Public Version

25, chemin de Pouvourville - BP 4215
31432 TOULOUSE CEDEX 04 - (FRANCE)
Fax : (33) 05 61 55 42 31 - Tél. (33) 05 61 17 61 61

SECURITY TARGET

L2000

	By	Date	Sign		Ref. ACTIA	Index
Draw	ERom			**SECURITY TARGET L 2000**	**P204070**	**L** Public
Verif	LMal					
Valid	ERom					
Appr	SBab				Page 1 / 51	Format A4

TABLE OF CONTENTS

I. FOREWORD

I.1 INTRODUCTION

This document is the public version of the security target of the ACTIA L2000 product. Some information are not available because of their restricted character.

The L2000 is a recording equipment (tachograph) vehicle unit (VU) conforming to Annex 1B of Council Regulation (EEC) n° 3821/85 as last amended by Council Regulation (EC) n° 1360/2002. The L2000 interface with a motion sensor is based on ISO 16844-3.

This security target is derived from Appendix 10 to above Council Regulation which contains a vehicle unit ITSEC generic security target. The L2000 security target is intended to be in full compliance with the vehicle unit ITSEC generic security target.

I.2 REFERENCE DOCUMENTS

[CC] ..... Common Criteria version 2.2, revision 456 – January 2004

[3821_1B] ..... Annex 1B of Council Regulation (EEC) n° 3821/85 as last amended by Council Regulation (EC) n° 432/2004 of 05/03/2004,

[1B_MB] ..... Main Body of [3821_1B] "Requirements for construction, testing, installation, and inspection"

[1B_10] ..... Appendix 10 to [3821_1B] "Generic security targets"

[1B_11] ..... Appendix 11 to [3821_1B] "Common security mechanisms"

[ISO 16844-3] ..... ISO/TC22/SC3 document: ISO/DIS 16844-3 – Road vehicles – Tachograph systems – Part 3: Motion Sensor Interface.

[RSA] ..... RSA Laboratories. PKCS#1 : RSA Encryption Standard. Version 2.0 October 1998.

[SHA – 1] ..... National Institute of Standards and Technology (NIST). FIPS Publication 180-1 : Secure Hash Standard. April 1995.

[TDES] ..... National Institute of Standards and Technology (NIST). FIPS Publication 46-3 : Data Encryption Standard. Draft 1999.
ANSI X9.52, Triple Data Encryption Algorithm Modes of operation. 1998.

[JIL] ..... Joint Interpretation Library. Security Evaluation and Certification of Digital Tachographs. Version 0.9 September 2002.

I.3 CONVENTIONS AND TERMINOLOGY

Throughout this document (req. xxx) means requirement (marginal) xxx of [1B_MB] and (AAA_xxx) means requirement AAA_xxx of [1B_10].

The text in [3821_1B] addressed by these references is to be considered as an integral part of the ST. This method is used to provide sense and clarification to the text of the ST while avoiding redundancy or incompatibility with this superseding document.

II. ST INTRODUCTION

II.1 ST IDENTIFICATION

Title : ..... **Security Target L2000**

Reference :..... **P204070**

TOE identification :..... **ACTIA L2000 Digital Tachograph**
This security target applies to the following configurations:
- 921435 Ind B (Standard family – full hardware options),
- 921439 Ind B (Standard family – light - Amber),
- 921463 Ind B (Standard family – light 2 - Green).

Key words : ..... Road transport vehicle, Digital tachograph, Recording Equipment, Vehicle unit, Security Target

EAL level : ..... **E3hAP (see [JIL]);**

Strength of functions : . **SOF-high**

CC conformance :..... CC version 2.2, revision 456 – January 2004, Parts 1 to 3.

II.2 ST OVERVIEW

This document contains a description of the L2000 and its security environment.

It specifies the security objectives for the L2000 and its environment, that address the environmental considerations.

It specifies the security functional measures offered by the L2000, and security assurance measures enforced during its development, that satisfy the stated security objectives.

It states the claimed minimum strength of functions (SOF) and the required level of assurance for the development and the CC evaluation.

III. TOE DESCRIPTION

III.1 L2000 DESCRIPTION AND METHOD OF USE

The L2000 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 with which it exchanges vehicle's motion data.

Users identify themselves to the L2000 using tachograph cards.

The L2000 records and stores user activities data in its data memory, it also records user activities data in tachograph cards.

The L2000 outputs user data to display, printer and external devices.

The L2000 operational environment while installed in a vehicle is summarised in the following figure:

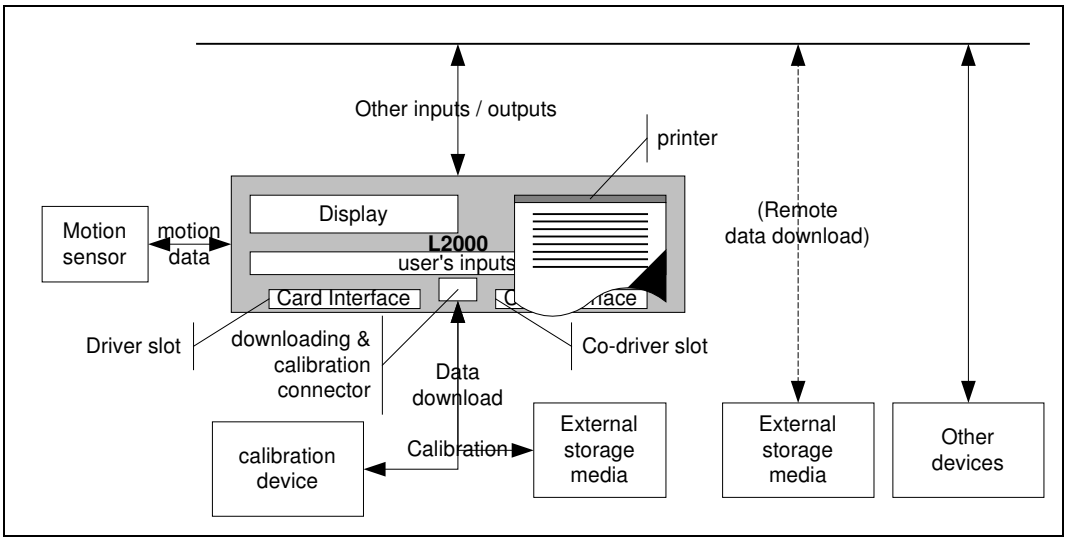

Figure 1: L2000 operational environment

The L2000 general characteristics, functions and mode of operations are described in chapter II of [1B_MB]. The L2000 functional requirements are specified in chapter III of [1B_MB].

It includes a processing unit, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration / downloading connector on the front panel, other connectors on the rear panel to allow for serial communications with other on-board devices (other inputs / outputs), and facilities for entry of user's inputs.

The L2000 provides selective access rights to data and functions according to user's type and/or identity.

The L2000 architecture is summarised in the following figure:

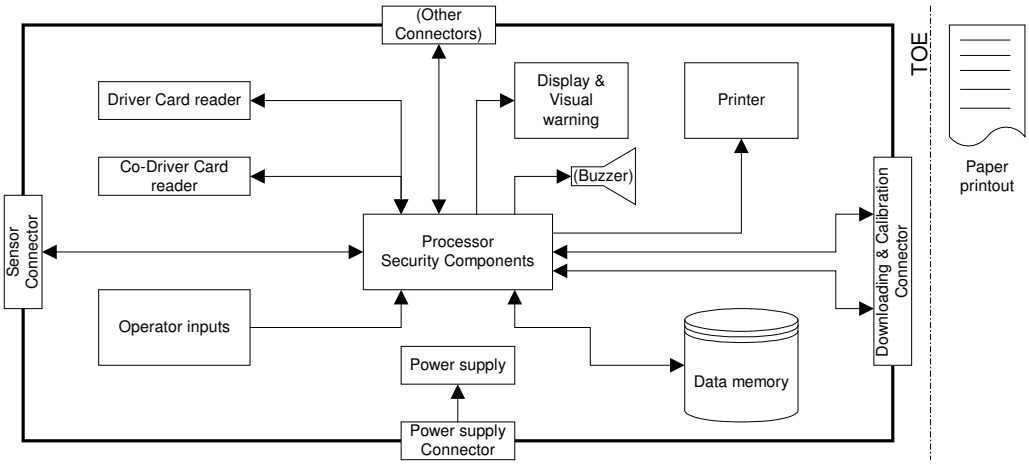

Figure 2: L2000

It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

III.2 L2000 LIFE CYCLE

The typical life cycle of the L2000 is described in the following figure:

