of the TOE defined in chapter 9.1. The mapping of the SFRs for the TOE to the relevant Security Functions is done in the following.

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

PP and ST Security Functional Requirements (SFR)	TOE Security Functionality (TSF)
FAU_GEN.1	SF.ACS, SF.IA_KEY, SF.SECAUDIT, SF.DATA_INT, SF.SELFTEST, SF.FAIL_PROT, SF.EX_INT
FAU_SAR.1	SF.SECAUDIT
FAU_STG.1	SF.ACS, SF.DATA_INT
FAU_STG.4	SF.SECAUDIT
FCO_NRO.1	SF.GEN_DIGSIG, SF.EX_INT
FCS_CKM.1	SF.GEN_SKEYS
FCS_CKM.2	SF.IA_KEY, SF.GEN_SKEYS
FCS_CKM.3	SF.ACS, SF.INF_PROT, SF.GEN_DIGSIG , SF.VER_DIGSIG
FCS_CKM.4	SF.INF_PROT, SF.GEN_SKEYS
FCS_COP.1/TDES	SF.EX_INT, SF.EX_CONF, SF.IA_KEY
FCS_COP.1/AES	SF.DATA_INT, SF.EX_INT, SF.EX_CONF, SF.UPDATE
FCS_COP.1/RSA	SF.ACS, SF.EX_INT, SF.GEN_DIGSIG, SF.VER_DIGSIG, SF.IA_KEY
FDP_ACC.1/FIL	SF.ACS
FDP_ACC.1/FUN	SF.ACS
FDP_ACC.1/DAT	SF.ACS
FDP_ACC.1/UDE	SF.ACS
FDP_ACC.1/IS	SF.ACS
FDP_ACC.1/SW-Upgrade	SF.ACS, SF.UPDATE
FDP_ACF.1/FIL	SF.ACS
FDP_ACF.1/FUN	SF.ACS
FDP_ACF.1/DAT	SF.ACS
FDP_ACF.1/UDE	SF.ACS
FDP_ACF.1/IS	SF.ACS
FDP_ACF.1/SW-Upgrade	SF.ACS, SF.UPDATE
FDP_ETC.2	SF.IA_KEY, SF.EX_INT, SF.SECAUDIT
FDP_ITC.1	SF.ACS
FDP_ITC.2/IS	SF.ACS, SF.EX_INT
FDP_ITC.2/SW-Upgrade	SF.EX_INT, SF.EX_CONF, SF.UPDATE
FDP_RIP.1	SF.INF_PROT, SF.GEN_SKEYS
FDP_SDI.2	SF.SECAUDIT, SF.DATA_INT
FIA_AFL.1/MS	SF.IA_KEY
FIA_AFL.1/TC	SF.IA_KEY
FIA_AFL.1/Remote	SF.IA_KEY
FIA_ATD.1//TC	SF.IA_KEY
FIA_UAU.1/TC	SF.IA_KEY
FIA_UAU.1/PIN	SF.IA_KEY
FIA_UAU.2//MS	SF.IA_KEY, SF.EX_INT
FIA_UAU.3/MS	SF.IA_KEY
FIA_UAU.3/TC	SF.IA_KEY
FIA_UAU.5//TC	SF.IA_KEY

