Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-ITSEC-0167-2004

for

Digital Tachograph DTCO 1381

from

Siemens VDO Automotive AG

Deutsches IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-ITSEC-0167-2004

for

Digital Tachograph DTCO 1381

from

Siemens VDO Automotive AG

IT Security Certified

SOGIS-MRA

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991* and the *Information Technology Security Evaluation Manual (ITSEM), Version, 1.0, September 1993*, extended by vehicle unit specific guidance.

Evaluation Results:	Functionality:	**according to Appendix 10 of Annex 1 (B) of Regulation (EC) no. 1360/2002, amending Regulation (EEC) no. 3821/85 on recording equipment in road transport;**
	Evaluation Level:	**E3**
	Minimum strength of mechanisms:	**high**

The rating of the strength of mechanisms does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The confirmed evaluation level only applies on the condition that all stipulations regarding generation, configuration and operation as far as specified in the Certification Results are kept and that the product is operated in the environment described, where one is specified.

This certificate is only valid in conjunction with the complete Certification Report.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 28. September 2004

The President of the Federal Office
for Information Security
In Vertretung

Samsel L.S.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991[5]
- Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993
- BSI certification: Application Notes and Interpretation of the Scheme (AIS / JIL)

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern on 15.7.1992 in the Gemeinsames Ministerialblatt 1992, p. 546

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Digital Tachograph DTCO 1381 has undergone the certification procedure at BSI.

The evaluation of the product Digital Tachograph DTCO 1381 was conducted by T-Systems GEI GmbH, BU ITC Security. The T-Systems GEI GmbH, BU ITC Security is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is Siemens VDO Automotive AG.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 28. September 2004

The confirmed evaluation level and minimum strength of mechanisms is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the evaluation levels and the confirmed strength of mechanisms, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-50.

The product Digital Tachograph DTCO 1381 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111 or via e-mail (zerti@bsi.de).

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Siemens VDO Automotive AG, Heinrich-Hertz-Str., 45, D-78052 Villingen-Schwenningen

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Security Target and Scope of the Evaluation....................................... 3

1.1 Security Target.. 3

1.2 Abbreviations and Definitions... 3

1.3 Product rationale 5

1.4 Subjects, objects, and access rights 12

1.5 Security Objectives and Threats 14

1.6 Physical, personnel or procedural means 16

1.7 Security Enforcing Functions 17

1.8 Definition of security mechanisms... 36

1.9 Minimum strength of security mechanisms 36

1.10 Level of assurance... 37

1.11 Rationale of SEFs 37

2 Evaluation Results 44

2.1 Effectiveness – Construction... 44

2.2 Effectiveness - Operation.. 45

2.3 Correctness - Construction - Development Process 46

2.4 Correctness - Construction - Development Environment 47

2.5 Correctness - Operation - Operational Documentation 48

2.6 Correctness - Operation - Operational Environment 48

3 Comments/Recommendations 49

4 Literature and References 50

1 Security Target[8] and Scope of the Evaluation

Chapter 1 and 2 of this document represents the complete Security Target [5] used for the evaluation.

1.1 Security Target

The security target contains a description of the Digital Tachograph DTCO 1381 (the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

The security target is based on the Vehicle Unit Generic Security Target, which is described in Appendix 10 [6] of Annex 1(B) [8] of Council Regulation (EC) No. 3821/85 amended by CR (EC) No. 1360/2002. The security target states the security functions and assumptions on the environment and describes how they are implemented in the Digital Tachograph DTCO 1381.

Requirements, referred to in the security target, are those of the body of Annex 1(B). For clarity of reading, duplication sometimes arises between Annex 1(B) body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex 1(B) body requirement referred by this security target requirement, the Annex 1(B) body requirement shall prevail.

Annex 1(B) body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

1.2 Abbreviations and Definitions

CAN	Controller Area Network
DTCO	Digital Tachograph
EQT_j.C	equipment certificate
EQT_j.SK	equipment private key
EQT_j.PK	equipment public key
EUR.PK	European public key
Km	Master key
Km_{vu}	Part of the Master key, will manage the pairing between a motion sensor and the vehicle unit
K_{id}	Individual device key for protection of the session key between motion sensor and vehicle unit
K_{sm}	Session key between motion sensor and vehicle unit
K_{st}	Session key between tachograph cards and vehicle unit

[8] The security target was made available by the sponsor.

LC display	Liquid Crystal display
MS_i.C	Member State certificate
PIN	Personal Identification Number
ROM	Read Only Memory
RTC	Real Time Clock
SEF	Security Enforcing Function
TBD	To Be Defined
TOE	Target Of Evaluation
VU	Vehicle Unit
Digital Tachograph	Recording Equipment.
Entity	A device connected to the VU (specific definition see S1).
Motion data	The data exchanged with the VU, representative of speed and distance travelled (specific definition see O17).
Motion Sensor	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.
Physically separated parts	Physical components of the vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys) (specific definition see O2,O3).
System	Equipment, people or organisations, involved in any way with the recording equipment.
Tachograph cards	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.
User	Users are to be understood as human user of the equipment. Normal users of the VU comprise drivers, controllers, workshops and companies (specific definition see S2).
User data	Any data, other than security data, recorded or stored by the VU, required by Chapter III.12. (specific definition

see O1, O4 to o16).

Vehicle Unit

The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.

1.3 Product rationale

1.3.1 Vehicle Unit description and method of use

The VU is intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. It is connected to a motion sensor, it exchanges vehicle's motion data with.

Users identify themselves to the VU using tachograph cards.

The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices.

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

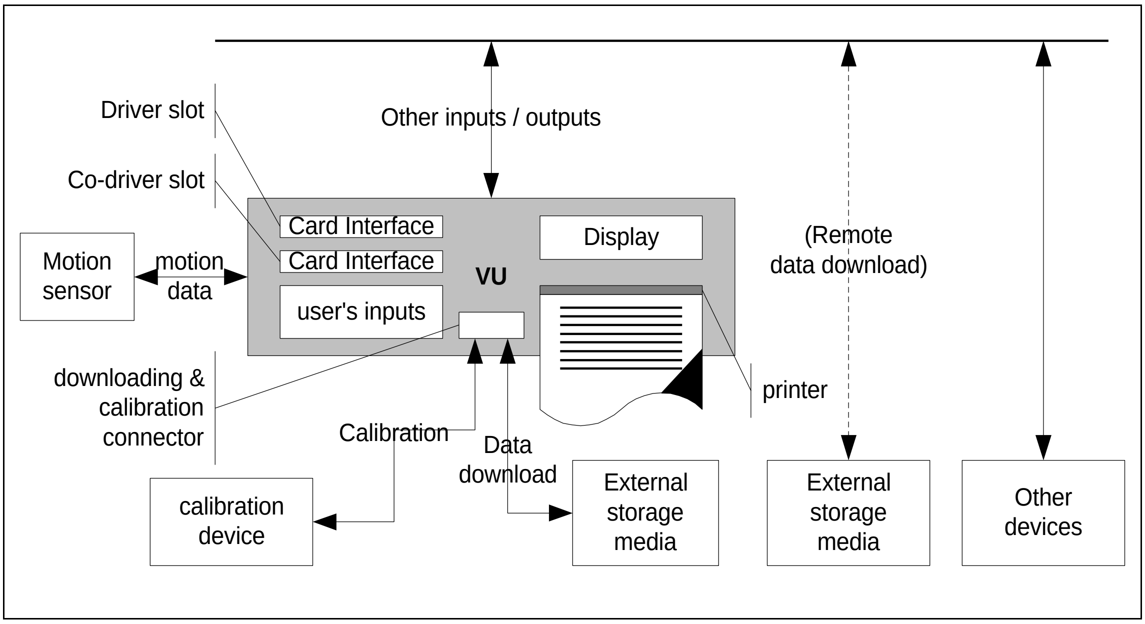

Figure 1 VU operational environment

The VU general characteristics, functions and modes of operation are described in Chapter II of Annex 1(B). The VU functional requirements are specified in Chapter III of Annex 1(B).