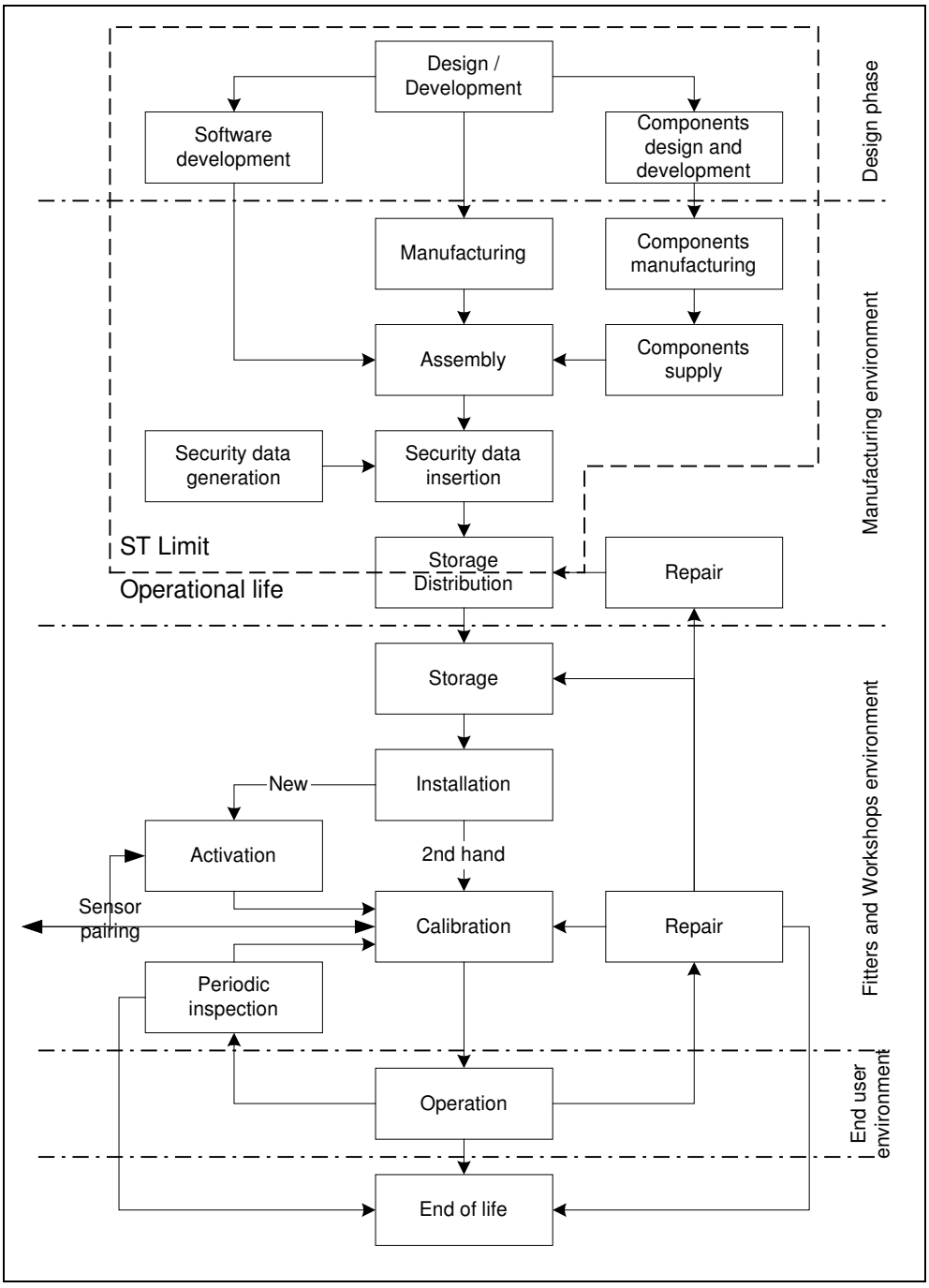

Figure 3: L2000 typical life cycle

ST Limit : The purpose of the security functions, designed and manufactured within the limit presented, is to control and protect the TOE during its operational life (product usage). The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases. This is why this ST addresses the functions used during product usage but developed and manufactured within the ST Limit.

During the design phase, the TOE is administrated by the development department.

During the manufacturing phase, the TOE is administrated by the manufacturing department. The main responsibility related to TOE administration during this phase relates to TOE personalisation and insertion of security data.

The TOE is then delivered in a non-activated mode, and no more administration features exist for the TOE which will only be handled by various users.

IV. TOE SECURITY ENVIRONMENT

This chapter describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. It includes a description of assumptions on the environment of the TOE, of threats to the assets against which specific protection within the TOE or its environment is required, and of organisational security policies.

IV.1 SECURE USAGE ASSUMPTIONS

This paragraph describes the secure usage assumptions on the environment of the L2000, as defined in [3821_1B].

A.Activation ..... The L2000 will be activated by vehicle manufacturers, fitters or workshops after its installation, before the vehicle leaves the premises where the installation took place.

A.Card_Delivery ..... Tachograph cards are available to the L2000 users. Tachograph cards are delivered by Member States authorities to authorised persons only.

A.Card_Traceability ..... Card delivery is traceable (white lists, black lists) and lists are used during security audits.

A.Controls ..... Law enforcement controls will be performed regularly and randomly, will include security audits as well as visual inspection of the equipment.

A.Driver_Card_Uniqueness ..... One driver possesses, at one time, one valid driver card only.

A.Faithfull_Drivers ..... Drivers play by the rules and act responsibly (e.g. use their driver card, properly select their activity for those manually selected…).

A.Periodic_Inspections ..... Periodic inspections of the equipment fitted to the vehicles will take place after any repair of the equipment, or after any alteration of the characteristic coefficient of the vehicle or of the effective circumference of the tyres, or after equipment UTC time is wrong by more than 20 minutes, or when the VRN has changed, and at least once within two years (24 months) of the last inspection.

A.Trusted_Workshops ..... The Member States will approve, regularly control and certify fitters and workshops to carry out installations, checks, inspections, repairs. Workshops will faithfully calibrate the L2000.

IV.2 THREATS

This paragraph describes the threats to the assets against which specific protection within the TOE or its environment is required. A threat is generally described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack.

The main assets to be protected are the user data, measured and recorded by the L2000, subject to check by law enforcement authorities in order to verify driver compliance to Council Regulation (EEC) 3820/85. Derived assets to be protected are the L2000 software and hardware. Security data supporting security mechanisms are secondary assets to protect.

The threat agents to these assets may be:
- Authorised users with no expertise, who can cause errors ;
- Hostile users or companies with high expertise, motivation and large resources.

In case of the L2000, all the threats are derived from the document [1B_10] (chapter 3.3, p21) and address the user data described above.

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.

T.Faults ..... Faults in hardware, software, communication procedures could place the L2000 in unforeseen conditions compromising its security.

T.Tests ..... The use of non invalidated test modes or of existing back doors could compromise the L2000 security.

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

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

T.Card_Data ..... Users could try to modify data while exchanged between the L2000 and tachograph cards (addition, modification, deletion, replay of signal).

T.Clock ..... Users could try to modify internal clock.

T.Environment ..... Users could compromise the L2000 security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).

T.Fake_Devices ..... Users could try to connect fake devices (motion sensor, smart cards) to the L2000.

T.Hardware ..... Users could try to modify the L2000 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 L2000 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 the L2000 software.

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

IV.3 ORGANISATIONAL SECURITY POLICIES

The following security policies are derived from the global security analysis of the whole tachograph system and are compliant to the main security objectives assigned to a vehicle unit by [1B_10](Chapter 3.4, p.22).

P.L2000_Main..... The data to be measured and recorded by the L2000 and then to be checked by control authorities shall 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.

P.L2000_Export.... The L2000 shall be able to export data to external storage media in such a way as to allow for later verification of their integrity and authenticity.

V. SECURITY OBJECTIVES

This chapter defines the security objectives for the TOE and its environment. The security objectives address all of the security environment aspects identified, are suitable to counter all identified threats, and cover all identified organisational security policies and assumptions.

V.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives the L2000 shall achieve are the following. These objectives are derived from the document [1B_10] (chapter 3.5, p22).

O.Access..... The L2000 shall control user access to functions and data.

O.Accountability..... The L2000 shall collect accurate accountability data.

O.Audit..... The L2000 shall audit attempts to undermine system security and should trace them to associated users.

O.Authentication..... The L2000 should authenticate users and connected entities (when a trusted path needs to be established between entities).