PP and ST Security Functional Requirements (SFR)	TOE Security Functionality (TSF)
FIA_UAU.6/MS	SF.IA_KEY, SF.EX_INT
FIA_UAU.6/TC	SF.IA_KEY
FIA_UID.2/MS	SF.IA_KEY, SF.EX_INT
FIA_UID.2/TC	SF.IA_KEY
FMT_MSA.1	SF.ACS, SF.IA_KEY
FMT_MSA.3/FUN	SF.IA_KEY, SF.ACS
FMT_MSA.3/FIL	SF.ACS
FMT_MSA.3/DAT	SF.ACS
FMT_MSA.3/IS	SF.IA_KEY, SF.ACS
FMT_MSA.3/UDE	SF.ACS
FMT_MOF.1	SF.SELFTEST
FMT_SMF.1/PP	SF.ACS
FMT_SMF.1/SW-Upgrade	SF.UPDATE
FMT_SMR.1//TC	SF.IA_KEY
FPR_UNO.1	SF.ACS
FPT_FLS.1	SF.SELFTEST, SF.FAIL_PROT
FPT_PHP.2//Power_Deviation	SF.FAIL_PROT
FPT_PHP.3	SF.FAIL_PROT
FPT_STM.1	SF.ACS, SF.SECAUDIT
FPT_TDC.1/IS	SF.ACS
FPT_TDC.1/SW-Upgrade	SF.UPDATE
FPT_TST.1	SF.SELFTEST
FRU_PRS.1	SF.ACS

Table 11: Coverage of Security Functional Requirements by TOE Security Functionality

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

FAU_GEN.1
SF.ACS contributes audit data through logging of events which deviate from the admissible FDP_ACC.1, SF.EX_INT contributes audit data through logging of data integrity faults, SF.IA_KEY contributes audit data through logging of authentication events, SF.FAIL_PROT contributes audit data through logging of assumed tampering events, SF.SELFTEST contributes audit data through logging of self-test failures.

The SF.SECAUDIT meets FAU_GEN.1 as it implements the SFR. In particular SF.SECAUDIT generates audit records as specified by the SFR.
SF.DATA_INT supports the SFR, it cares for the preservation of integrity of stored audit data.

FAU_SAR.1
SF.SECAUDIT meets FAU_SAR.1 as it implements the SFR. In particular SF.SECAUDIT allows for printing, displaying and downloading audit records.

FAU_STG.1

SF.ACS supports FAU_STG.1 as it denies unauthorised writing/deletion access to stored audit data records, in combination with SF.DATA_INT which contributes to the detection of modified or deleted audit records it implements the SFR.

FAU_STG.4
SF.SECAUDIT meets FAU_STG.4 as it implements the SFR.

FCO_NRO.1
SF.EX_INT implements the SFR FCO_NRO.1.
SF.GEN_DIGSIG allows for the generation of digital signatures as proof of origin.

FCS_CKM.1
SF.GEN_SKEYS directly implements FCS_CKM.1.

FCS_CKM.2
SF.IA_KEY and SF.GEN_SKEYS directly implement FCS_CKM.2.

FCS_CKM.3
SF.ACS as it denies unauthorised access to stored data. Authorised access takes place by the functions SF.GEN_DIGSIG, SF.VER_DIGSIG.
SF.INF_PROT as it explicitly erases security relevant material.

FCS_CKM.4
SF.GEN_SKEYS as it allows for implicit key destruction as soon as adequate.
SF.INF_PROT erases the temporarily needed and used keys.

FCS_COP.1/TDES
TDES algorithm is implemented and used by the functions SF.EX_INT, SF.EX_CONF and SF.IA_KEY in accordance with specified protocols and referenced standards.

FCS_COP.1/AES
AES algorithm is implemented and used by the function SF.DATA_INT, SF.EX_INT, SF.EX_CONF, SF.UPDATE in accordance with specified protocols and referenced standards.

FCS_COP.1/RSA
SF.EX_INT and SF.IA_KEY implement FCS_COP.1/RSA for tachograph card communication (see [GST] CSM_020), relying on SF.GEN_DIGSIG, SF.VER_DIGSIG, while SF.EX_INT and SF.GEN_DIGSIG fulfil [GST] CSM_032.

FDP_ACC.1/FIL
SF.ACS directly implements FDP_ACC.1/FIL

FDP_ACC.1/FUN
SF.ACS directly implements FDP_ACC.1/FUN.

FDP_ACC.1/DAT
SF.ACS directly implements FDP_ACC.1/DAT.