The typical VU is described in the figure 2 in the next chapter. It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

1.3.2 Realisation of the TOE

The following figure shows the basic architecture of the actual TOE, the vehicle unit DTCO 1381:

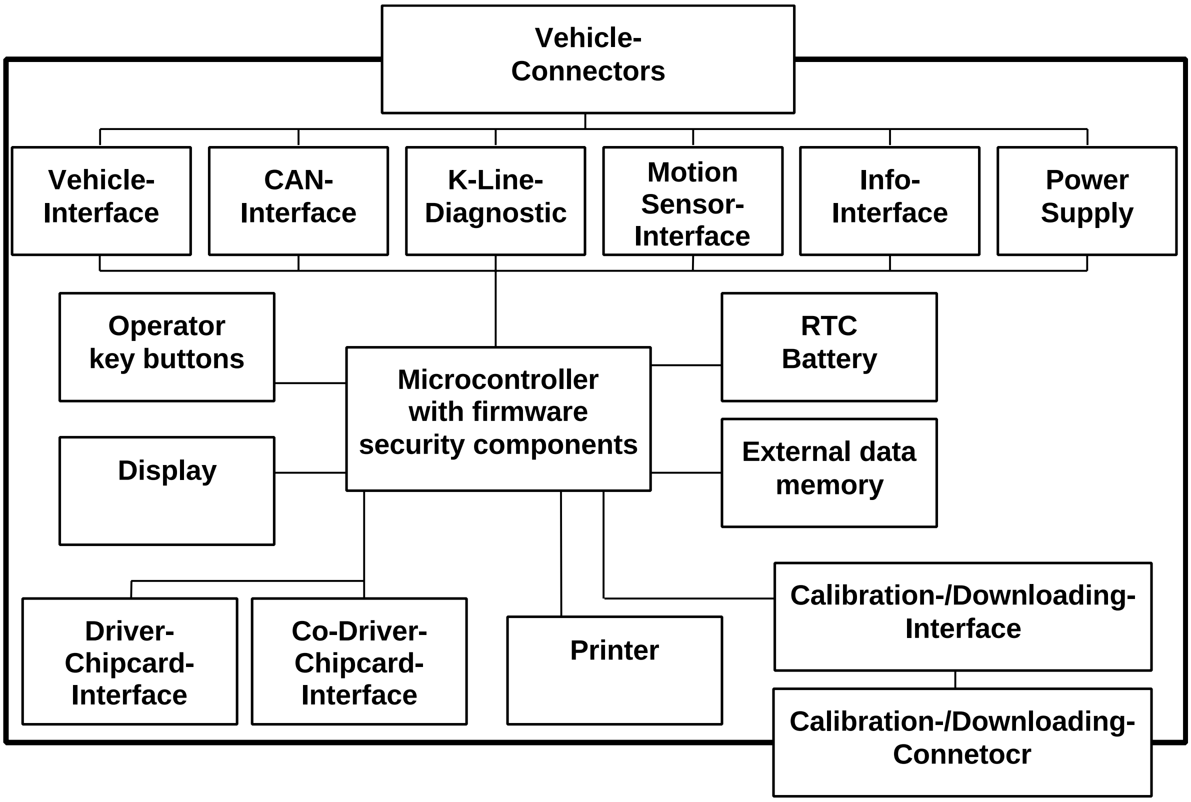

Figure 2 Basic architecture TOE DTCO 1381

The Scope of supply of the TOE includes the DTCO 1381 and the appropriate manuals.

1.3.3 General functions in the TOE

The following description shows the general functions implemented in the TOE.

(1) monitoring tachograph cards insertions and withdrawals
The TOE monitors two chip card interfaces (for a driver and a co-driver) to detect tachograph card insertions and withdrawals.
Upon tachograph card insertion the TOE detects:

- whether the card inserted is a valid tachograph card
- and in such a case identifies the card type.

(2) speed and distance measurement
Vehicle speed and distance are recorded using the real-time signal of the motion sensor.
The current speed value is stored every second in the data memory over a driving time of 24 hours. The speed resolution value is 1 km/h, the speed range is 0 km/h up to 220 km/h.
The distance resolution value is 0,1 km, the distance range is 0 km up to 9 999 999,9 km.
The TOE records speed profiles as an optional feature.

(3) time measurement

The TOE incorporates a real-time clock buffered by a battery. The basis for the measurement is the required UTC-format. The time resolution value is 1 sec.

(4) monitoring driver activities

The TOE permanently and separately monitors the activities of one driver and one co-driver as DRIVING, WORK, AVAILABILITY or BREAK/REST.
With the operator key buttons the driver and/or the co-driver can manually select WORK, AVAILABILITY or BREAK/REST.
When the vehicle is moving, the TOE selects automatically DRIVING for the driver and AVAILABILITY for the co-driver.

(5) monitoring driving status

The TOE selects the driving status CREW when two valid driver cards are inserted in the equipment, the driving status SINGLE is selected in any other case.

(6) drivers manual entries

With the operator key buttons on the front panel of the TOE the driver and/or the co-driver have the possibility to manually enter the places where the daily work periods begin and/or end.
After card insertion the cardholder can manually enter activities with their dates and times of beginning and end, among WORK or AVAILABILITY or BREAK/REST only, strictly included within the period last card withdrawal – current insertion only.
The driver can enter the following two specific conditions in real time: “OUT OF SCOPE” (begin, end) and “FERRY / TRAIN CROSSING”.

(7) company locks management

This function of the TOE manages the locks placed by a company to restrict data access in company mode to itself. Locking-in is possible at the insertion of a company card.
Locking-out is only possible for the company whose lock is “in” or if another company locks in. A previous locked-in company will then be automatically locked-out.

(8) monitoring control activities

This function of the TOE monitors DISPLAYING, PRINTING, VU and card DOWNLOADING activities carried out while in control mode. This function also monitors OVER SPEEDING CONTROL activities while in control mode.

(9) detection of events and/or faults

The following events and faults are detected and stored:

- "Insertion of a non valid card" event
- "Card conflict" event
- "Time overlap" event
- "Driving without an appropriate card" event
- "Card insertion while driving" event
- "Last card session not correctly closed" event
- "Over speeding" event
- "Power supply interruption" event
- "Motion data error" event
- "Security breach attempt" event
- "Card" fault
- "Recording equipment" fault includes
    - Internal fault
    - Printer fault

- Display fault
- Downloading fault
- Motion sensor fault

Additional specific faults (e.g. CAN-transmission-fault) are also detected and stored in the TOE.

(10) built-in and self tests
The TOE is provided with the capacity to detect automatically system malfunctions related to firmware, external data memory, chipcard interfaces, downloading and the motion sensor.

(11) reading from data memory
The TOE is able to read any data stored in its external data memory.

(12) recording and storing in data memory
The external data memory is used for recording all activities of both drivers (1 and 2) and the vehicle over a period of 365 calendar days under the assumptions of Annex 1 (B). The TOE is able to record and store the following data: (see O1 to O18).

(13) reading from tachograph cards
The TOE is able to read from tachograph cards the necessary data related to the functional requirements.

(14) recording and storing in tachograph cards
The TOE is able to record and store in tachograph cards the necessary data related to the functional requirements.

(15) displaying
The display is a LC display. There may be shown on the display different display menus and data.

(16) printing
The TOE incorporates a thermo-printer. The paper roll can be changed. The printouts can be selected and activated by use of display and operator keys.

(17) warning
The TOE warns the user when detecting any event and/or fault. It also warns the driver 15 minutes before and at the time of exceeding 4 h:30 min. continuous driving time. The warnings are visualised by the use of pictograms combined with text announcement and by the use of the display.

(18) data downloading to external media
The calibration-/downloading connector on the front is used for the downloading of the external data memory or a driver card contents during control, calibration and company mode. The TOE provides the downloading through its calibration-/ downloading interface.

(19) output data to additional external devices
The TOE is able to output data (e.g. speed and distance) to instrument clusters and to the vehicle. Other data can be output to other components via the vehicle connectors. The TOE is able to output data (e.g. driver activities) via a separated info-interface (external interface).

(20) calibration
The front calibration-/downloading connector is used for the calibration of the necessary parameters (w-factor, odometer, VIN etc.). The TOE provides the calibration through its calibration-/ downloading interface.
Furthermore, the functions of the equipment and the measuring of the signals are checked during periodic inspection (every two years) via this connector.
For calibration and measuring via this connector, approved tools (e.g. the MTC mobile test computer) will be available.
The calibration in calibration mode is also possible via K-line-diagnostic and CAN interface.

(21) time adjustment
The time adjustment function in the TOE allows the user to adjust the current time in amounts of one minute maximum at intervals of not less than seven days. Only in calibration mode this function is without limitation.

1.3.4 General functions in the TOE

A power saving mode is implemented as an additional, optional feature. It is only used by vehicle manufacturers, which need this feature. In this case the TOE is programmed at the Vehicle Unit manufacturer site to enable the power saving mode.
In the power saving mode the microcontroller changes its state between normal running and the so called interruptible power down mode, in which nearly the whole microcontroller is switched off and only some interrupts remain enabled to wake up the microcontroller.
By one of this interrupt-inputs the controller is cyclically waked up by a signal, generated by the real time clock RTC. Then it works out all of its normal functions and afterwards enters the power down mode again.
When the TOE is in the power saving mode, the display is switched off.
The power saving mode is only entered, when specific conditions are fulfilled.
The power saving mode is ended and the display is switched on, if one of these specific conditions for the entrance into this mode is no more fulfilled.
Some events make it necessary, respectively useful, to wake up the microcontroller directly by an interrupt and not to wait for the cyclic interrupt of the RTC.
These interrupt sources are separate inputs of the controller. So the reason for the wake up can be detected in the program.
All of the functions of the program of the TOE are performed too in the power saving mode with some exceptions.