O.Data_Exchange..... The L2000 shall secure data exchanges with the motion sensor and with tachograph cards.

O.Download..... The L2000 shall be able to export data to external storage media in such a way as to allow for later verification of their integrity and authenticity.

O.Integrity..... The L2000 shall maintain stored data integrity.

O.Output..... The L2000 shall ensure that data output reflects accurately data measured or stored.

O.Processing..... The L2000 shall ensure that processing of inputs to derive user data is accurate.

O.Phys_Protection..... The L2000 shall be designed such that it is not openable, and that any attempts to open it, will be clearly identifiable through visual inspection.

O.Reliability..... The L2000 shall provide a reliable service.

O.Software_Upgrade..... The L2000 shall authenticate and verify the integrity of imported software before accepting the upgrade.

V.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The security objectives that the L2000 environment shall achieve are the following. These objectives are derived from the document [1B_10] (chapter 3.6, p21).

V.2.1 Design phase

OE.Dvpt_Security..... L2000 developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

OE.Reliable_Design..... L2000 developers should design the L2000 such as to minimise potential design flaws.

OE.Software_Analysis ..... L2000 design shall be such that there shall be no way to analyse or debug software in the field after the L2000 activation.

OE.Software_Upgrade..... Software revisions shall be granted security certification before they can be delivered for implementation in a L2000.

V.2.2 Manufacturing phase

OE.Data_Generation..... Security data generation algorithms shall be accessible to authorised and trusted persons only.

OE.Data_Transport ..... Security data shall be generated, transported, and inserted into the L2000, in such a way to preserve its appropriate confidentiality and integrity.

OE.Mnft_Security ..... The L2000 manufacturer shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the L2000 is protected from physical attacks which might compromise IT security.

OE.Manufacturing ..... The L2000 manufacturer shall ensure that manufacturing conforms with design.

OE.Personalisation..... The L2000 manufacturer shall personalise the L2000 before delivery.

OE.Tests_Points..... All commands, actions or test points, specific to the testing needs of the manufacturing phase of the L2000 shall be disabled or removed before the L2000 delivery. It shall not be possible to restore them for later use.

V.2.3 Delivery

OE.Users..... Users shall be informed of their responsibility when using the TOE. Vehicle manufacturers, fitters and workshop shall particularly be informed of their responsibility related to L2000 activation after installation.

V.2.4 Product usage phase

OE.Activation ..... The L2000 shall be activated by vehicle manufacturers, fitters or workshops after its installation, before the vehicle leaves the premises where the installation took place.

OE.Card_Delivery..... Tachograph cards shall be available to the L2000 users. Tachograph cards shall be delivered by Member States authorities to authorised persons only.

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

OE.Controls ..... Law enforcement controls shall be performed regularly and randomly, shall include security audits as well as visual inspection of the equipment.

OE.Driver_Card_Uniqueness
One driver shall possess, at one time, one valid driver card only.

OE.Faithfull_Drivers ..... Drivers shall play by the rules and act responsibly (e.g. use their driver card, properly select their activity for those manually selected…).

OE.Periodic_Inspections.. Periodic inspections of the equipment fitted to the vehicles shall take place after any repair of the equipment, or after any alteration of the characteristic coefficient of the vehicle or of the effective circumference of the tyres, or after equipment UTC time is wrong by more than 20 minutes, or when the VRN has changed, and at least once within two years (24 months) of the last inspection.

OE.Trusted_Workshops.. The Member States shall approve, regularly control and certify fitters and workshops to carry out installations, checks, inspections, repairs. Workshops shall faithfully calibrate the L2000.

VI. IT SECURITY REQUIREMENTS

This chapter defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

VI.1 TOE SECURITY REQUIREMENTS

VI.1.1 TOE Security Functional Requirements

These requirements are derived from the document [1B_10] (chapter 4, p24).

Component	Description	Operation
FAU_GEN.1	Audit data generation	Yes
FAU_SAR.1	Audit review	Yes
FAU_STG.2	Guarantees of audit data availability	Yes
FCS_CKM.1	Cryptographic key generation	Yes
FCS_CKM.2	Cryptographic key distribution	Yes
FCS_CKM.3	Cryptographic key access	Yes
FCS_CKM.4	Cryptographic key destruction	Yes
FCS_COP.1	Cryptographic operation	Yes
FDP_ACC.2	Complete access control	Yes
FDP_ACF.1	Security attribute based access control	Yes
FDP_DAU.1	Basic data authentication	Yes
FDP_ETC.2	Export of user data with security attributes	Yes
FDP_IFC.1	Subset information flow control	Yes
FDP_IFF.1	Simple security attributes	Yes
FDP_ITC.2	Import of user data with security attributes	Yes
FDP_RIP.1	Subset residual information protection	Yes
FDP_SDI.1	Stored data integrity monitoring and action	Yes
FDP_UIT.1	Data exchange integrity	Yes
FIA_AFL.1	Authentication failure handling	Yes
FIA_ATD.1	User attribute definition	Yes
FIA_UAU.2	User authentication before any action	
FIA_UAU.3	Unforgeable authentication	Yes
FIA_UAU.6	Re-authenticating	Yes
FIA_UID.2	User identification before any action	Yes

Component	Description	Operation
FPT_AMT.1	Abstract machine testing	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
FPT_PHP.1	Passive detection of physical attack	
FPT_SEP.1	TSF domain separation	Yes
FPT_STM.1	Reliable time stamps	
FPT_TST.1	TSF testing	Yes
FRU_PRS.1	Limited priority of service	Yes
FTP_ITC.1	Inter-TSF trusted channel	Yes

FAU_GEN.1 Audit data generation

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

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

b) All auditable events for the *minimum* level of audit ; and

c) *The following events and faults:*
- *Unauthorised change of motion sensor,*
- *Last card session not correctly closed (RLB_214),*
- *Motion data error,*
- *Detection of power supply variation, including cut-off (RLB_210),*
- *Detection of an internal fault during self test (RLB_203),*
- *The audit records sent by the motion sensor,*

The following accountable events:
- *Motion sensor pairing,*
- *Driver / Workshop card insertion and withdrawal cycle (ACT_201),*
- *Driver activity change (ACT_201),*
- *Entry of place where the daily work period begin and/or end (ACT_201),*
- *Entry of a specific condition (ACT_201),*
- *Calibration of the equipment (ACT_203),*
- *Time adjustment (ACT_203),*
- *Control by enforcement authorities (ACT_204),*
- *Midnight (ACT_205),*
- *Speed change (ACT_205).*

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the following audit relevant information :*

- *For the L2000 internal records:*
  - *Events and faults : see (AUD_201, req. 094 and 096),*
  - *Motion sensor pairing : see (Req. 079),*
  - *Driver / Workshop card insertion and withdrawal cycle : see (req. 081),*
  - *Driver activity change : see (Req. 084),*
  - *Entry of place where the daily work period begin and/or end : see (Req. 087),*
  - *Entry of a specific condition : see (Req. 105a),*
  - *Calibration of the equipment : see (Req. 098),*
  - *Time adjustment : see (Req. 101),*
  - *Control by enforcement authorities : see (Req. 102 103),*
  - *Midnight : see (Req. 090),*
  - *Speed change : see (Req. 093).*
- *For the records written by the L2000 on tachograph cards : see (Req. 109 and 109a)*

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide *users* with the capability to read *appropriate audit information (AUD_205)* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to *prevent* modifications to the audit records *(ACT_206, 207).*

FAU_STG.2.3 The TSF shall ensure that *in accordance with (Reqs. 079, 083, 086, 089, 092, 093, 094, 096, 097, 100, 102, 105b, 110)* audit records will be maintained when the following conditions occur : *audit storage exhaustion*.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet the following:

Purpose	**Algorithm and size**	**Key generation specification**
Diversified Transport Key	2 Key TDES	TDES
Session keys with cards	2 Key TDES	[1B_11] CSM_020
Session key with motion sensor	2 Key TDES	[ISO 16844_3] 7.4.5
Public key cryptographic operations	RSA key pair 1024 bits	On board generation of key pair.

