ICitizen Tachograph

Common Criteria / ISO 15408

Security Target – Public version

EAL4+

CONTENT

List of figures

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: ICitizen Tachograph Security Target
Registration: Ref. MRD11STT033047 rev 1.0
Origin: SCHLUMBERGER

TOE reference: M256LFCHRON_SI_A5_05_01

The TOE is composed with:

Component	Version number	Supplier
Micro-controller SLE66CX322P	GC/B14	Infineon
RMS library	1.3	Infineon
ACE library	1.0	Infineon
ROM MASK	SB102 (Infineon)	Schlumberger
SOFT MASK	No softmask	Schlumberger
GEOS	PLATFORM_T_SC_04_02;9	Schlumberger
Tachograph Applet	SC_V0.9.0	Schlumberger

TOE function type and options: Secure signature generation card.

This ST:
- claims the Protection Profile [PP/BSI-0002] for the IC,
- Is based on the Protection Profile [PP/9911] for the ES.

The IC is evaluated under the German scheme for Common Criteria. The certification body is the 'Bundesamt für Sicherheit in der Informationstechnik' (BSI).
This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the IC. This evaluation is done under the French scheme for Common Criteria. The certification body is the 'Direction Centrale de la Sécurité des Systèmes d'Information' (DCSSI).

1.2 ST OVERVIEW

Context
The Commission of the European Communities has adopted a council regulation concerning a recorded equipment in road transport. The annex 1B of this document ([EEC/A1B]) gives the requirements for construction, testing, installation and inspection of this recording equipment.
The purpose of the recording equipment is to record, store, display, print, and output data related to driver activities.
[EEC/A1B] defines the tachograph card that is used in this equipment and [EEC/A1B] Appendix 10 gives a generic Security Target for this tachograph card.
In [JIL/Tacho], DCSSI and other Certification bodies have given an interpretation that defines the rules to be applied for the evaluation of the Tachograph Card.
The product to be evaluated complies with the requirements of [EEC/A1B], as interpreted by [JIL/Tacho].

Objectives
The main objectives of this security target are:
- To describe the Target of Evaluation (TOE). This ST focuses on the Tachograph Card.
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by its environment.

- To describe the security objectives of the TOE and its supporting environment.
- To specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.
- To specify the TOE summary specification, which includes the TOE security functions specifications and the assurance measures.

Assurance level

The assurance level for this product and its documentation is EAL4 augmented with:

ADO_IGS.2: Generation log,
ADV_IMP.2: Implementation of the TSF,
ALC_DVS.2: Sufficiency of security measures.
ATE_DPT.2: Testing low-level design,
AVA_MSU.3: Analysis of insecure states,
AVA_VLA.4: Highly resistant,

The strength level for the TOE security functional requirements is “SOF high” (Strength Of Functions high).

1.3 CC CONFORMANCE

The compliance is assumed with CC version V2.1 (ISO 15408) (see reference in 1.5.1).
This ST is built on [EEC/A1B], [PP/9911] and [PP/BSI-0002]. It is conformant to [EEC/A1B] as interpreted by [JIL/Tacho]. It is conformant to [PP/BSI-0002]. It is based on [PP/9911]: it includes all assets, threats, assumptions, objectives and SFR of this PP but it includes an IC which claims [PP/BSI-0002], not the older [PP/9806] required by [PP/9911].
This ST is CC V2.1 conformant with Part2.
This ST is CC V2.1 conformant with Part3 augmented as stated in [PP/9911] and [PP/BSI-0002].

1.4 CURRENT ST VS. [ST/INFINEON]

This ST is defined for the whole TOE, including the IC and the ES. However, the IC has its own ST, [ST/Infineon] and the assets, threats, objectives, SFR and Security functions specific to the IC that are described in this ST are not described in the current ST.
[ST/Infineon] refines the assets, threats, objectives and SFR of [PP/BSI-0002].
The current ST refines the assets, threats, objectives and SFR of [PP/9911] and [EEC/A1B]. It also states how the SF of the current ST relies on the SF of [ST/Infineon].

1.5 REFERENCES

1.5.1 EXTERNAL REFERENCES [ER]

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB - 99-031, version 2.1, August 1999 (conform to ISO 15408)
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-99-032, version 2.1, August 1999 (conform to ISO 15408)
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-99-033, version 2.1, August 1999 (conform to ISO 15408)
[CEM]	Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0, August 1999.
[PP/9806]	Protection Profile - Smart Card Integrated Circuit
[PP/9911]	Protection Profile - Smart Card Integrated Circuit With Embedded Software
[PP/BSI-0002]	Smartcard IC Platform Protection Profile
[EEC/A1B]	Council Regulation No 3821/85 on recording equipment in road transport – Annex 1B Requirements for construction, Installation and Inspection

[JIL/Tacho]	Joint Interpretation Library – Security Evaluation and Certification of Digital Tachograph
[OP2.0.1']	Open Platform – Card Specification version 2.0.1' dated 7 April 00
[RSA-PKCS#1]	PKCS1 v2.1 RSA Cryptography Standard
[SHA-1]	FIPS PUB 180-1 Secure Hash Standard
[FIPS 46-3]	FIPS PUB 46-3 Data Encryption Standard (DES)

2 TOE DESCRIPTION

This part of the ST describes the TOE, to enable the understanding of its security requirements.
It addresses the product type, the smart card product life cycle, the TOE environment along the smart card life cycle and the general IT features of the TOE.