1.3.5 Manuals

For the TOE exist the following manuals:

<u>Operating instructions:</u>

1. **BA00.1381.00 100 101-OPM 000 AA** for drivers/co-drivers and haulage companyas [9] a specification which gives the operating instructions for the driver/co- driver for normal usage and informs the driver/co-driver about the behaviour of the TOE as a specification to inform the staff of the haulage company about the behaviour of the TOE and gives the operating instructions for the staff of the haulage company for normal usage of the TOE by the company (company lock, data downloading, etc.).

2. **BA00.1381.00 200 101-OPM 000 AA** for control officers [10] as a specification to inform the control officers about the behaviour of the TOE and gives the operating

instructions for the national control authorities for normal usage of the TOE by control officers (data downloading, over speeding control, etc.).

3. Technical product manual **TD 00.1381.00 120 101-OPM 000 AA** [11]

This Manual contains a description of the process to

- install the TOE into the vehicle,
- activate the TOE,
- pair the TOE with the motion sensor,
- calibrate the TOE (with the description of default parameters) and
- carry out the periodic inspection of the TOE.

This manual is the guidance document for authorised workshop staff, fitters and vehicle manufacturers.

1.3.6 Life Cycle of the Digital Tachograph DTCO 1381

The typical life cycle of the VU is described in the following figure:

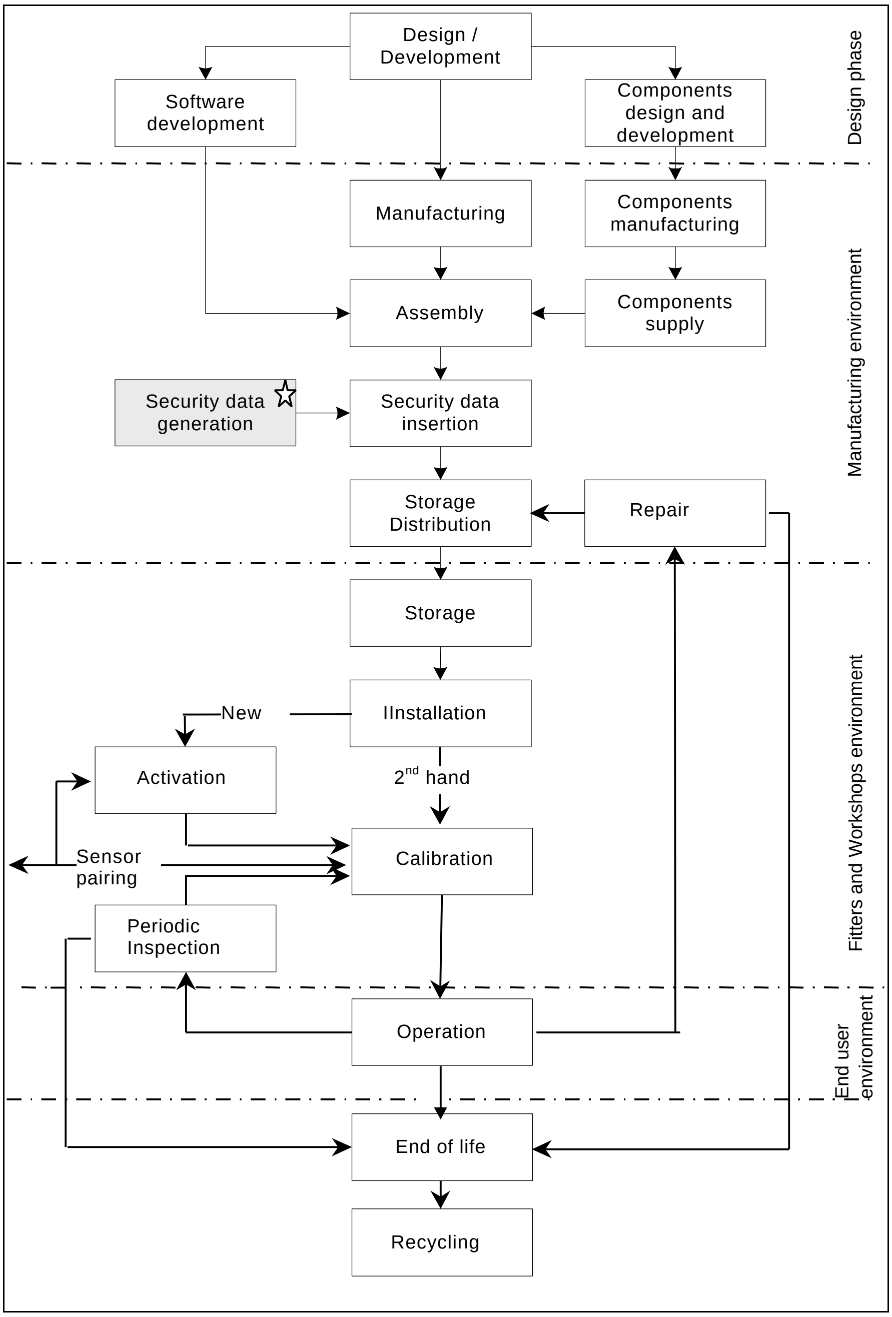

Figure 3 Life Cycle of the TOE DTCO 1381

For the TOE a repair in the fitters and workshop environments isn't planned. Fitters or workshops can only change elements of the TOE as e.g. front covers, printer.... Note: The security data generation is performed in a trusted environment in the production and the keys will be certified by the National Certification Authority.

1.4 Subjects, objects, and access rights

1.4.1 Subjects

For the TOE the following types of subjects exist:

S1 entities:

S1.1 installation device in the manufacturing process for storing objects O1, O2, O18 in the external data memory of the TOE

S1.2 motion sensor in pairing and operational mode

S1.3 calibration device (programming tools)

S1.4 intelligent dedicated equipment for downloading (e.g. personal computer)

S1.5 tachograph cards

S2 users:

S2.1 drivers and co-drivers (in operational mode)

S2.2 workshop staff , fitters and staff of vehicle manufacturers (in calibration mode)

S2.3 control officers from national control authorities (in control mode)

S2.4 staff of the respective haulage company (in company mode)

S2.5 unknown

Note: The human users S2.1 to S2.4 of the recording equipment in road transport vehicles identify themselves to the TOE using tachograph cards. Authentication and access control for those users is performed by TOE unit by identifying the type of tachograph cards.

1.4.2 Objects

For the specification of the security functions of the TOE the following objects are relevant. Definitions of data objects are provided in the Appendix 1 [12] of Annex 1(B).

O1 equipment identification data:

O1.1 vehicle unit identification data

O1.2 motion sensor identification data

O2 security elements to be stored in the TOE:

O2.1 european public key EUR.PK

O2.2 member State certificate MS_i.C

O2.3 equipment certificate EQT_j.C includes equipment public key EQT_j.PK

O2.4 equipment private key EQT_j.SK

O2.5 part of the Master key Km_{vu}

O3 security elements to generate and to be stored in the TOE:

O3.1 session key between motion sensor and vehicle unit K_{sm}

O3.2 session key between tachograph cards and vehicle unit K_{st}

O4 driver card insertion and withdrawal data

O5 driver activity data

O6 places where daily work periods start and/or end

O7 odometer data

O8 detailed speed data

O9 events data

O9.1 card conflict

O9.2 driving without an appropriate card

O9.3 card insertion while driving

O9.4 last card session not correctly closed

O9.5 over speeding

O9.6 power supply interruption

O9.7 motion data error

O9.8 security breach attempt

O10 faults data

O10.1 card fault

O10.2 recording equipment faults

O11 calibration data

O12 time adjustment data

O13 control activity data

O14 company locks data

O15 download activity data

O16 specific conditions data

O17 motion data representative of vehicle's speed and distance travelled

O18 individual device key K_{id}

O19 PIN from workshop card

1.4.3 Access rights

The Table 4 describes the access rights

	O1.1	O1.2	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	O12	O13	O14	O15	O16	O17	O18	O19
S1.1	w (once)		w (once)																w (once)	
S1.2		w		g/u														w/r	u	
S1.3												w/r	w/r							
S1.4																r				
S1.5						r	r			r	r	r	r	r	r	r	r			u
S2.1	r	r	u	g/u	w/r	w/r	w/r	w/r	w/r	w/r	w/r	r	r	r	r		w/r			
S2.2	r	r	u	g/u	w/r	w/r	w/r	w/r	w/r	w/r	w/r	w/r	w/r	r	r	w/r	w/r			u
S2.3	r	r	u	g/u	w/r	r	r	r	r	r	r	r	r	w/r	r	w/r	r			
S2.4	r	r	u	g/u	w/r	r	r	r	r	r	r	r	r	r	w/r	w/r	r			
S2.5						w	w	w	w	w	w						w			

r = read; w = write; g = generate, u = use

Table 4

1.5 Security Objectives and Threats

1.5.1 Threats

This paragraph describes the threats the VU may face.