FCS_CKM.2 Cryptographic key distribution

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

Distributed key	**Distribution method / Reference**
Session keys with cards	[1B_11] CSM_020
Session key to motion sensor	[ISO 16844_3] 7.4.5
L 2000 public key to other tachograph system components	[1B_11] CSM_020 [1B_07] DDP_029 Distributed with its certificates
L 2000 public key to key certification authority	Signed by diversified transport key

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform *cryptographic key accesses* in accordance with a specified cryptographic key access method that meets the following:

Key	**Key access method and reference**
Motion sensor Master key	Temporarily reconstructed from half keys stored in workshop card and L2000. L2000 half key stored during personalisation. [1B_11] CSM_036 CSM_037
Motion sensor Pairing key	Sent by motion sensor [ISO 16844_3]
Cards, motion sensor Session keys	Internally generated and temporarily stored during session
L 2000 private key	Stored during L2000 personalisation.
Public keys of Tachograph system components (cards, key certification authorities)	Root CA key stored in L2000 during personalisation, Other public keys distributed by components embedded in relevant certificates, temporarily stored after certificate verification.
Actia public key	Stored during manufacturing (hard coded).
Transport key	Stored during manufacturing (hard coded).
Diversified Transport key	Internally computed from Transport key.

FCS_CKM.4 Cryptographic key destruction

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

Key	**Key destruction method**
Motion sensor Master key	Modification of key value
Motion sensor Pairing key	Modification of key value
Session keys	Replacement / Modification of key value
Public keys of Tachograph system components	Replacement
Diversified Transport key	Modification of key value
L2000 RSA key pair, European public key, L2000 certificates, VU half key (of motion sensor Master key).	Modification of key value

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *cryptographic operations* in accordance with a specified cryptographic algorithm and cryptographic key sizes that meets the following:

Cryptographic operations	**Crypto algorithms, and key size**
Hash	SHA – 1
Encryption Decryption	Triple DES – 2 key option ECB and CBC modes
MACs	Triple DES – 2 key option
Secure messaging with tachograph cards	ISO 7816 – 4, ISO 7816 – 8 Triple DES – 2 Key option
Signature	PKCS#1, RSA 1024 bits
Verification	RSA 1024 bits
Authentication	RSA 1024 bits

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the *functions_access_policy* on *functions* and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the *L2000_ID_policy* on *data memory* and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the *file_structure_policy* on *data memory* and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *functions_access_policy* to objects based on *the L2000 mode of operation (Reqs. 006, 007, 008) and the L2000 activation status.*

The TSF shall enforce the *L2000_ID_policy* to objects based on *files attributes (identification data in accordance with Req. 075, and security elements in accordance with Req. 080).*

The TSF shall enforce the *file_structure_policy* to objects based on *files attributes.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *functions_access_policy : Access to functions shall be in accordance with (Req. 010). Software upgrade shall be allowed in CALIBRATION mode of operation only.*

- *L2000_ID_policy : L2000 identification data and security elements are written ONCE in accordance with (Req. 076 and 080).*
- *file_structure_policy : Application and data files structure and access conditions are created during the manufacturing process, and then locked from any future modification or deletion.*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *rules*.

FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity *of data downloaded to external media*.

FDP_DAU.1.2 The TSF shall provide *external media* with the ability to verify evidence of the validity of the indicated information.

FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the *Data_download_policy* when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: *no additional rules*.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the *Motion_data_flow_policy* on *motion data imported from the motion sensor*,

The TSF shall enforce the *Motion_sensor_exchanges_policy* on *other data exchanged with the motion sensor*,

The TSF shall enforce the *Card_release_policy* on *card interface devices*,

The TSF shall enforce the *Internal_data_flow_policy* on *internal data transfers and processing*,

The TSF shall enforce the *Manual_inputs_policy* on *user inputs*,

The TSF shall enforce the *Tacho_card_exchanges_policy* on *data exchanged with tachograph cards*,

The TSF shall enforce the *Data_download_policy* on *data downloaded to an external media or a remotely connected company*,

The TSF shall enforce the *Software_import_policy* on *software upgrade data*.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *Motion_data_flow_policy* based on the following types of subject and information security attributes: *pulse counter value*.

The TSF shall enforce the *Motion_sensor_exchanges_policy* based on the following types of subject and information security attributes: *data integrity and authenticity attributes*.

The TSF shall enforce the *Card_release_policy* based on the following types of subject and information security attributes: *card update pending*.

The TSF shall enforce the *Internal_data_flow_policy* based on the following types of subject and information security attributes: *none*.

The TSF shall enforce the *Manual_inputs_policy* based on the following types of subject and information security attributes: *time of events entered manually*.

The TSF shall enforce the *Tacho_card_exchanges_policy* based on the following types of subject and information security attributes: *data integrity attributes*.

The TSF shall enforce the *Data_Download_Policy* based on the following types of subject and information security attributes: *none*.

The TSF shall enforce the *Software_import_policy* based on the following types of subject and information security attributes: *data integrity and authenticity attributes*.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *Motion_sensor_exchanges_policy* : *Data, other than motion data, imported from the motion sensor shall be accepted only when its integrity has been verified,*
- *Tacho_card_exchanges_policy* : *Data imported from tachograph cards shall be accepted only when its integrity has been verified,*
- *Software_import_policy* : *Data imported as software upgrade shall be accepted only when its authenticity and integrity has been verified.*

FDP_IFF.1.3 The TSF shall enforce the *following additional information flow rule:*

- *Internal_data_flow_policy* : *The L2000 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, L2000 real time clock, calibration parameters, tachograph cards, user's inputs,*
- *Manual_inputs_policy : The L2000 shall ensure that user data related to (Req. 109a) may only be entered for the period last card withdrawal - current insertion (Req. 050a),*

- *Card_release_policy* : :*The L2000 shall ensure that cards cannot be released before relevant data have been stored to them.*

FDP_IFF.1.4 The TSF shall provide the following *additional SFP capabilities:*

Motion_data_flow_policy : *The L2000 shall periodically check motion data integrity. Upon detection of integrity errors of motion data, the L2000 shall continue to use motion data to process speed.*

Data_Download_Policy : The L2000 shall download data with a signature appended to provide for further data authentication and integrity.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: *none*.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: *none*.

FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the *Software_import_policy* when importing user data, controlled under the SFP, from outside of the TSC.

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

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

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

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *none.*

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from* the following objects : *motion sensor Master Key, motion sensor Pairing Key, Workshop card PIN code, Session keys*.

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1A a) Minimal : *Unsuccessful attempts to check the integrity of user data.*

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for *integrity errors* on all objects, based on the following attributes : *Checksum on data blocks.*

FDP_UIT.1 Data exchange integrity

FDP_UIT.1A a) Minimal : *Integrity error on receipt of data.*

FDP_UIT.1.1 The TSF shall enforce the *Motion_sensor_exchanges_policy and the Tacho_card_exchanges_policy* to be able to *transmit and receive* user

data in a manner protected from *modification, deletion and insertion* errors

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion or insertion* has occurred.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1A a) Minimal : *The reaching of the threshold for the unsuccessful authentication attempts*.

FIA_AFL.1.1 The TSF shall detect when *20 consecutive* unsuccessful authentication attempts occur related to *motion sensor authentication*.

The TSF shall detect when *5 consecutive* unsuccessful authentication attempts occur related to *driver or co-driver or remotely connected company authentication*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall :

- *Motion sensor :*
  - *generate an audit record of the event,*
  - *warn the user,*
  - *continue to accept and use non secured motion data sent by the motion sensor.*
- *Driver or Co-Driver :*
  - *generate an audit record of the event,*
  - *warn the user,*
  - *assume the user as UNKNOWN, and the card as non valid (UIA_214).*
- *Remotely connected company :*
  - *warn the remotely connected company.*

FIA_ATD.1 User attribute definition

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual users :

- *Motion sensor : sensor approval number and sensor serial number,*
- *Driver and Co-Driver : user group and user ID (UIA_208),*
- *Remotely connected company : user ID (UIA_216).*

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall *detect and prevent* use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall *detect and prevent* use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the following conditions :

- *Motion sensor :*
  - *at each calibration of the recording equipment,*
  - *at power supply recovery,*
  - *periodically (more frequently than once per hour),*
- *Driver and Co-Driver :*
  - *at power supply recovery,*
  - *periodically or after occurrence of specific events (more frequently than once per day).*

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user *(UIA_201, UIA_207, UIA_215, UIA_221).*

FPT_AMT.1 Abstract machine testing

FPT_AMT.1A a) Minimal : *Test failure (L2000 internal fault).*

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, and during normal operation* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF *(RLB_202).*

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1A a) Minimal : *Unauthorised power supply deviation*.