FDP_ACC.1/UDE
SF.ACS directly implements FDP_ACC.1/UDE.

FDP_ACC.1/IS
SF.ACS directly implements FDP_ACC.1/IS.

FDP_ACC.1/SW-Upgrade
SF.ACS and SF.UPDATE directly implement FDP_ACC.1/SW-Upgrade.

FDP_ACF.1/FIL
SF.ACS directly implements FDP_ACF.1/FIL.

FDP_ACF.1/FUN
SF.ACS directly implements FDP_ACF.1/FUN.

FDP_ACF.1/DAT
SF.ACS directly implements FDP_ACF.1/DAT.

FDP_ACF.1/UDE
SF.ACS directly implements FDP_ACF.1/UDE.

FDP_ACF.1/IS
SF.ACS directly implements FDP_ACF.1/IS.

FDP_ACF.1/SW-Upgrade
SF.ACS and SF.UPDATE directly implement FDP_ACF.1/SW-Upgrade.

FDP_ETC.2
SF.IA_KEY is used for preserving the validity of the authenticity proof, SF.EX_INT is used for securing the exported data against unauthorised change, SF.SECAUDIT provides everybody with the capability to read recorded information possibly secured as required in FDP_ETC.2.

FDP_ITC.1
SF.ACS directly implements FDP_ITC.1.

FDP_ITC.2/IS
SF.ACS directly implements the access control aspect of FDP_ITC.2/IS.
SF.EX_INT ensures that imported user data is authenticated towards the TOE.

FDP_ITC.2/SW-Upgrade
SF.EX_INT and SF.EX_CONF directly implement the FDP_ITC.2/SW-Upgrade.

FDP_RIP.1
SF.INF_PROT and SF.GEN_SKEYS directly implement FDP_RIP.1.

FDP_SDI.2
SF.SECAUDIT implements the audit record generation while SF.DATA_INT detects possible integrity violations.

FIA_AFL.1/MS
SF.IA_KEY directly implements FIA_AFL.1/MS.

FIA_AFL.1/TC
SF.IA_KEY directly implements FIA_AFL.1/TC.

FIA_AFL.1/Remote
SF.IA_KEY directly implements FIA_AFL.1/Remote

FIA_ATD.1//TC
SF.IA_KEY directly implements FIA_ ATD.1//TC.

FIA_UAU.1/TC
SF.IA_KEY directly implements FIA_UAU.1/TC.

FIA_UAU.1/PIN
SF.IA_KEY directly implements FIA_ UAU.1/PIN.

FIA_UAU.2//MS
SF.IA_KEY directly implements FIA_UAU.2//MS.
SF.EX_INT checks the integrity-association between data and originator.

FIA_UAU.3/MS
SF.IA_KEY directly implements FIA_UAU.3/MS.

FIA_UAU.3/TC
SF.IA_KEY directly implements FIA_UAU.3/TC.

FIA_UAU.5//TC
SF.IA_KEY directly implements FIA_UAU.5//TC.

FIA_UAU.6/MS
SF.IA_KEY directly implements FIA_UAU.6/MS
SF.EX_INT checks the integrity-association between data and originator.

FIA_UAU.6/TC
SF.IA_KEY directly implements FIA_UAU.6/TC

FIA_UID.2/MS
SF.IA_KEY directly implements FIA_UID.2/MS
SF.EX_INT checks the integrity-association between data and originator.

FIA_UID.2/TC
SF.IA_KEY directly implements FIA_UID.2/TC

FMT_MSA.1
SF.IA_KEY directly implements FMT_MSA.1
SF.ACS denies access to the stored data to everybody.

FMT_MSA.3/FUN
SF.IA_KEY directly implements FMT_MSA.3/FUN.
SF.ACS denies access to the stored data to everybody.