1.5.1.1 Threats to identification and access control policies

T.Access Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function).

T.Identification Users could try to use several identifications or no identification.

1.5.1.2 Design related threats

T.Faults Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.

T.Tests The use of non invalidated test modes or of existing back doors could compromise the VU security.

T.Design Users could try to gain illicit knowledge of design either from manufacturer’s material (through theft, bribery, …) or from reverse engineering.

1.5.1.3 Operation oriented threats

T.Calibration_Parameters Users could try to use mis-calibrated equipment (through calibration data modification or through organisational weaknesses).

T.Card_Data_Exchange Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).

T.Clock Users could try to modify internal clock.

T.Environment Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).

T.Fake_Devices Users could try to connect faked devices (motion sensor, smart cards) to the VU.

T.Hardware Users could try to modify VU hardware.

T.Motion_Data Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).

T.Non_Activated Users could use non activated equipment.

T.Output_Data Users could try to modify data output (print, display or download).

T.Power_Supply Users could try to defeat the VU security objectives by modifying (cutting, reducing, increasing) its power supply.

T.Security_Data Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.

T.Software Users could try to modify VU software.

T.Stored_Data Users could try to modify stored data (security or user data).

1.5.2 Security Objectives

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

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

Therefore the security objectives of the VU, contributing to the global security objective, are the following:

O.VU_Main The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

O.VU_Export The VU must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity.

1.5.2.1 Information Technology Security Objectives

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

O.Access The VU must control user access to functions and data.

O.Accountability The VU must collect accurate accountability data.

O.Audit The VU must audit attempts to undermine system security and should trace them to associated users.

O.Authentication The VU should authenticate users and connected entities (when a trusted path needs to be established between entities).

O.Integrity The VU must maintain stored data integrity.

O.Output The VU must ensure that data output reflects accurately data measured or stored.

O.Processing The VU must ensure that processing of inputs to derive user data is accurate.

O.Reliability The VU must provide a reliable service.

O.Secured_Data_ Exchange The VU must secure data exchanges with the motion sensor and with tachograph cards.

1.6 Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the VU.

1.6.1 Equipment Design

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

M.Manufacturing VU manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

1.6.2 Equipment delivery and activation

M.Delivery VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the VU is done in a manner which maintains IT security.

M.Activation Vehicle manufacturers and fitters or workshops must activate the VU after its installation before the vehicle leaves the premises where installation took place.

1.6.3 Security data generation and delivery

M.Sec_Data_Generation Security data generation algorithms must be accessible to authorised and trusted persons only. They must be cryptographic strong.

M.Sec_Data_Transport Security data must be generated, transported and inserted into the VU in such a way to preserve its appropriate confidentiality and integrity.

M.Sec_Data_Crypt Security data inserted into the VU must be cryptographic strong.

1.6.4 Cards delivery

M.Card_Availability Tachograph cards must be available and delivered to authorised persons only.

M.Driver_Card_Uniqueness Drivers must possess at one time one valid driver card only.

M.Card_Traceability Card delivery must be traceable (white lists, black lists) and black lists must be used during security audits.

1.6.5 Recording equipment installation, calibration and inspection

M.Approved_Workshops Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.

M.Regular_Inpections Recording equipment must be periodically inspected and calibrated.

M.Faithful_Calibration Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.

1.6.6 Equipment operation

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

1.6.7 Law enforcement control

M.Controls Law enforcement controls must be performed regularly and randomly and must include security audits.

1.6.8 Software upgrades

M.Software_Upgrade Software revisions must be granted security certification before they can be implemented in a VU.

1.7 Security Enforcing Functions

1.7.1 Identification and authentication

<SEF1> The TOE provides this security enforcing function of identification and authentication of entities and human users.

This SEF includes the following features:

1.7.1.1 Motion sensor identification and authentication

UIA_201 The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.

UIA_202 The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.

UIA_203 The VU shall authenticate the motion sensor it is connected to:

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

Authentication shall be mutual and triggered by the VU.

UIA_204 The VU shall periodically (*period TBD by manufacturer: every 30 seconds, in calibration mode up to 45 minutes and more frequently than once per hour*) re-identify and re-authenticate the motion sensor it is connected to and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.

UIA_205 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_206 After (*TBD by manufacturer: 2 and not more than 20)* consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the SEF shall:

- generate an audit record of the event,
- warn the user,
- continue to accept and use non secured motion data sent by the motion sensor.

1.7.1.2 User identification and authentication

UIA_207 The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.

UIA_208 The user identity shall consist of:

- a user group:

  DRIVER (driver card),

  CONTROLLER (control card),

  WORKSHOP (workshop card),

  COMPANY (company card),

  UNKNOWN (no card inserted),

- a user ID, composed of :

  the card issuing Member State code and of the card number,

  UNKNOWN if user group is UNKNOWN.

UNKNOWN identities may be implicitly or explicitly known.

UIA_209 The VU shall authenticate its users at card insertion.

UIA_210 The VU shall re-authenticate its users:

- at power supply recovery,
- periodically or after occurrence of specific events (*TBD by manufacturers: every 12 hours and more frequently than once per day*).

UIA_211 Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.

UIA_212 In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PIN's shall be at least four characters long.

Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.

UIA_213 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_214 After five consecutive unsuccessful authentication attempts have been detected, the SEF shall:

- generate an audit record of the event,
- warn the user,
- assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007).

definition z in [8]

"non valid card" means:

a card detected as faulty, or which initial authentication failed, or which start of validity date is not yet reached, or which expiry date has passed.

requirement 007/008 in [8]

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

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

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

1.7.1.3 Remotely connected company identification and authentication

***This feature is not implemented in the TOE*.**

Company remote connection capability is optional. This paragraph therefore applies only if this feature is implemented.

UIA_215 For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.

UIA_216 The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.

UIA_217 The VU shall successfully authenticate the remotely connected company before allowing any data export to it.

UIA_218 Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.

UIA_219 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_220 After five consecutive unsuccessful authentication attempts have been detected, the VU shall warn the remotely connected company.

1.7.1.4 Management device identification and authentication

This feature is not implemented in the TOE.

VU manufacturers may foresee dedicated devices for additional VU management functions (e.g. software upgrading, security data reloading, …). This paragraph therefore applies only if this feature is implemented.

UIA_221 For every interaction with a management device, the VU shall be able to establish the device identity.

UIA_222 Before allowing any further interaction, the VU shall successfully authenticate the management device.

UIA_223 The VU shall detect and prevent use of authentication data that has been copied and replayed.

1.7.2 Access control

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

Requirement 011 of Annex 1(B):

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

- *in the operational mode, any personal identification (surname and first name(s)) not corresponding to a tachograph card inserted shall be blanked and any card number not corresponding to a tachograph card inserted shall be partially blanked (every odd character shall be blanked),*
- *in the company mode, driver related data can be output only for periods not locked by another company (as identified by the first 13 digits of the company card number),*
- *when no card is inserted in the recording equipment, driver related data can be output only for the current and 8 previous calendar days.*

<SEF2> The TOE provides this security enforcing function of access control for access to function and data of the TOE.

This SEF includes the following features:

1.7.2.1 Access control policy

ACC_201 The VU shall manage and check access control rights to functions and to data.