FPT_FLS.1 The TSF shall preserve a secure state when the following types of failures occur : *power supply deviation, transaction stopped before completion, or any other reset conditions (RLB_209, RLB_210, RLB_211).*

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF *(RLB_206)*.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_SEP.1	**TSF domain separation**
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects *(RLB_215).*
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC *(RLB_215).*
FPT_STM.1	**Reliable time stamps**
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
FPT_TST.1	**TSF testing**
FPT_TST.1A	a) Minimal : *Test failure (L2000 internal fault).*
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, and during normal operation* to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.
FRU_PRS.1	**Limited priority of service**
FRU_PRS.1.1	The TSF shall assign a priority to each subject in the TSF.
FRU_PRS1.2.	The TSF shall ensure that access to *resources* shall be mediated on the basis of the subjects assigned priorities *(RLB_212).*
FTP_ITC.1	**Inter-TSF trusted channel**
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *the TSF* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for *data exchanges with the motion sensor and tachograph cards*.

VI.1.2 TOE Security Assurance Requirements

The assurance level required by the European Regulation for a Vehicle Unit is an ITSEC E3 High level ([1B_10]).

A CC assurance package named E3hAP ([JIL]), providing a technical correspondence as close as possible from the required ITSEC assurance level, has therefore been selected from Common Criteria part 3, with a minimum strength of functions claim of **SOF-high**, consistent with the TOE Security Objectives.

Class	Component	Description
ACM Configuration management	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL.2	Detection of modifications
	ADO_IGS.2	Generation log
ADV Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_TAT.1	Well-defined development tools
ATE Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing : Low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.4	Highly resistant

ADO_IGS.2 is selected with the interpretation / refinement according to [JIL] 41.
No other refinement are made to the above security assurance requirements.

VI.2 TOE ENVIRONMENT SECURITY REQUIREMENTS

There is no security functional requirements for the IT environment.

VII. TOE SUMMARY SPECIFICATION

The main purpose of this section is to specify the TOE-specific solution to the identified security needs, showing how the TOE provides the security functions and assurance measures to satisfy the defined TOE security requirements. The strength of all functions shall be **SOF-high.**

VII.1 TOE SECURITY FUNCTIONS

The TOE security functions are not described in the public version of the document, however these functions are listed in section IX.3 “Security functions rationale”.

VII.2 ASSURANCE MEASURES

The section providing a general mapping from the documentation or evidence the developer intends to provide to the appropriate assurance measures is not available in the public version of the document.

VIII. PP CLAIMS

None.

IX. RATIONALE

IX.1 SECURITY OBJECTIVES RATIONALE

These rationale are derived from the document [1B_10] (chapter 8, p29). These rationale demonstrate that the identified security objectives are suitable, addressing all aspects of the security needs as specified in the TOE Security Environment.

IX.1.1 Mapping the security objectives to the TOE security environment

			TOE Security Environment																													
			Assumptions								Threats																		Pol			
			A.Activation	A.Card_Delivery	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithfull_Drivers	A.Periodic_Inspections	A.Trusted_Workshops	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration	T.Card_Data	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	P.L2000_Main	P.L2000_Export
Security Objectives	TOE	O.Access									x					x		x										x		
		O.Accountability										x				x		x											x	
		O.Audit									x					x	x	x				x			x			x	x	
		O.Authentication									x	x								x										
		O.Data_Exchange															x					x								
		O.Download																						x						x
		O.Integrity														x										x	x	x	x	
		O.Output																						x					x	x
		O.Processing																										x	x	
		O.Phys_Protection													x				x		x			x			x			
		O.Reliability											x						x						x			x	x	
		O.Software_Upgrade																									x			
	TOE Environment	OE.Dvpt_Security											x		x						x						x			
		OE.Reliable_Design											x						x						x			x		
		OE.Software_Analysis																									x			
		OE.Software_Upgrade											x														x			
		OE.Data_Generation																								x				
		OE.Data_Transport																								x				
		OE.Mnft_Security																			x					x	x			
		OE.Manufacturing											x								x						x			
		OE.Personalisation																											x	
		OE.Tests_Points												x																
		OE.Users										x											x							
		OE.Activation	x																				x							
		OE.Card_Delivery		x								x																		
		OE.Card_Traceability			x							x																		

	TOE Security Environment																												
	Assumptions								Threats																			Pol	
	A.Activation	A.Card_Delivery	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithfull_Drivers	A.Periodic_Inspections	A.Trusted_Workshops	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration	T.Card_Data	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	P.L2000_Main	P.L2000_Export
OE.Controls				x						x			x	x		x		x	x				x					
OE.Driver_Card_ Uniqueness					x					x																		
OE.Faithfull_Drivers						x				x																		
OE.Periodic_ Inspections							x						x	x		x		x	x		x		x					
OE.Trusted_Workshops								x						x		x					x							

IX.1.2 Policies

P.L2000_Main..... The data to be measured and recorded by the L2000 and then to be checked by control authorities shall 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.

P.L2000_Main is addressed by the O.Accountability and O.Audit objectives to ensure storage and availability of the appropriate data, by the O.Integrity objective to ensure that measured and stored data will not be un-authorisedly modified , and by the O.Output objective to ensure data will be properly output. The O.Processing and O.Reliability objectives contribute to addressing the policy by ensuring the accuracy of the whole process. The OE.Personalisation objective contributes to addressing the policy by providing the L2000 with necessary permanent identification data.

P.2000_Export..... The L2000 shall be able to export data to external storage media in such a way as to allow for later verification of their integrity and authenticity.

P.L2000_Export is addressed by the O.Output and O.Download objectives to ensure that data will be properly output and bear appropriate security attributes.

IX.1.3 Threats

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

T.Access is addressed by the O.Authentication objective to ensure the identification of the user, the O.Access objective to control access of the user to functions and the O.Audit objective to trace attempts of unauthorised accesses.

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

T.Identification is addressed by the O.Authentication objective to ensure the identification of the user. The O.Accountability objective contributes to address this threat by storing all activity carried (even without an identification) with the L2000. Accountability data gathered at a large scale (from VUs or tachograph cards) by enforcement officers can be analysed to discover such attempts. This analysis is included in the OE.Controls objective for the environment. Users are informed of their responsibility related to properly identifying themselves to the L2000 through the OE.Users objective, and through their obligation to do so by law which explains the OE.Faithfull_Drivers objective. The OE.Driver_Card_Uniqueness, OE.Card_Delivery and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.

T.Faults..... Faults in hardware, software, communication procedures could place the L2000 in unforeseen conditions compromising its security.

T.Faults is mostly addressed by the OE.Reliable_Design, OE.Dvpt_Security and OE.Software_Upgrade objectives for the environment in order to obtain as good a design as possible, by the OE.Manufacturing objective to ensure that manufacturing will correctly follow the design. The O.Reliability objective contributes to address the threat by providing a fault tolerant design.

T.Tests ..... The use of non invalidated test modes or of existing back doors could compromise the L2000 security.

T.Tests is addressed by the OE.Tests_Points objective.

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

T.Design is mostly addressed by the OE.Dvpt_Security objective. The O.Phys_Protection objective contributes to address the threat in conjunction with the OE.Controls and OE.Periodic_Inspections objectives for the environment.

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

T.Calibration is addressed by the O.Access objective to ensure that the calibration function is accessible to workshops only, by the O.Accountability and O.Audit objectives to keep records of calibrations made by the workshops and by the O.Integrity objective to maintain the integrity of calibration parameters stored. Workshops are approved by Member States authorities and are therefore trusted to calibrate properly the equipment (OE.Trusted_Workshops objective). Periodic inspections and calibration of the equipment, as required by law (OE.Periodic_Inspections objective), contribute to address the threat. Finally, the OE.Controls objective includes controls by law enforcement officers of calibration data records held in the L2000, which helps addressing the threat.

T.Card_Data ..... Users could try to modify data while exchanged between L2000 and tachograph cards (addition, modification, deletion, replay of signal).

T.Card_Data is addressed by the O.Data_Exchange objective. The O.Audit objective contributes to address the threat by recording events related to card data exchange integrity or authenticity errors.

T.Clock ..... Users could try to modify internal clock.

T.Clock is addressed by the O.Access objective to ensure that the full time adjustment function is accessible to workshops only, and by the O.Accountability and O.Audit objectives to keep records of time adjustments made by the workshops. Workshops are approved by Member States authorities and are therefore trusted to properly set the clock (OE.Trusted_Workshops objective). Periodic inspections and calibration of the equipment, as required by law (OE.Periodic_Inspections objective), contribute to address the threat. Finally, the OE.Controls objective includes controls by law enforcement officers of time adjustment data records held in the L2000, which helps addressing the threat.

T.Environment..... Users could compromise the L2000 security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).

T.Environment is mostly addressed by the OE.Reliable_Design, objective in order to obtain as good a design as possible, and by the O.Phys_Protection objective to ensure that direct attacks cannot be made inside the equipment. The O.Reliability objective contributes to address the threat by providing a failure tolerant design.