FMT_MSA.3/FIL
SF.ACS directly implements FMT_MSA.3/FIL

FMT_MSA.3/DAT
SF.ACS directly implements FMT_MSA.3/DAT

FMT_MSA.3/IS
SF.IA_KEY and SF.ACS directly implement FMT_MSA.3/IS

FMT_MSA.3/UDE
SF.ACS directly implements FMT_MSA.3/UDE

FMT_MOF.1
SF.SELFTEST directly implements FMT_MOF.1

FMT_SMF.1/PP
SF.ACS directly implements FMT_SMF.1/PP.

FMT_SMF.1/SW-Upgrade
SF.UPDATE directly implements FMT_SMF.1/SW-Upgrade.

FMT_SMR.1//TC
SF.IA_KEY relates authentication data to IDs and associated roles and thus fulfils FMT_SMR.1//TC.

FPR_UNO.1
SF.ACS directly implements FPR_UNO.1.

FPT_FLS.1
SF.SELFTEST preserves the secure state on internal faults ([GST] RLB_203).
SF.FAIL_PROT preserves the secure state on deviations of specific values for power supply or even interruptions ([GST] RLB_210, RLB_210).

FPT_PHP.2//Power_Deviation
SF.FAIL_PROT directly implements FPT_PHP.2//Power_Deviation

FPT_PHP.3
SF.FAIL_PROT directly implements FPT_PHP.3

FPT_STM.1
SF.ACS ensures that user data (here time information) may only be processed from the right input sources – VU's real time clock. SF.SECAUDIT is able to provide reliable time stamps.

FPT_TDC.1/IS
SF.ACS directly implements FPT_TDC.1/IS.

FPT_TDC.1/SW-Upgrade
SF.UPDATE directly implements FPT_TDC.1/SW-Upgrade.

FPT_TST.1
SF.SELFTEST directly implements FPT_TST.1.

FRU_PRS.1
SF.ACS directly implements FRU_PRS.1.

9.3.2 Assurance Measures Rationale

The assurance measures of the developer as referred in sections 8.2 and 9.2 are suitable and sufficient to meet the CC assurance level EAL4 augmented by AVA_VAN.5 and ATE_DPT.2 as claimed in section 8.2. In particular, the deliverables listed in chapter 9.2 are suitable and sufficient to document that the assurance requirements are met.

10 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the INFINEON Security Controller M7801 A12 [SCST].
It is made in strict accordance with [AIS36].

10.1 Relevance of Security Controller TSF

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

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

Table 12: Relevance of Security Controller TSF for Composite ST

Cryptographic support includes Triple-DES (relevant), AES (relevant), RSA (relevant), EC (not relevant), SHA-2 (SHA-256 and SHA512 – both not relevant), TRNG (relevant) and PRNG (not relevant).

10.2 Security Requirements

10.2.1 Security Functional Requirements

Security Functional Requirements of the TOE

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

FAU_GEN.1
FAU_SAR.1
FAU_STG.4
FCS_CKM.2
FCS_CKM.3
FCS_CKM.4
FDP_ETC.2
FDP_ITC.1
FDP_ITC.2/IS
FDP_ITC.2/SW-Upgrade
FIA_AFL.1/MS
FIA_AFL.1/TC
FIA_AFL.1/Remote
FIA_ATD.1//TC
FIA_UAU.1/TC
FIA_UAU.1/PIN
FIA_UAU.2//MS

FIA_UAU.3/MS
FIA_UAU.3/TC
FIA_UAU.5/TC
FIA_UAU.6/MS
FIA_UAU.6/TC
FIA_UID.2/MS
FIA_UID.2/TC
FMT_MOF.1
FMT_SMF.1/PP
FMT_SMF.1/SW-Upgrade
FMT_SMR.1//TC
FPT_STM.1
FPT_TDC.1/IS
FPT_TDC.1/SW-Upgrade
FRU_PRS.1