1.7.2.2 Access rights to functions

ACC_202 The VU shall enforce the mode of operation selection rules (requirements 006 to 009).

requirement 006 in [8] :

The recording equipment shall possess four modes of operation:
- *operational mode,*
- *control mode,*
- *calibration mode,*
- *company mode.*

requirement 007/008 in [8] :

see chapter 2.10.1.2 security enforcing function UIA_214

requirement 009 in [8] :

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

ACC_203 The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).

requirement 010 in [8] (the functions in the TOE as described in 2.3 are the same as listed in ([8], II.2)):

All functions listed in II.2. shall work in any mode of operation with the following exceptions:

- *the calibration function is accessible in the calibration mode only,*
- *the time adjustment function is limited when not in the calibration mode,*
- *the driver manual entries function are accessible in operational or calibration modes only,*
- *the company locks management function is accessible in the company mode only,*
- *the monitoring of control activities function is operational in the control mode only,*
- *the downloading function is not accessible in the operational mode.*

1.7.2.3 Access rights to data

ACC_204 The VU shall enforce the VU identification data write access rules (requirement 076)

requirement 076 in [8]:

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

ACC_205 The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)

requirement 079 in in [8]:

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

- *serial number,*
- *approval number,*
- *first pairing date,*

requirement 155 in [8]:

- *pairing the motion sensor to the VU shall consist, at least, in:*
- *updating motion sensor installation data held by the motion sensor (as needed),*
- *copying from the motion sensor to the VU data memory necessary motion sensor identification data.*

ACC_206 After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).

requirement 154 in [8]:

The calibration function shall allow:

- *to automatically pair the motion sensor with the VU,*
- *to digitally adapt the constant of the recording equipment (k) to the characteristic coefficient of the vehicle (w) (vehicles with two or more axle ratios shall be fitted with a switch device whereby these various ratios will automatically be brought into line with the ratio for which the equipment has been adapted to the vehicle),*

- *to adjust (without limitation) the current time,*
- *to adjust the current odometer value,*
- *to update motion sensor identification data stored in the data memory,*
- *to update or confirm other parameters known to the recording equipment: vehicle identification, w, l, tyre type and speed limiting device setting if applicable.*

requirement 156 in [8]:

The calibration function shall be able to input necessary data through the calibration/downloading connector in accordance with the calibration protocol defined in Appendix 8 [14]. *The calibration function may also input necessary data through other connectors.*

ACC_207 After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).

requirement 097 in [8]:

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

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

ACC_208 After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).

requirement 157 in [8]:

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

requirement 158 in [8]:

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

ACC_209 After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).

requirement 100 in [8]:

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

- *the most recent time adjustment,*
- *the five largest time adjustments, since last calibration,*

performed in calibration mode outside the frame of a full calibration.

ACC_210 The VU shall enforce appropriate read and write access rights to security data (requirement 080).

requirement 080 in [8]:

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

- *European public key,*
- *Member State certificate,*
- *Equipment certificate,*
- *Equipment private key.*

Recording equipment security elements are inserted in the equipment by the vehicle unit manufacturer.

1.7.2.4 File structure and access conditions

ACC_211 Application and data files structure and access conditions shall be created during the manufacturing process and then locked from any future modification or deletion.

1.7.3 Accountability

<SEF3> The TOE provides this security enforcing function of accountability for collection of accurate data in the TOE.

This SEF includes the following features:

ACT_201 The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087 105a, 105b 109 and 109a).

requirement 081 in [8]:

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

- *the card holder's name and first names as stored in the card,*
- *the card's number, issuing Member State and expiry date as stored in the card,*
- *the insertion date and time,*
- *the vehicle odometer value at card insertion,*
- *the slot in which the card is inserted,*
- *the withdrawal date and time,*
- *the vehicle odometer value at card withdrawal,*

the following information about the previous vehicle used by the driver, as stored in the card:

- *VRN and registering Member State,*
- *card withdrawal date and time;*
- *a flag indicating whether, at card insertion, the card holder has manually entered activities or not.*

requirement 084 in [8]:

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

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

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

requirement 087 in [8]:

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

- *if applicable, the (co-)driver card number and card issuing Member State,*
- *the date and time of the entry,*
- *the type of entry (begin or end),*

- *the country and region entered,*
- *the vehicle odometer value.*

requirement 105a in [8]:

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

- *Date and time of the entry,*
- *Type of specific condition.*

requirement 105b in [8]:

The data memory shall be able to hold specific conditions data for at least 365 days (with the assumption that on average, 1 condition is opened and closed per day). When storage capacity is exhausted, new data shall replace oldest data.

requirement 109 in [8]:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

requirement 109a in [8]:

The recording equipment shall update driver activity data (as specified in Chapter IV paragraph 5.2.5), stored on valid driver and/or workshop cards, with activity data manually entered by the cardholder.

ACT_202 The VU shall hold permanent identification data (requirement 075).

requirement 075 in [8]:

The recording equipment shall be able to store in its data memory the following vehicle unit identification data:

- *name of the manufacturer,*
- *address of the manufacturer,*
- *part number,*
- *serial number,*
- *software version number,*
- *software version installation date,*
- *year of equipment manufacture,*
- *approval number*

ACT_203 The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).

requirement 098 in [8]:

The following data shall be recorded for each of these calibrations:

- *Purpose of calibration (activation, first installation, installation, periodic inspection, other)*
- *workshop name and address,*
- *workshop card number, card issuing Member State and card expiry date,*
- *vehicle identification,*
- *parameters updated or confirmed: w, k, l, tyre type, speed limiting device setting, odometer (old and new values), date and time (old and new values).*

requirement 101 in [8]:

The following data shall be recorded for each of these time adjustments:

- *date and time, old value,*
- *date and time, new value,*
- *workshop name and address,*
- *workshop card number, card issuing Member State and card expiry date.*

requirement 109 in [8]:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

ACT_204 The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).

requirement 102 in [8]:

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

- *date and time of the control,*
- *control card number and card issuing Member State,*
- *type of the control (displaying and/or printing and/or VU downloading and/or card downloading).*

requirement 103 in [8]:

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

requirement 109 in [8]:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

ACT_205 The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).

requirement 090 in [8]:

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

requirement 093 in [8]:

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

ACT_206 The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.

requirement 081 to 083 in [8]: *Driver card insertion and withdrawal data*

requirement 084 to 086 in [8]: *Driver activity data*

Places where daily work periods start and/or end

requirement 090 to 092 in [8]: *Odometer data*

requirement 093 in [8]: *Detailed speed data* *requirement 102 to 103 in [8]:* *Control activity data*

requirement 104 in [8]: *Company locks data*

requirement 105 in [8]: *Download activity data*

ACT_207 The VU shall ensure that it does not modify data already stored in a tachograph card (requirement 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1.Note [12].

requirement 109 in [8]:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

requirement 109a in [8]:

see ACT_201

requirement 110 in [8]:

Tachograph cards data update shall be such that, when needed and taking into account card actual storage capacity, most recent data replace oldest data.

1.7.4 Audit

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

<SEF4> The TOE provides this security enforcing function of audit related to attempts to undermine the security of the TOE and provides the traceability to associated users.

This SEF includes the following features:

Note: The security breach attempt "internal data transfer" does not apply to the TOE, because it does not make use of physically separated parts (see 6.6.2.).

AUD_201 The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).

requirement 094 in [8]:

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

Event	***Storage rules***	***Data to be recorded per event***
Card conflict	- *the 10 most recent events.*	- *date and time of beginning of event,* - *date and time of end of event,* - *cards' type, number and issuing Member State of the two cards creating the conflict.*
Driving without an appropriate card	- *the longest event for each of the 10 last days of occurrence,* - *the 5 longest events over the last 365 days.*	- *date and time of beginning of event,* - *date and time of end of event,* - *cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,* - *number of similar events that day.*
Card insertion while driving	- *the last event for each of the 10 last days of occurrence,*	- *date and time of the event,* - *card's type, number and issuing Member State,* - *number of similar events that day*
Last card session not correctly closed	- *the 10 most recent events.*	- *date and time of card insertion,* - *card's type, number and issuing Member State,* - *last session data as read from the card:* - *date and time of card insertion,* - *VRN and Member State of registration.*

Over speeding (1)	- *the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed),* - *the five most serious events over the last 365 days.* - *the first event having occurred after the last calibration*	- *date and time of beginning of event,* - *date and time of end of event,* - *maximum speed measured during the event,* - *arithmetic average speed measured during the event,* - *card's type, number and issuing Member State of the driver (if applicable),* - *number of similar events that day*
Power supply interruption (2)	- *the longest event for each of the 10 last days of occurrence,* - *the five longest events over the last 365 days*	- *date and time of beginning of event,* - *date and time of end of event,* - *cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,* - *number of similar events that day*
Motion data error	- *the longest event for each of the 10 last days of occurrence,* - *the five longest events over the last 365 days*	- *date and time of beginning of event,* - *date and time of end of event,* - *cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,* - *number of similar events that day*

Security breach attempt	- *the 10 most recent events per type of event*	- *date and time of beginning of event,* - *date and time of end of event (if relevant),* - *cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,* - *type of event*

requirement 096 in [8]:

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

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

requirement 109 in [8]:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

AUD_202 The events affecting the security of the VU are the following:

- Security breach attempts:
  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorised change of motion sensor,

    - card data input integrity error,
    - stored user data integrity error,
    - internal data transfer error,
    - unauthorised case opening,
    - hardware sabotage,
- Last card session not correctly closed,
- Motion data error event,
- Power supply interruption event,
- VU internal fault.

AUD_203 The VU shall enforce audit records storage rules (requirement 094 and 096).

requirement 094 in [8]:

see security enforcing function AUD_201

requirement 096 in [8]:

see security enforcing function AUD_201

AUD_204 The VU shall store audit records generated by the motion sensor in its data memory.

AUD_205 It shall be possible to print, display and download audit records.