T.Fake_Devices..... Users could try to connect fake devices (motion sensor, smart cards) to the L2000.

T.Fake_Devices is addressed by the O.Authentication objective. The OE.Controls and OE.Periodic_Inspections help addressing the threat through visual inspection of the whole installation.

T.Hardware..... Users could try to modify the L2000 hardware.

T.Hardware is mostly addressed in the user environment by the O.Phys_Protection objective. During design and manufacture, T.Hardware is addressed by the OE.Dvpt_Security, OE.Mnft_Security and OE.Manufacturing objectives. The OE.Controls and OE.Periodic_Inspections help addressing the threat through visual inspection of the installation.

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

T.Motion_Data is addressed by the O.Data_Exchange objective. The O.Audit objective contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

T.Non_Activated... Users could use non activated equipment.

T.Non_Activated is addressed by the OE.Users objective ensuring that the workshops are aware of their responsibility in this domain. Workshops are approved by Member States authorities and are therefore trusted to activate properly the equipment (A.Trusted_Workshops assumption). Periodic inspections and calibration of the equipment, as required by law (A.Periodic_Inspections assumption), also contribute to address the threat.

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

T.Output_Data is mainly addressed by the O.Download objective for data downloaded and by the O.Output and O.Phys_Protection objectives for data displayed of printed.

T.Power_Supply ... Users could try to defeat the L2000 security objectives by modifying (cutting, reducing, increasing) its power supply.

T.Power_Supply is mainly addressed by the OE.Reliable_Design objective and by the O.Reliability objective to ensure appropriate behaviour of the L2000 against the attack. The O.Audit objective contributes to address the threat by keeping records of attempts to tamper with 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.Security_Data is addressed by the OE.Data_Generation, OE.Data_Transport and OE.Mnft_Security objectives in the manufacturing environment. It is addressed by the O.Integrity objective to ensure appropriate protection while stored in the L2000.

T.Software..... Users could try to modify the L2000 software.

T.Software is mostly addressed in the user environment by the O.Integrity objective to ensure the integrity of the code, by the OE.Software_Analysis objective to prevent software analysis in the field and by the O.Phys_Protection objective to prevent physical tampering to the code. The O.Software_Upgrade objective also address the threat by preventing loading of unauthorised software. During design and manufacture, T.Software is addressed by the OE.Dvpt_Security and OE.Software_Upgrade objectives.

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

T.Stored_Data is addressed mainly by the OE.Reliable_Design O.Integrity and O.Access objectives to ensure that no illicit access to data is permitted. The O.Audit objective contributes to address the threat by recording data integrity errors. The O.Processing and O.Reliability objectives contribute also to address the threat.

IX.2 SECURITY REQUIREMENTS RATIONALE

These rationale demonstrate that the identified IT security requirements (and the SFRs in particular) are suitable to meet the identified security objectives and that all dependencies between SFRs and SARs are solved.
This following table demonstrates that the SFRs are necessary to satisfy the security objectives.

				O.Access	O.Accountability	O.Audit	O.Authentication	O.Data_Exchange	O.Download	O.Integrity	O.Output	O.Processing	O.Phys_Protection	O.Reliability	O.Software_Upgrade
FAU	GEN	1	Audit data generation		X	X									
FAU	SAR	1	Audit review		X	X									
FAU	STG	2	Guarantees of audit data availability		X	X				X					
FCS	CKM	1	Cryptographic key generation				X	X							
FCS	CKM	2	Cryptographic key distribution					X							
FCS	CKM	3	Cryptographic key access				X	X	X						
FCS	CKM	4	Cryptographic key destruction				X	X							
FCS	COP	1	Cryptographic operation				X	X	X						
FDP	ACC	2	Complete access control	X						X					
FDP	ACF	1	Security attribute based access control	X						X					
FDP	DAU	1	Basic data authentication						X						
FDP	ETC	2	Export of user data with security attributes						X						
FDP	IFC	1	Subset information flow control		X			X	X		X	X			X
FDP	IFF	1	Simple security attributes		X			X			X	X			X
FDP	ITC	2	Import of user data with security attributes									X			X
FDP	RIP	1	Subset residual information protection	X								X		X	
FDP	SDI	1	Stored data integrity monitoring							X	X				
FDP	UIT	1	Data exchange integrity			X		X							
FIA	AFL	1	Authentication failure handling			X	X								
FIA	ATD	1	User attribute definition		X										
FIA	UAU	2	User authentication before any action				X								
FIA	UAU	3	Unforgeable authentication				X								
FIA	UAU	6	Re-authenticating				X								
FIA	UID	2	User identification before any action	X	X	X									
FPT	AMT	1	Abstract machine testing			X						X		X	
FPT	FLS	1	Failure with preservation of secure state			X						X		X	
FPT	PHP	1	Passive detection of physical attack								X		X		
FPT	SEP	1	TSF domain separation	X						X		X		X	
FPT	STM	1	Reliable time stamps		X	X									
FPT	TST	1	TSF testing			X						X		X	
FRU	PRS	1	Limited priority of service									X		X	
FTP	ITC	1	Inter-TSF trusted channel					X							

This following table demonstrates that the SFRs are sufficient to satisfy the security objectives.

Security objectives	IT security requirements
O.Access	FDP_ACC.2: ..... Controls access to user data and to L2000 functions FDP_ACF.1:..... Defines security attributes of user data and function, according to the mode of operation FDP_RIP.1: ..... Cleans temporary storage objects FIA_UID.2: ..... Identifies user, or process acting for the user, before any action FPT_SEP.1 ..... Separates logically applications in the VU
O.Accountability	FAU_GEN.1:..... Generates correct audit records FAU_SAR.1: ..... Allows users to read accountability records FAU_STG.2: ..... Ensures the availability of accountability data to users. FDP_IFC.1, FDP_IFF.1: ..... Defines information flow control policies FIA_ATD.1: ..... Defines users attributes FIA_UID.2: ..... Identifies user, or process acting for the user, before any action FPT_STM.1:..... Provides accurate time
O.Audit	FAU_GEN.1:..... Generates correct audit records FAU_SAR.1: ..... Allows users to read audit records FAU_STG.2: ..... Ensures the availability of audit data to users. FDP_UIT.1:..... Ensures the integrity of audit records sent by motion sensor for storage in the L2000 FIA.AFL.1 ..... Provides authentication failure events; FIA_UID.2: ..... Identifies user, or process acting for the user, before any action FPT_AMT.1, FPT_FLS.1, FPT_TST.1: Provide failure events. FPT_STM.1:..... Provides accurate time

Security objectives	IT security requirements
O.Authentication	FCS_CKM.1:..... Generates motion sensor's master key FCS_CKM.3:..... Controls access keys stored in the L2000 FCS_CKM.4:..... Controls destruction of keys, which are no more used after authentication process. FCS_COP.1:..... Provides cryptographic operations to authenticate users FIA_AFL.1:..... Controls authorised number of unsuccessful authentication, FIA_UAU.2:..... Authenticates user, or process acting for the user, before any action. FIA_UAU.3:..... Prevent forgeable authentication of users FIA_UAU.6:..... Periodically re-authenticates user, or process acting for the user
O.Data_Exchange	FCS_CKM.1:..... Generate user's session keys FCS_CKM.2:..... Controls distribution of user's session keys FCS_CKM.3:..... Controls access to the session keys stored in the L2000 FCS_CKM.4:..... Controls destruction of user's session keys, which are no more used FCS_COP.1:..... Provides cryptographic operations to secure data exchanges FDP_IFC.1, FDP_IFF.1: ..... Defines information flow control policies FDP_UIT.1:..... Controls data exchanges with motion sensor and tachograph cards to prevent accepting incorrect data. FTP_ITC.1:..... Provides trusted channel to communicate between L2000 and tachograph cards or motion sensor
O.Download	FCS_CKM.3:..... Controls access to keys stored in the L2000 used for securing data download FCS_COP.1:..... Provides cryptographic operations to secure data downloaded FDP_DAU.1:..... Provides evidence to guarantee the validity of data downloaded FDP_ETC.2:..... Provides attributes to data downloaded to enforce data downloading policy FDP_IFC.1: ..... Defines the data downloading policy

Security objectives	IT security requirements
O.Integrity	FAU_STG.2: ..... Controls integrity of audit and accountability records stored in the L2000 FDP_ACC.2: ..... Controls accesses to user data and to L2000 functions FDP_ACF.1:..... Defines security attributes of user data and function, according to the mode of operation FDP_SDI.1: ..... Controls integrity of user data stored in the L2000 FPT_SEP.1 ..... Separates logically applications in the L2000
O.Output	FDP_IFC.1, FDP_IFF.1: ..... Defines information flow control policies FDP_SDI.1: ..... Controls integrity of user data stored in the L2000 FPT_PHP.1:..... Ensures physical attacks on the L2000 may be easily detected.
O.Processing	FDP_IFC.1, FDP_IFF.1: ..... Defines information flow control policies to prevent unauthorised software upgrade. FDP_ITC.2: ..... Controls data imports to prevent accepting unauthorised executable code FDP_RIP.1: ..... Cleans temporary storage objects FPT_FLS.1: ..... Preserves a secure state of the L2000 when failure occurs FPT_AMT.1, FPT_TST.1: ..... Self-tests demonstrate correct operation of data processing FPT_SEP.1: ..... Separates logically applications in the L2000 FRU_PRS.1:..... Ensures that resources will be available when needed.
O.Phys_Protection	FPT_PHP.1:..... Ensures physical attacks on the L2000 may be easily detected.