Security Functional Requirements of the Security Controller

FAU_SAS.1	not relevant, because not applicable, no conflict
FCS_RNG.1	covered by FCS_CKM.1
FCS_COP.1/DES	covered by FCS_COP.1/TDES
FCS_COP.1/AES	covered by FCS_COP.1/AES
FCS_COP.1/RSA	covered by FCS_COP.1/RSA
FCS_COP.1/ECDSA	not relevant, because not used, no conflict
FCS_COP.1/EC	not relevant, because not used, no conflict
FCS_COP.1/ECDH	not relevant, because not used, no conflict
FCS_COP.1/SHA	not relevant, because not used, no conflict
FCS_CKM.1/RSA	not relevant, because not used, no conflict
FCS_CKM.1/EC	not relevant, because not used, no conflict
FDP_ACC.1	covered by FDP_ACC.1/* (see table below)
FDP_ACF.1	covered by FDP_ACF.1/* (see table below)
FDP_IFC.1	covered by FDP_RIP.1, FPR_UNO.1
FDP_ITT.1	covered by FDP_RIP.1, FPR_UNO.1
FDP_SDI.1	covered by FDP_SDI.2, FAU_STG.1
FDP_SDI.2	covered by FDP_SDI.2, FAU_STG.1
FMT_LIM.1	covered by FDP_RIP.1, FPR_UNO.1
FMT_LIM.2	covered by FDP_RIP.1, FPR_UNO.1
FMT_MSA.1	covered by FMT_MSA.1
FMT_MSA.3	covered by FMT_MSA.3/* (see table below)
FMT_SMF.1	covered by FDP_ACC.1/*, FDP_ACF.1/* (see table below)
FPT_FLS.1	covered by FPT_FLS.1
FPT_ITT.1	covered by FDP_RIP.1, FPR_UNO.1
FPT_PHP.3	covered by FPT_PHP.2//Power_Deviation, FPT_PHP.3
FPT_TST.2	covered by FPT_TST.1
FRU_FLT.2	covered by FPT_FLS.1

Tracing of Security Controller SFRs to TOE SFRs

Security Controller SFRs / TOE SFRs	FCS_RNG.1	FCS_COP.1/DES	FCS_COP.1/AES	FCS_COP.1/RSA	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITT.1	FDP_SDI.1	FDP_SDI.2	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FPT_FLS.1	FPT_ITT.1	FPT_PHP.3	FPT_TST.2	FRU_FLT.2
FAU_STG.1									X	X										
FCS_CKM.1	X																			
FCS_COP.1/TDES		X																		
FCS_COP.1/AES			X																	
FCS_COP.1/RSA				X																
FDP_ACC.1/FIL					X										X					
FDP_ACC.1/FUN					X										X					
FDP_ACC.1/DAT					X										X					
FDP_ACC.1/UDE					X										X					
FDP_ACC.1/IS					X										X					
FDP_ACC.1/SW-Upgrade					X										X					
FDP_ACF.1/FIL						X									X					
FDP_ACF.1/FUN						X									X					
FDP_ACF.1/DAT						X									X					
FDP_ACF.1/UDE						X									X					
FDP_ACF.1/IS						X									X					
FDP_ACF.1/SW-Upgrade						X									X					
FDP_RIP.1							X	X			X	X					X			
FDP_SDI.2									X	X										
FMT_MSA.1													X							
FMT_MSA.3/FUN														X						
FMT_MSA.3/FIL														X						
FMT_MSA.3/DAT														X						
FMT_MSA.3/IS														X						
FMT_MSA.3/UDE														X						
FMT_MSA.3/SW-Upgrade														X						
FPR_UNO.1							X	X			X	X					X			
FPT_FLS.1																X				X
FPT_PHP.2//Power_Deviation																		X		
FPT_PHP.3																		X		