1.7.5 Object re-use

<SEF5> The TOE provides this security enforcing function of object reuse.

This SEF includes the following features:

REU_201 The VU shall ensure that temporary storage objects can be reused without this involving inadmissible information flow.

1.7.6 Accuracy

<SEF6> The TOE provides this security enforcing function of accuracy of stored data in the TOE.

This SEF includes the following features:

1.7.6.1 Information flow control policy

ACR_201 The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:

- vehicle motion data,
- VU's real time clock,
- recording equipment calibration parameters,

- tachograph cards,
- user's inputs.

__requirement 081, 084, 087, 105, 105a, 109 in [8]:__

see chapter 2.10.3 security enforcing function ACT_201

__requirement 102 in [8]:__

see chapter 2.10.3 security enforcing function ACT_204

__requirement 090, 093 in [8]:__

see chapter 2.10.3 security enforcing function ACT_205

__requirement 104 in [8]:__

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

- *lock-in date and time,*
- *lock-out date and time,*
- *company card number and card issuing Member State,*
- *company name and address.*

ACR_201a The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).

__requirement 109a in [8]:__

see chapter 2.10.3 security enforcing function ACT_201

__requirement 50a in [8]:__

Upon driver (or workshop) card insertion, and only at this time, the recording equipment shall remind to the cardholder the date and time of his last card withdrawal and the activity selected at that time, and shall prompt the cardholder for a "Declaration ?". If the prompt is negatively answered, the recording equipment shall require the cardholder to confirm his answer. If the prompt is positively answered, the recording equipment shall:

- *allow the cardholder to manually enter activities, with their dates and times of beginning and end, among WORK or AVAILABILITY or BREAK/REST only, strictly included within the period last card withdrawal – current insertion only,*
- *allow the cardholder to modify or delete any such activities manually entered, until validation by selection of a specific command, and then forbid any such modification,*
- *not allow entry of activities that overlap activities already entered.*

A positive answer to the prompt followed by no activity entries, shall be interpreted by the recording equipment as a negative answer to the prompt.

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

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

- *if the card is withdrawn or another driver (or workshop) card is inserted or*
- *as soon as the vehicle is moving,*

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

1.7.6.2 Internal data transfers

The requirements of this paragraph apply only if the VU makes use of physically separated parts.

ACR_202 If data are transferred between physically separated parts of the VU, the data shall be protected from modification.

ACR_203 Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

***Since the TOE is a single protected entity, this requirement does not apply for the TOE*.**

1.7.6.3 Stored data integrity

ACR_204 The VU shall check user data stored in the data memory for integrity errors.

ACR_205 Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

1.7.7 Reliability of service

<SEF7> The TOE provides this security enforcing function of reliability of service

This SEF includes the following features:

1.7.7.1 Tests

RLB_201 All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. It shall not be possible to restore them for later use.

RLB_202 The VU shall run self tests, during initial start-up and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).

RLB_203 Upon detection of an internal fault during self test, the SEF shall:

- generate an audit record (except in calibration mode) (VU internal fault),
- preserve the stored data integrity.

1.7.7.2 Software

RBL_204 There shall be no way to analyse or debug software in the field after the VU activation.

RLB_205 Inputs from external sources shall not be accepted as executable code.

1.7.7.3 Physical protection

RLB_206 If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 six months. In such a case, the SEF shall generate an audit record. (It is acceptable that the audit record is generated and stored after power supply reconnection).

If the VU is designed so that it cannot be opened, it shall be designedsuch that physical tampering attempts can be easily detected (e.g. through visual inspection).

RLB_207 After its activation, the VU shall detect specified (*TBD by manufacturer*) hardware sabotage:

- Presence of the display,
- Presence of the printer,
- Manipulation of the mechanisms for the cart reader.

RLB_208 In the case described above, the SEF shall generate an audit record and the VU shall: (*TBD by manufacturer*).

For the display:
The audit record is submitted to the display and is stored in the memory for event and faults.

For the printer:
The audit record is displayed and stored in the memory for event and faults. An on-going pront out is stopped and a new print out is not started.

For the mechanisms of the cart reader:
The audit record is displayed and stored in the memory for event and faults. If possible the data will be stored on the tachograph card and than the tachograph card withdrawals.

1.7.7.4 Power supply interruptions

RLB_209 The VU shall detect deviations from the specified values of the power supply, including cut-off.

RLB_210 In the case described above, the SEF shall:

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

1.7.7.5 Reset conditions

RLB_211 In case of a power supply interruption or if a transaction is stopped before completion or on any other reset conditions, the VU shall be reset cleanly.

1.7.7.6 Data availability

RLB_212 The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

RLB_213 The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).

requirement 015 in [8]:

The recording equipment shall be so designed that the tachograph cards are locked in position on their proper insertion into the card interface devices.

requirement 016 in [8]:

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 on behalf of the release.

RLB_214 In the case described above, the SEF shall generate an audit record of the event.

1.7.7.7 Multiple applications

The VU provides only the tachograph application.

RLB_215 If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.

1.7.8 Data exchange

This paragraph addresses data exchange between the VU and connected devices.

<SEF8> The TOE provides this security enforcing function of data exchange with connected entities.

This SEF includes the following features:

1.7.8.1 Data exchange with motion sensor

DEX_201 The VU shall verify the integrity and authenticity of motion data imported from the motion sensor.

DEX_202 Upon detection of a motion data integrity or authenticity error, the SEF shall:

- generate an audit record,
- continue to use imported data.

1.7.8.2 Data exchange with tachograph cards

DEX_203 The VU shall verify the integrity and authenticity of data imported from tachograph cards.

DEX_204 Upon detection of a card data integrity or authenticity error, the SEF shall:

- generate an audit record,
- not use the data.

DEX_205 The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

1.7.8.3 Data exchange with external storage media (downloading function)

DEX_206 The VU shall generate an evidence of origin for data downloaded to external media.

DEX_207 The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.

DEX_208 The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.

1.7.9 Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions.

<SEF9> The TOE provides this security enforcing function of cryptographic support.

This SEF includes the following features:

CSP_201 Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.

CSP_202 If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes

CSP_203 If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.

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

CSP_205 If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.

1.8 Definition of security mechanisms

The required security mechanisms are specified in Appendix 11 [15].
The TOE implements all necessary security mechanisms.

1.9 Minimum strength of security mechanisms

The minimum strength of the Vehicle Unit security mechanisms is **High**, as defined in ITSEC [1].

1.10 Level of assurance

The target level of assurance for the Vehicle Unit is ITSEC level **E3**, as defined in ITSEC [1].

1.11 Rationale of SEFs

The following matrixes give a rationale for the SEFs by showing:

- which SEFs or means counteract which threats,
- which SEFs fulfil IT security objectives.

	Threats																			IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Physical Personnel Procedural Means																												
Development			x	x	x																							
Manufacturing				x	x																							
Delivery													x															
Activation	x												x															
Security Data Generation																	x											
Security Data Transport																	x											
Security Data Crypt																	x											
Card Availability		x																										
One Driver Card		x																										
Card Traceability		x																										
Approved Workshops						x		x																				
Regular Inspection Calibration						x		x			x				x			x										
Faithful workshops						x		x																				
Faithful drivers		x														-												
Law enforcement controls		x				x		x	x		x		x		x	x	x											

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Software Upgrade																		x											
Security Enforcing Functions																													
<SEF1> Identification and Authentication																													
UIA_201	Sensor identification										x		x											x					x
UIA_202	Sensor identity										x		x											x					x
UIA_203	Sensor authentication										x		x											x					x
UIA_204	Sensor re-identification and re-authentication										x		x											x					x
UIA_205	Unforgeable authentication										x		x											x					
UIA_206	Authentication failure										x		x										x					x	
UIA_207	Users identification	x	x								x										x			x					x
UIA_208	User identity	x	x								x										x			x					x
UIA_209	User authentication	x	x								x										x			x					x
UIA_210	User re-authentication	x	x								x										x			x					x
UIA_211	Authentication means	x	x								x										x			x					
UIA_212	PIN checks	x	x				x		x												x			x					
UIA_213	Unforgeable authentication	x	x								x										x			x					

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
UIA_214	Authentication failure	x	x								x												x						
UIA_215	Remote user identification	x	x																		x			x					x
UIA_216	Remote user identity	x	x																		x			x					
UIA_217	Remote user authentication	x	x																		x			x					x
UIA_218	Authentication means	x	x																		x			x					
UIA_219	Unforgeable authentication	x	x																		x			x					
UIA_220	Authentication failure	x	x																										
UIA_221	Management device Identification	x	x																		x			x					
UIA_222	Management device Authentication	x	x																		x			x					
UIA_223	Unforgeable authentication	x	x																		x			x					
<SEF2> Access Control																													
ACC_201	Access control policy	x					x		x									x		x	x								
ACC_202	Access rights to functions	x					x		x												x								
ACC_203	Access rights to functions	x					x		x												x								
ACC_204	VU ID																			x	x								