Security objectives	IT security requirements
O.Reliability	FDP_RIP.1: ..... Cleans temporary storage objects FPT_FLS.1: ..... Preserves a secure state of the L2000 when failure occurs FPT_SEP.1: ..... Separates logically applications in the L2000 FPT_AMT.1, FPT_TST.1: Self-tests demonstrate correct operation of the L2000 FRU_PRS.1 ..... Ensures that resources will be available when needed.
O.Software_Upgrade	FDP_IFC.1, FDP_IFF.1: ..... Defines information flow control policies to prevent unauthorised software upgrade. FDP_ITC.2: ..... Controls data imports to prevent accepting unauthorised executable code

This following table demonstrates and justifies that all dependencies between SFRs and SARs are solved.

IT security requirements	Dependencies
FAU_GEN.1	FPT_STM.1: .....selected
FAU_SAR.1	FAU_GEN.1: .....selected
FAU_STG.2	FAU_GEN.1: .....selected
FCS_CKM.1	FMT_MSA.2: .....not selected, because there is no need for management of security attributes in the L2000 FCS_CKM.4: .....selected [FCS_CKM.2 or FCS_COP.1]: ..... both selected
FCS_CKM.2	FMT_MSA.2: .....not selected, because there is no need for management of security attributes in the L2000 FCS_CKM.4: .....selected [FCS_CKM.1 or FDP_ITC.1]: ..... FCS_CKM.1 selected
FCS_CKM.3	FMT_MSA.2: .....not selected, because there is no need for management of security attributes in the L2000 FCS_CKM.4: .....selected [FCS_CKM.1 or FDP_ITC.1]: ..... FCS_CKM.1 selected
FCS_CKM.4	FMT_MSA.2: .....not selected, because there is no need for management of security attributes in the L2000 [FCS_CKM.1 or FDP_ITC.1]: ..... FCS_CKM.1 selected
FCS_COP.1	FMT_MSA.2: .....not selected, because there is no need for management of security attributes in the L2000 FCS_CKM.4: .....selected [FCS_CKM.1 or FDP_ITC.1]: ..... FCS_CKM.1 selected
FDP_ACC.2	FDP_ACF.1: .....selected
FDP_ACF.1	FMT_MSA.3: .....not selected, because there is no need for management of security attributes in the L2000 FDP_ACC.1:.....selected
FDP_DAU.1	None
FDP_ETC.2	[FDP_IFC.1 or FDP_ACC.1]: ..... FDP_IFC.1 selected

IT security requirements	Dependencies
FDP_IFC.1	FDP_IFF.1 .....selected
FDP_IFF.1	FDP_IFC.1 .....selected FMT_MSA.3 .....not selected, because there is no need for management of security attributes in the L2000
FDP_ITC.2	[FDP_IFC.1 or FDP_ACC.1]: ..... FDP_IFC.1 selected [FTP_ITC.1 or FTP_TRP.1]:..... FTP_ITC.1 selected FPT_TDC.1: .....not selected, because the VU doesn't need to exchange TSF data with another trusted IT product.
FDP_RIP.1	None
FDP_SDI.1	None
FDP_UIT.1	[FDP_IFC.1 or FDP_ACC.1]: ..... FDP_IFC.1 selected [FTP_ITC.1 or FTP_TRP.1]:..... FTP_ITC.1 selected
FIA_AFL.1	FIA_UAU.1: .....selected
FIA_ATD.1	None
FIA_UAU.2	FIA_UID.1:.....selected
FIA_UAU.3	None
FIA_UAU.6	None
FIA_UID.2	None
FPT_AMT.1	None
FPT_FLS.1	ADV_SPM.1:.....not selected, because assurance requirement not needed at the assurance level sought.
FPT_PHP.1	FMT_MOF.1.....not selected, because there is no need for management of security functions in the L2000
FPT_SEP.1	None
FPT_STM.1	None
FPT_TST.1	FPT_AMT.1: .....selected
FRU_PRS.1	None
FTP_ITC.1	None

IX.3 SECURITY FUNCTIONS RATIONALE

These rationale demonstrate that the identified IT security functions cover all security functional requirements and that each IT security function is mapped onto at least one security functional requirement.

This following table demonstrates that the identified IT security functions are necessary to satisfy the security functional requirements.

	F.Events_Faults_Management	F.L2000_Memory_Management	F.TC_Memory_Management	F.Security_Data_Management	F.Data_Download	F.MS_Pairing	F.MS_Management	F.Speed	F.TC_Authenticate	F.TC_Data_Exchange	F.Functions_Access_Control	F.Activities	F.L2000_Management	F.Manual_Inputs_Control	F.Self_Tests	F.Clean	F.Software_Upgrade	F.Power_Supply_Monitoring	F.Time	F.Physical_Tampering_Detection	F.Secrets_Protection
FAU_GEN.1	x	x	x			x	x	x	x	x		x	x		x			x	x		
FAU_SAR.1		x	x		x								x								
FAU_STG.2		x	x																		
FCS_CKM.1				x		x			x												
FCS_CKM.2				x		x			x												
FCS_CKM.3				x		x			x												
FCS_CKM.4				x		x			x							x					
FCS_COP.1				x	x	x	x		x	x							x				
FDP_ACC.2		x		x							x										
FDP_ACF.1		x		x							x										
FDP_DAU.1					x																
FDP_ETC.2					x																
FDP_IFC.1			x		x		x			x		x		x			x				
FDP_IFF.1			x		x		x			x		x		x			x				
FDP_ITC.2																	x				
FDP_RIP.1						x			x							x					
FDP_SDI.1		x													x						
FDP_UIT.1							x			x											
FIA_AFL.1						x	x		x												
FIA_ATD.1						x			x												
FIA_UAU.2						x	x		x												
FIA_UAU.3						x	x		x												
FIA_UAU.6						x	x		x												
FIA_UID.2						x	x		x												
FPT_AMT.1															x						
FPT_FLS.1							x			x							x	x			
FPT_PHP.1																				x	x
FPT_SEP.1																	x				
FPT_STM.1																			x		

	F.Events_Faults_Management	F.L2000_Memory_Management	F.TC_Memory_Management	F.Security_Data_Management	F.Data_Download	F.MS_Pairing	F.MS_Management	F.Speed	F.TC_Authenticate	F.TC_Data_Exchange	F.Functions_Access_Control	F.Activities	F.L2000_Management	F.Manual_Inputs_Control	F.Self_Tests	F.Clean	F.Software_Upgrade	F.Power_Supply_Monitoring	F.Time	F.Physical_Tampering_Detection	F.Secrets_Protection
FPT_TST.1															x						
FRU_PRS.1											x										
FTP_ITC.1						x	x		x	x											

This following table demonstrates that the identified IT security functions are sufficient to satisfy the security functional requirements

IT security requirements	**Security functions**
FAU_GEN.1	F.Time: .....Provides reliable time stamps. F.Activities, F.L2000_Management: .....Provides records of accountable events derived from TOE's inputs. F.Speed .....Provides speed changes. F.MS_Pairing, F.MS_Management, F.TC_Authenticate, F.TC_Data_Exchange, F.Self_Tests, F.Power_Supply_Monitoring: .....Raise events or faults. F.Events_Faults_Management; .....Provides records of events and faults. F.L2000_Memory_Management: .....Manages records storage in L2000 memory. F.TC_Memory_Management: .....Manages records storage in tachograph cards, raises event 'last card session not correctly closed'.
FAU_SAR.1	F.Data_Download:.....Exports audit and accountability data to external media. F.L2000_Memory_Management, F.TC_Memory_Management: .....Reads audit and accountability records. F.L2000_Management: .....Displays or prints audit and accountability data.
FAU_STG.2	F.L2000_Memory_Management: .....Manages records deletion in L2000 memory. F.TC_Memory_Management: .....Manages records deletion in tachograph cards.