Security Controller SFRs / TOE SFRs	FCS_RNG.1	FCS_COP.1/DES	FCS_COP.1/AES	FCS_COP.1/RSA	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITT.1	FDP_SDI.1	FDP_SDI.2	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FPT_FLS.1	FPT_ITT.1	FPT_PHP.3	FPT_TST.2	FRU_FLT.2
FPT_TST.1																			X	

10.2.2 Security Assurance Requirements

The level of assurance of the TOE given in chapter 4 is EAL4 augmented with the components ATE_DPT.2 and AVA VAN.5.
The level of assurance of the Security Controller is EAL 5 augmented with the components ALC_DVS.2 and AVA_VAN.5 according to [SCST].
This shows that the Security Assurance Requirements of the TOE matches the Security Assurance Requirements of the hardware.

10.3 Security Objectives

Security Objectives for the Security Controller

O.Phys-Manipulation	Protection against Physical Manipulation:	No conflict.
O.Phys-Probing	Protection against Physical Probing:	No conflict.
O.Malfunction	Protection against Malfunction due to Environmental Stress:	No conflict.
O.Leak-Inherent	Protection against Inherent Information Leakage:	No conflict.
O.Leak-Forced	Protection against Forced Information Leakage:	No conflict.
O.Abuse-Func	Protection against Abuse of Functionality:	No conflict.
O.Identification	TOE Identification:	No conflict.
O.RND	Random Numbers:	No conflict.
O.Add-Functions	Additional specific security functionality:	No conflict.
O.Mem-Access	Area based Memory Access Control:	No conflict.

Security Objectives for the Security Controller Environment

OE.Process-Sec-IC	Protection during composite product manufacturing:	No conflict
OE.Plat-Appl	Usage of Hardware Platform:	No conflict
OE.Resp-Appl	Treatment of User Data:	No conflict

Security Objectives of the TOE

O.Access:	No conflict.
O.Accountability:	No conflict.
O.Audit:	No conflict.
O.Authentication:	No conflict.
O.Integrity:	No conflict.
O.Output:	No conflict.
O.Processing:	No conflict.
O.Reliability:	No conflict.
O.Secured_Data_Exchange:	No conflict.
O.Software_Analysis:	No conflict.
O.Software_Upgrade:	No conflict.

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

OE.Development	No conflict.
OE.Manufacturing	No conflict.
OE.Sec_Data_Generation	No conflict.
OE.Sec_Data_Transport	No conflict.
OE.Delivery	No conflict.
OE.Software_Upgrade	No conflict.
OE.Sec_Data_Strong	No conflict.
OE.Test_Points	No conflict.

Tracing of Security Controller objectives to TOE objectives

Objectives for the Security Controller hardware \ Objectives for the TOE	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
O.Phys-Manipulation			X			X	X	X		X	
O.Phys-Probing						X	X	X		X	
O.Malfunction		X	X		X	X		X			
O.Leak-Inherent	X					X	X	X		X	
O.Leak-Forced	X		X			X	X	X		X	
O.Abuse-Func	X	X	X		X	X	X	X		X	
O.RND	X	X	X		X	X	X	X	X	X	
O.Add-Functions									X		X
O.Mem-Access	X						X	X	X	X	X

Table 13: Mapping of Security Controller objectives to TOE objectives

The security objectives of the design and manufacturing environment of the TOE include in general meaning parts of the security objectives of the Security Controller. Other parts are covered by the security objectives of the TOE (O.Access, O.Authenticate, O.Integrity, O.Processing, O.Secured_Data_Exchange, O.Software_Analysis, O.Software_Upgrade), see assumption section 10.4.1.
The security objective of the Security Controller O.Identification can not be mapped because it is related to the production life cycle phase only.

10.4 Compatibility: TOE security environment

10.4.1 Assumptions

The following list shows that neither assumption of the TOE nor of the Security Controller has any conflicts between each other. They are covered by appropriate Security Objectives.