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
ACC_205	Connected sensor ID										x									x	x								
ACC_206	Calibration data	x					x													x	x								
ACC_207	Calibration data						x													x	x								
ACC_208	Time adjustment data	X							x											x	x								
ACC_209	Time adjustment data								x											x	x								
ACC_210	Security Data																	x		x	x								
ACC_211	File structure and access conditions	x					x											x		x	x								
<SEF3> Accountability																													
ACT_201	Drivers account-ability																					x							
ACT_202	VU ID data																					x	x						
ACT_203	Workshops account-ability																					x							
ACT_204	Controllers accountabil-ity																					x							
ACT_205	Vehicle movement account-ability																					x							
ACT_206	Account-ability data modification																			x					x			x	

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
ACT_207	Accountability data modification																			x					x			x	
<SEF4> Audit																													
AUD_201	Audit records																						x						
AUD_202	Audit events list	x						x				x	x		x	x				x			x						
AUD_203	Audit records storage rules																						x						
AUD_204	Sensor audit records																						x						
AUD_205	Audit tools																						x						
<SEF5> Re-use																													
REU_201	Re-use																	x									x	x	
<SEF6> Accuracy																													
ACR_201	Information flow control policy							x			x		x														x	x	
ACR_201a	Information flow control policy							x			x		x														x	x	
ACR_202	Internal transfers														x											x	x	x	
ACR_203	Internal transfers														x								x						
ACR_204	Stored data integrity																			x					x			x	
ACR_205	Stored data integrity																			x			x						
<SEF7> Reliability																													
RLB_201	Manufacturing tests				x	x																						x	

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
RLB_202	Self tests			x								x				x			x									x	
RLB_203	Self tests											x				x			x				x						
RLB_204	Software analysis					x													x									x	
RLB_205	Software input																		x							x	x	x	
RLB_206	Case opening					x				x		x			x			x	x	x						x		x	
RLB_207	Hardware sabotage											x																x	
RLB_208	Hardware sabotage											x											x						
RLB_209	Power supply interruptions															x												x	
RLB_210	Power supply interruptions															x							x						
RLB_211	Reset			x																								x	
RLB_212	Data Availability																										x	x	
RLB_213	Card release																											x	
RLB_214	card session not correctly closed																						x						
RLB_215	Multiple Applications																											x	
<SEF8> Data exchange																													
DEX_201	Secured motion data import												x																x
DEX_202	Secured motion data import												x										x						

		Threats																			IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
DEX_203	Secured card data import							x																					x
DEX_204	Secured card data import							x															x						
DEX_205	Secured data export to cards							x																					x
DEX_206	Evidence of origin														x											x			
DEX_207	Evidence of origin														x											x			
DEX_208	Secured export to external media														x											x			
<SEF9> Cryptographic support																													
CSP_201	Algorithms							x			x		x					x										x	x
CSP_202	key generation							x			x		x					x										x	x
CSP_203	key distribution							x			x		x					x										x	x
CSP_204	key access							x			x		x					x										x	x
CSP_205	key destruction							x			x		x					x										x	x

2 Evaluation Results

The TOE provides the functionality according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [7].

The changes according Annex 1B of Council Regulation (EC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated from 13.03.2004 (OJ L 77) are implemented.

2.1 Effectiveness – Construction

2.1.1 Analysis of Suitability of the Functionalities

The suitability analysis assigns the security enforcing functions and mechanisms to the threats which have been identified in the security target and detailed design and which it counteracts. It also shows how the security enforcing functions and mechanisms counteract the identified threats and that there are no identified threats which are not adequately counteracted by one or more of the listed security enforcing functions.

The evaluation facility has examined, that the suitability analysis meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information.

2.1.2 Analysis of the Binding of the Functionalities

This analysis of the binding concerns all the possible relationships between the security enforcing functions and mechanisms. It shows that a security enforcing function or mechanism cannot be made to conflict with or counteract the tasks of other security enforcing functions or mechanisms.

The evaluation facility has examined, that the analysis of the binding meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information.

2.1.3 Analysis of the Strength of Mechanisms

The ability of the mechanisms to counteract direct attacks has been evaluated.

The analysis of the strength of mechanisms lists all security enforcing mechanisms as critical within the TOE. It contains analyses of the algorithms and principles underlying these mechanisms. The analysis of the strength of mechanisms has shown, that all mechanisms identified as critical, fulfil the claimed strength of mechanism.

The evaluation facility has examined, that all critical mechanisms have been identified as such. The evaluation facility has examined, that analysis of the strength of mechanisms, as submitted, meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has examined, that all mechanisms identified as critical, fulfil the claimed strength of mechanism.

The rating of the strength of mechanisms does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, clause 2).

2.1.4 Constructional Vulnerabilities

The developer has provided a list of known vulnerabilities. These known vulnerabilities have been assessed to determine whether they could in practice compromise the security of the TOE as specified by the security target.

The analysis of the potential impact of each known vulnerability shows that the vulnerabilities in question cannot be exploited in the intended environment for the TOE because either

- the vulnerability is adequately covered by other uncompromised security mechanisms or
- it could be shown that the vulnerability is irrelevant to the security target, will not exist in practice or can be countered adequately by documented technical, personnel, procedural or physical security measures outside the TOE. These external security measures have been defined within the appropriate documentation.

The evaluation facility has examined, that the list of known vulnerabilities meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has performed an independent vulnerability analysis. It has checked that all combinations of known vulnerabilities have been addressed. It has checked that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. It has checked that all assumptions and requirements for external security measures have been appropriately documented.

2.2 Effectiveness - Operation

2.2.1 Ease of Use Analysis

The TOE cannot be configured or used in a manner which is insecure but which an administrator or user of the TOE would reasonably believe to be secure.

The evaluation facility has examined, that the ease of use analysis provided meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The analysis has been checked for undocumented or unreasonable assumptions about the intended environment. The evaluation facility has checked that all assumptions and requirements for external security measures have been appropriately documented. The procedure for configuration has been assessed to examine, that the TOE can be configured and used in a secure manner.

2.2.2 Operational Vulnerabilities

The developer identified one operational vulnerability. The analysis of the potential impact of this vulnerability shows that the vulnerability in question cannot be exploited in the intended environment for the TOE because either

- the vulnerability is adequately covered by other uncompromised external security measures, or
- it could be shown that the vulnerability is irrelevant to the security target or will not be exploitable in practice, or

The instructions for the user have to be followed.

The evaluation facility has examined, that the list of known operational vulnerabilities meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has performed an independent vulnerability analysis under consideration of the listed vulnerabilities and those found during the evaluation process. It has checked that all combinations of known vulnerabilities have been addressed. It has checked that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. It has checked that all assumptions and requirements for external security measures have been appropriately documented.

2.3 Correctness - Construction - Development Process

2.3.1 Security Target

The security target describes the security enforcing functions provided by the TOE. They contain specifications identifying the way in which the product is used, the intended operational environment and the threats assumed for this operational environment. The security enforcing functions listed in the security target are specified using an informal notation. The security target explains, why the functionality is appropriate for this type of use and how it counteracts the threats.

The security target correspond fully to the generic security target [13] for the vehicle unit.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence and that there are no inconsistencies within the security target.

2.3.2 Architectural Design

The architectural design describes the general structure and all external interfaces of the TOE. It describes the separation of the TOE into security enforcing and other components and how the security enforcing functions are provided.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.3.3 Detailed Design

The detailed design describes the realisation of all security enforcing and security relevant functions. It specifies all basic components, identifies all security mechanisms and maps the security enforcing functions to mechanisms and components. All interfaces of the security enforcing and security relevant components are documented together with their purposes and parameters. Specifications for the mechanisms have been provided. These specifications are suitable for the analysis interrelationships between the mechanisms employed. The detailed design describes how the secuirty mechanisms realise the security enforcing functions as specified in the security target.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.3.4 Implementation

The test documentation contains the test plan, test objectives, test procedures and test results. The library of test programs contains test programs and test tools which are suitable for repeating all the tests described in the test documentation. This documentation describes the correspondence between the tests and

- the security enforcing functions as described in the security target,
- the security relevant and security enforcing functions and mechanisms as defined in the detailed design, and
- the security mechanism as described in the source code.

All tests show the expected results.

A description of correspondence describes the correspondence between source code and basic components of the detailed design.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.The library of test programs was used to check by sampling the test results. The evaluation facility has examined, that the tests cover all security enforcing and security relevant functions. Additional tests were performed to search for errors.