IT security requirements	Security functions
FCS_CKM.1	F.Security_Data_Management: .....Generates on board the L2000 RSA key pair, and computes a Diversified Transport key. F.MS_Pairing:.....Generates the motion sensor TDES master key by combining one part received from workshop card and the second stored in the L2000, derives a motion sensor TDES Pairing Key from data received from the motion sensor, and generates a TDES session key for further exchanges between the L2000 and the motion sensor. F.TC_Authenticate: .....Generates a TDES session key for further exchanges between the L2000 and a tachograph card.
FCS_CKM.2	F.Security_Data_Management: .....Sends the L2000 public key to key Certification Authority. F.MS_Pairing:.....Sends a session key to the motion sensor. F.TC_Authenticate: .....Exchanges data with a tachograph card to allow the L2000 and the card to agree a common session key. Distributes the L2000 public key to cards
FCS_CKM.3	F.Security_Data_Management: .....Provides the diversified transport key, L2000 RSA key pair, L2000 public key certificates, European public key, VU half key (of motion sensor Master key). F.MS_Pairing:.....Provides motion sensor Master key, pairing key and session key. F.TC_Authenticate .....Provides the public keys of tachograph cards, or Member states
FCS_CKM.4	F.Security_Data_Management: .....Controls the conditions under which security data may be erased. Erases the diversified transport key after use. F.MS_Pairing, F.TC_Authenticate, F.Clean: .....Ensures that temporary objects, like session keys, parts of keys, PIN codes, are cleanly erased before de-allocated.

IT security requirements	Security functions
FCS_COP.1	F.Security_Data_Management: .....Signs (MAC) the L2000 public key when sending to the key Certification Authority, Verifies MACs when importing security data, Decrypts (TDES) security data when importing. F.MS_Pairing:.....Performs decryption of the part of the motion sensor Master Key received from a Workshop card, performs TDES encryption and decryption of data exchanged with the motion sensor during the pairing and authentication process. F.MS_Management: ....Performs TDES encryption and decryption of data with a session key. F.TC_Authenticate: .....Performs RSA encryption and decryption. F.TC_Data_Exchange: Performs encryption and decryption of MACs with session keys. F.Data_Download:.....Signs data to be downloaded with the L2000 private RSA key. F.Software_Upgrade:...Performs signature verification with the manufacturer's RSA public key.
FDP_ACC.2	F.L2000_Memory_Management: .....Enforces the file_structure_policy. F.Security_Data_Management: .....Enforces the L2000_ID_policy. F.Functions_Access_Control: .....Enforces the functions_access_policy.
FDP_ACF.1	F.L2000_Memory_Management: .....Enforces the file_structure_policy. F.Security_Data_Management: .....Enforces the L2000_ID_policy. F.Functions_Access_Control: .....Enforces the functions_access_policy.
FDP_DAU.1	F.Data_Download:.....Signs data to be downloaded with the L2000 private RSA key.
FDP_ETC.2	F.Data_Download:.....Signs data to be downloaded with the L2000 private RSA key.
FDP_IFC.1	F.TC_Memory_Management: .....Enforces the Card_release_policy. F.Data_Download:.....Enforces the Data_download_policy. F.MS_Management: ....Enforces the Motion_sensor_exchanges_policy and the Motion_data_flow_policy. F.TC_Data_Exchange: Enforces the Tacho_card_exchanges_policy. F.Activities: .....Enforces the Internal_data_flow_policy. F.Manual_Inputs_Control: .....Enforces the Manual_inputs_policy. F.Software_Upgrade:...Enforces the Software_import_policy.

IT security requirements	Security functions
FDP_IFF.1	F.TC_Memory_Management: .....Enforces the Card_release_policy. F.Data_Download:.....Enforces the Data_download_policy. F.MS_Management: ....Enforces the Motion_sensor_exchanges_policy and the Motion_data_flow_policy. F.TC_Data_Exchange: Enforces the Tacho_card_exchanges_policy. F.Activities: .....Enforces the Internal_data_flow_policy. F.Manual_Inputs_Control: .....Enforces the Manual_inputs_policy. F.Software_Upgrade:...Enforces the Software_import_policy.
FDP_ITC.2	F.Software_Upgrade:...Verifies the authenticity and integrity of imported software.
FDP_RIP.1	F.MS_Pairing, F.TC_Authenticate, F.Clean: .....Cleans temporary storage objects.
FDP_SDI.1	F.L2000_Memory_Management: .....Verifies records integrity after writing to memory. F.Selft_Tests:.....Stored data integrity monitoring.
FDP_UIT.1	F.MS_Management: ....Controls integrity of data exchanged with the motion sensor. F.TC_Data_Exchange: Controls integrity of data exchanged with tachograph cards.
FIA_AFL.1	F.MS_Pairing:.....Raises an authentication failure event after 20 unsuccessful authentication of the motion sensor. F.MS_Management: ....Raises an authentication failure event after 20 unsuccessful authentication of the motion sensor. F.TC_Authenticate: .....Raises an authentication failure event after 5 unsuccessful authentication of a tachograph card.
FIA_ATD.1	F.MS_Pairing:.....Authenticates the motion sensor and establishes its identity during pairing sequence. F.TC_Authenticate: .....Authenticates tachograph cards and establishes their identity.
FIA_UAU.2	F.MS_Pairing:.....Authenticates the motion sensor during pairing sequence. F.MS_Management: ....Authenticates the motion sensor regularly during normal operation. F.TC_Authenticate: .....Authenticates tachograph cards at insertion and regularly.
FIA_UAU.3	F.MS_Pairing:.....Combines use of the master key, a pairing key and a session key for sensor authentication. F.MS_Management: ....Combines the use of the session key and randoms for sensor authentication F.TC_Authenticate: .....Combines the use of the VU private key, the tachograph card's public key and randoms for card authentication.

IT security requirements	Security functions
FIA_UAU.6	F.MS_Pairing.....Re-authenticates the motion sensor at each calibration, or session key renewal. F.MS_Management: ....Authenticates the motion sensor regularly during normal operation. F.TC_Authenticate: .....Authenticates tachograph cards at insertion and regularly.
FIA_UID.2	F.MS_Pairing:.....Authenticates the motion sensor and establishes its identity during pairing sequence. F.MS_Management: ....Verifies the motion sensor's identity regularly during normal operation. F.TC_Authenticate: .....Authenticates tachograph cards and establishes their identity.
FPT_AMT.1	F.Self_Tests: .....Runs hardware tests to verify correct L2000 operation.
FPT_FLS.1	F.MS_Management, F.TC_Data_Exchange: .....Manage failed transactions. F.Software_Upgrade:...Prevents use of software upgrade data when errors occurred during update. F.Power_Supply_Monitoring: .....Monitors power supply deviations to restrict processing when out of specified range.
FPT_PHP.1	F.Physical_Tampering_Detection, F.Secrets_Protection: .....Ensure that any tampering attempt shall be easily detected.
FPT_SEP.1	F.Software_Upgrade:...Ensures that untrusted code cannot modify or damage the TSF.
FPT_STM.1	F.Time: .....Provides reliable time stamps.
FRU_PRS.1	F.Functions_Access_Control: .....Manages tasks priorities.
FTP_ITC.1	F.MS_Pairing:.....Initialises the channel with the motion sensor. F.MS_Management: ....Maintains the channel during normal operation. F.TC_Authenticate: .....Initialises the channel with a tachograph card. F.TC_Data_Exchange: Maintains the channel during normal operation.

X. GLOSSARY

CC ..... Common Criteria
DES ..... Data Encryption Standard
EAL..... Evaluation Assurance Level
IT..... Information Technology
MAC ..... Message Authentication Code
MS..... Motion Sensor
PP..... Protection Profile
RSA..... Asymmetric encryption algorithm
SF ..... Security Function
SFP..... Security Function Policy
SOF ..... Strength Of Function
ST ..... Security Target
TBD..... To Be Defined
TC ..... Tachograph Card
TDES..... Triple DES
TOE..... Target Of Evaluation
TSC ..... TSF Scope of Control
TSF..... TOE Security Functions
TSFI..... TSF Interface
TSP..... TOE Security Policy
VU ..... Vehicle Unit