Assumptions of the Security Controller hardware

A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation:	No conflict
A.Plat-Appl	Usage of Hardware Platform:	No conflict
A.Resp-Appl	Treatment of User Data:	No conflict
A.Key-Function	Usage of Key-dependent Functions:	No conflict

Assumptions of the TOE

A.Activation	Activation of the TOE:	No conflict
A.Approved_Workshop	Approved workshops:	No conflict
A.Card_Availability	Availability of Tachograph Cards:	No conflict
A.Card_Tracebility	Tracebility of delivered Tachograph Cards:	No conflict
A.Controls	Law conformance controls:	No conflict
A.Driver_Card_Uniqueness	Uniqueness of the driver card:	No conflict
A.Faithful_Calibration	Faithful calibration:	No conflict
A.Faithful_Drivers	Faithful drivers:	No conflict
A.Regular_Inspections	Regular inspection and calibration:	No conflict

The assumptions do not have conflicts because it is obviously that the assumptions are made for different levels - controller level without respect to an application and Tachograph application level.

Tracing of Security Controller assumptions to Security Objectives

Assumptions for the Security Controller	Security Objectives of the TOE and environment covering them
A.Process-Sec-IC	OE.Development, OE.Manufacturing, OE.Sec_Data_Transport
A.Plat-Appl	OE.Development, OE.Manufacturing, OE.Sec_Data_Transport
A.Resp-Appl	OE.Development, OE.Manufacturing, OE.Test_Points, O.Access, O.Authenticate, O.Integrity, O.Processing, O.Secured_Data_Exchange, O.Software_Analysis, O.Software_Upgrade
A.Key-Function	OE.Development, OE.Manufacturing, OE.Sec_Data_Transport, OE.Test_Points, O.Access, O.Authenticate, O.Integrity, O.Secured_Data_Exchange, O.Software_Analysis, O.Software_Upgrade

Table 14: Mapping of Security Controller assumptions to TOE objectives

10.4.2 Threats

The threats of the TOE and the Security Controller have no conflicts between each other. They are shown in the following.

Threats of the Security Controller

T.Phys-Manipulation	Physical Manipulation:	No conflict
T.Phys-Probing	Physical Probing:	No conflict
T.Malfunction	Malfunction due to Environmental Stress:	No conflict
T.Leak-Inherent	Inherent Information Leakage:	No conflict
T.Leak-Forced	Forced Information Leakage:	No conflict
T.Abuse-Func	Abuse of Functionality:	No conflict
T.RND	Deficiency of Random Numbers:	No conflict
T.Mem-Access	Memory Access Violation:	No conflict

Threats of the TOE

T.Card_Data_Exchange:	No conflict
T.Faults:	No conflict
T.Output_Data:	No conflict
T.Access:	No conflict
T.Calibration_Parameters:	No conflict
T.Clock:	No conflict
T.Design:	No conflict
T.Environment:	No conflict
T.Fake_Device:	No conflict
T.Hardware:	No conflict
T.Identification:	No conflict
T.Motion_Data:	No conflict
T.Power_Supply:	No conflict
T.Security_Data:	No conflict
T.Software:	No conflict
T.Stored_Data:	No conflict
T.Tests:	No conflict
T.Non_Activated:	No conflict

Tracing of Security Controller threats to TOE threats

Threats for the TOE / Threats for the Security Controller hardware	T.Card_Data_Exchange	T.Faults	T.Output_Data	T.Access	T.Calibration_Parameters	T.Clock	T.Design	T.Environment	T.Fake_Device	T.Hardware	T.Identification	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	T.Tests	T.Non_Activated
T.Phys-Manipulation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
T.Phys-Probing	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	
T.Malfunction	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	
T.Leak-Inherent	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	
T.Leak-Forced	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	
T.Abuse-Func	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	
T.RND	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X	
T.Mem-Access	X	X		X	X	X	X	X	X	X		X	X	X	X	X	X	

Table 15: Mapping of Security Controller threats to TOE threats

The results are not unexpected, because all security features of the Security Controller are important for and used by the TOE. The whole security of the TOE is based on the security of the Controller. If the Security Controller would not be able to counter one of its threats nearly all threats could not be countered by the TOE.