2.4 Correctness - Construction - Development Environment

2.4.1 Configuration Control

The development process is supported by a tool based configuration control system and an acceptance procedure. The configuration list provided enumerates all basic components of the TOE. The TOE, its basic components and all documents that have been supplied, including the manuals and the source code, have unique identification. This identification is used in references. The configuration control system ensures that the TOE corresponds to the documentation which has been supplied and that only authorised changes are possible.

The information on the configuration control system describe the use of the system in practice and how it can be used in the development process together with the vendor's quality management procedure.

The evaluation facility has examined, that the documented procedures are applied and that the information provided meets all the requirements with regard to content, presentation and evidence.

2.4.2 Programming Languages and Compilers

For the implementation of the TOE C compiler and the assembler for the vehicle unit microprocessor was used. All used instructions and statements of the assembler are completely and clearly defined so that the meaning of all instructions and statements used in the source code are unambigously defined.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.4.3 Security in the Developer's Environment

The document on the security of the developer's environment describes the measures taken to protect the integrity of the TOE and the confidentiality of the relevant documents. Descriptions of the physical, personnel and procedural security measures as used by the developer were provided.

The evaluation facility has examined, that the documented procedures are applied and that the information provided meets all the requirements with regard to content, presentation and evidence. The evaluation facility has searched for errors in the procedures.

The TOE was developed and manufactured by:

Siemens VDO Automotive AG
Heinrich-Hertz-Strasse 45
D-78052 Villingen-Schwenningen

2.5 Correctness - Operation - Operational Documentation

2.5.1 User Documentation

The user documentation [9] and [10] describes the security enforcing functions relevant to the unprivilidged user. The description of these functions is provided in a way understandable for the user.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.5.2 Administrators Documentation

The technical product documentation targeted to the authorised workshop staff, fitters and vehicle manufactures is considered as the administration documentation [11] in this case. This documentation is structured, internally consistent, and consistent with all other documents supplied for this level.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.6 Correctness - Operation - Operational Environment

2.6.1 Delivery and Configuration

The procedure for delivery is described. A procedure approved by BSI for this evaluation level is applied to guarantee the authenticity of the delivered TOE. The information supplied describes how the described procedures maintain security.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

The following components are provided for a customer, who purchases the TOE:

- Digital Tachograph DTCO 1381(Vehicle Unit), SW-version: 00.05.0M.P026, Sicherheitsmodul: 1381.73.900.05
- Digitaler Tachograph DTCO 1381, Technische Beschreibung, TD00.1381.00 120 101-OPM 000 AA [11]
- Digitaler Tachograph DTCO 1381, Betriebsanleitung Unternehmer und Fahrer, BA00.1381.00 100 101-OPM 000 AA [9]
- Digitaler Tachograph DTCO 1381, Leitfaden für Kontrollorgane, BA00.1381.00 200 101-OPM 000 AA [10]

The TOE is labled with its identification number ’DTCO 1381’. On every restart the important part of the SW-version number ’0P0.26.M’ is indicated and under the menu point “Technische Daten” the SW-version number ’P0.26’ can read back.

2.6.2 Start-up and Operation

Secure start-up and operation is guaranteed by the secure state of the TOE at start-up and by various self tests and diagnostic procedures of the vehicle unit hardware and software. If an error is detected, a reset is performed or the error is displayed or recorded.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

3 Comments/Recommendations

The user has to observe the following instructions:

1. The operator of the digital tachograph system has to make sure, that the organisational measures being relevant for him and defined in [7] (cf. chapter 2.9 of this document) are adequately implemented. These are at least the following measures:

   -M.Sec_Data_Generation,
   -M.Sec_Data_Transport,
   -M.Card_Availability,
   -M.Card_Traceability,
   -M.Approved_Workshops

   Such measures could be defined e.g. by the National Policy (MSA Policy) and enforced by accreditation and audit procedures.

2. It must be assured by organisational measures, that the certificates and key pairs respectively for a successful device authentication are only granted to trustworthy tachograph cards. Furthermore this tachograph cards must be able to protect these secrets in a sufficient manner and they must be evaluated and certified in accordance with [7] and [5] to ITSEC on an evaluation level E3 and with a minimum strength of function high.

3. It must be assured by organisational measures, that the necessary data for the pairing process are only granted to trustworthy motion sensors. Furthermore the motion sensors must be able to protect these data in a sufficient manner and they must be evaluated and certified in accordance with [7] and [5] to ITSEC on an evaluation level E3 and with a minimum strength of function high.

4. The evaluator advises the operator of the digital tachograph system, that the control officers will be fit out with equipment, which can download data from the tachograph and then analyse it efficiently. Such automated data analysis will remarkably facilitate the search of important events.

4 Literature and References

[1] Information Technology Security Evaluation Criteria (ITSEC), CEC, Version 1.2, June 1991.

[2] Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993

[3] ITSEC Joint Interpretation Library (ITSEC JIL), Version 2.0, November 1998

[4] BSI certification: Procedural Description (BSI 7125, Version 5.1, January 1998)

[5] Security Target DTCO 1381, Digital Tachograph – Vehicle Unit, Revision 4.3

[6] Evaluation Technical Report, Version1.01, 21.09.2004 (confidential document)

[7] Appendix 10 of Annex 1(B) of Council Regulation (EC) No. 1360/2002 - Generic Security Targets

[8] Annex 1(B) of Council Regulation (EC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated from 13.03.2004 (OJ L 77)

[9] Digitaler Tachograph DTCO 1381, Betriebsanleitung Unternehmer & Fahrer, BA00.1381.00 100 101-OPM 000 AA

[10] Digitaler Tachograph DTCO 1381, Leitfaden für Kontrolorgane, BA00.1381.00200 101-OPM 000 AA

[11] Digitaler Tachograph DTCO 1381, Technische Beschreibung, TD00.1381.00 120 101-OPM 000 AA

[12] Appendix 1 of Annex 1(B) of Council Regulation (EC) No. 1360/2002 - Datadictionary

[13] Appendix 10 of Annex 1(B) of Council Regulation (EC) No. 1360/2002 – Generic Security Target

[14] Appendix 8 of Annex 1(B) of Council Regulation (EC) No. 1360/2002 – Calibration Protocol

[15] Appendix 11 of Annex 1(B) of Council Regulation (EC) No. 1360/2002 – Common Security Mechanisms

C Excerpts from the Criteria

The following quotes from the ITSEC and ITSEM describe the requirements for the specified product and explain the assurance levels achieved.

Six levels for correctness and effectiveness are defined for assessment of the assurance. E1 designates the lowest level and E6 designates the highest level defined here.

The abbreviation TOE (Target Of Evaluation) used means the certified product. The Section numbers have been taken from the ITSEC rsp. ITSEM.

1 Effectiveness

ITSEC:

”Assessment of effectiveness involves consideration of the following aspects of the TOE:

a) the suitability of the TOE’s security enforcing functions to counter the threats to the security of the TOE identified in the security target;

b) the ability of the TOE’s security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c) the ability of the TOE’s security mechanisms to withstand direct attack;

d) whether known security vulnerabilities in the construction of the TOE could in practice compromise the security of the TOE;

e) that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure;

f) whether known security vulnerabilities in the operation of the TOE could in practice compromise the security of the TOE.”

2 Correctness

ITSEC:

”The seven evaluation levels can be characterised as follows:”

Level E0

4.4 This level represents inadequate assurance.

Level E1

4.5 At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.

Level E2

4.6 In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

Level E3

4.7 In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.

Level E4

4.8 In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

Level E5

4.9 In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

Level E6

4.10 In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.”

3 Classification of Security Mechanisms

ITSEM:

”6.C.4 A type A mechanism is a security mechanism with a potential vulnerability in its algorithm, principles or properties, whereby the mechanism can be overcome by the use of sufficient resources, expertise and opportunity in the form of a direct attack. An example of a type A mechanism would be an authentication program using a password: if the password can be guessed by attempting all possible passwords in succession, the authentication mechanism is of type A. Type A mechanisms often involve the use of a ”secret” such as a password or cryptographic key.

6.C.5 All type A mechanisms in a TOE have a strength, which corresponds to the level of resources, expertise and opportunity required to compromise security by directly attacking the mechanism.

6.C.7 A type B mechanism is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses."

4 Minimum Strength of the Security Mechanisms

ITSEC:

"3.5 All critical security mechanisms (i.e. those mechanisms whose failure would create a security weakness) are assessed for their ability to withstand direct attack. The minimum strength of each critical mechanism shall be rated either basic, medium or high.

3.6 For the minimum strength of a critical mechanism to be rated basic it shall be evident that it provides protection against random accidental subversion, although it may be capable of being defeated by knowledgeable attackers.

3.7 For the minimum strength of a critical mechanism to be rated medium it shall be evident that it provides protection against attackers with limited opportunities or resources.

3.8 For the minimum strength of a critical mechanism to be rated high it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality."

This page is intentionally left blank.