10.4.3 Organisational Security Policies

The Organisational Security Policies of the TOE and the Security Controller have no conflicts between each other. They are shown in the following list.

Organisational Security Policies of the Security Controller

P.Process-TOE	Protection during TOE Development and Production:	No conflict.
P.Add-Functions	Additional Specific Security Functionality:	No conflict.

Organisational Security Policies of the TOE

OSP.Accountability:	No conflict.
OSP.Audit:	No conflict.
OSP.Processing:	No conflict.
OSP.Test_Points:	No conflict.
OSP.Type_Approved_MS:	No conflict.
OSP.SW_Upgrade:	No conflict.
OSP.PKI:	No conflict.
OSP.MS_Keys:	No conflict.

Tracing of Security Controller objectives to TOE objectives

OSPs for the Security Controller \ OSPs for the TOE	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.SW_Upgrade	OSP.PKI	OSP.MS_Keys	Not applicable
P.Process-TOE (Protection during TOE Development and Production)									X
P.Add-Functions (Additional Specific Security Functionality)						X			
Not applicable	X	X	X	X	X		X	X	

Table 16: Mapping of Security Controller OSPs to TOE OSPs

10.5 Conclusion

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

11 Annex

11.1 Glossary and list of acronyms

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

OE.x	Security Objective of the Environment
OS	Operating System
OSP	Organisational security policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
RAD	Reference Authentication Data
RAM	Random Access Memory (loses data if detached from a power supply)
REQxxx	A requirement from [EU], where 'xxx' represents the requirement number.
ROM	Read Only Memory (stores data independent of a power supply)
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
RTC	Real time clock
SC	Security Controller
SEF	Security Enforcing Function
SF	Security Function
SFP	Security Function Policy (see CC part 2)
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
ToSS	TOE Security Service
TSF	TOE Security Functionality
T.x	Threat
UDI.PK	public key of the update issuer
UDI.SK	private key of the update issuer
VAD	Verification Authentication Data
VU	Vehicle Unit

11.2 Bibliography

[CC1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and general model, Version 3.1, July 2009

[CC2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation,
Part 2: Security functional components, Version 3.1, July 2009

[CC3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation,
Part 3: Security assurance components, Version 3.1, July 2009

[CM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 3, July 2009

[AIS36] Anwendungshinweise und Interpretationen zum Schema, AIS36, Version 3, 19.10.2010, Bundesamt für Sicherheit in der Informationstechnik

[CSM] Appendix 11 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Common Security Mechanisms

[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).

corrected by

Commission Regulation (EC) No 432/2004 of 5 March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport

corrected by

COMMISSION REGULATION (EC) No 68/2009 of 23 January 2009 adapting for the ninth time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport.

corrected by

COMMISSION REGULATION (EU) No 1266/2009 of 16 December 2009 adapting for the tenth time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Text with EEA relevance)

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

[GST] Appendix 10 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Generic Security Targets

[SCST] Security Target M7801 A12 including optional Software Libraries RSA - EC – SHA-2, Version 0.6, 2011-04-15, Hans-Ulrich Buchmüller

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

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

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

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

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

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

[ISO9796] ISO/IEC 9796-2 Information Technology . Security techniques . Digital signature schemes giving message recovery . Part 2: Mechanisms using a hash function. First edition: 1997

[ISO16844] ISO 16844-3 Road vehicles . Tachograph systems . Motion Sensor Interface. WD 3-20/05/99.

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

[PPT] Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)', BSI-CC-PP-0057, version 1.0 as of 13th July 2010

[TR-02102] Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI-Technische Richtlinie, Version 1.0, 20.06.2008

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

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

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