2.1 PRODUCT TYPE

2.1.1 SCOPE OF THE TOE

The Target of Evaluation (TOE) is the Tachograph micro-module “PHAESTOS” defined by:

- The underlying Integrated Circuit and its libraries;
- The Generic Operating System (GEOS), corresponding to the generic system software and the Java Virtual Machine (JVM);
- The Tachograph Application.

In the personalization and usage phases, the micro-module will be inserted in a plastic card. Therefore when the TOE is in personalization and usage phases, the expression “Tachograph card” will often be used instead of “Tachograph micro-module”

The Figure below gives a description of the TOE and its boundaries. The bold line defines the limits of the TOE.

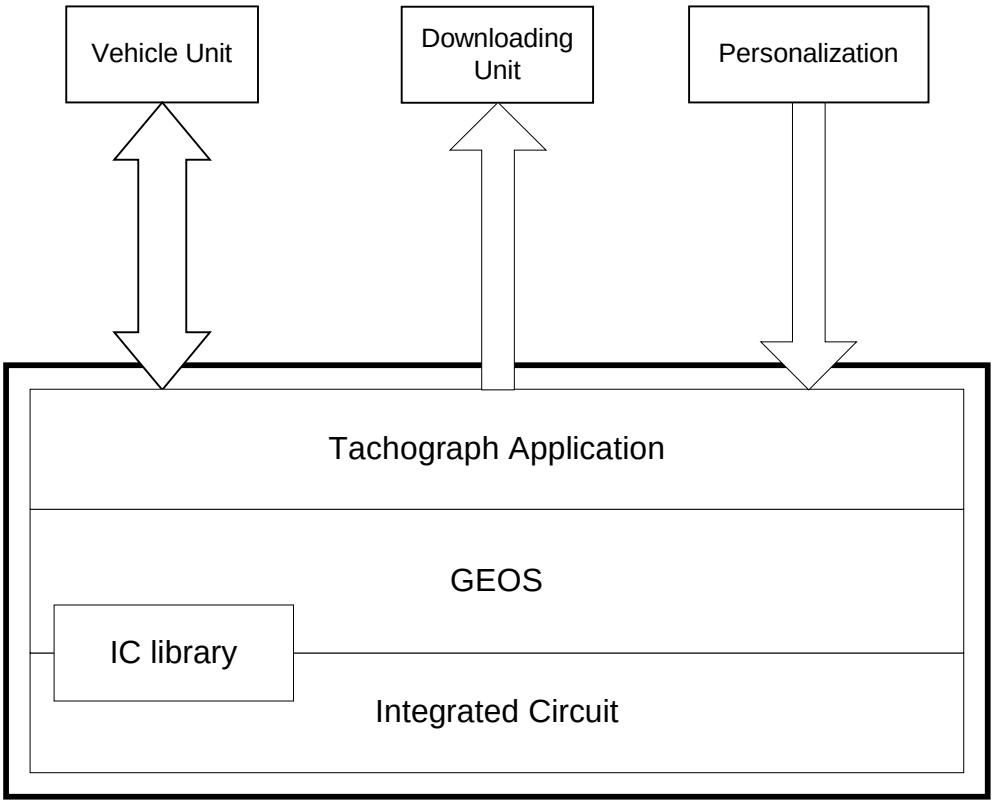

Figure 1 The Tachograph card and its boundaries

The TOE is the micro-module made of the Integrated Circuit (IC) and its embedded software (ES). The ES comprises GEOS and the Tachograph Applet. It includes the associated embedded data of the smart card working on the micro-controller unit in accordance with the functional specifications.
The plastic card is outside the scope of this Security Target.

2.1.2 TOE DESCRIPTION

A tachograph card is a smart card, as described in [PP/BSI-0002] and [PP/9911], carrying an application intended for its use with the recording equipment.
The basic functions of the tachograph card are:

- to store card identification and card holder identification data. These data are used by the vehicle unit to identify the cardholder, provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

A tachograph card is therefore intended to be used by a card interface device of a vehicle unit. It may also be used by any card reader (e.g. of a personal computer) who shall have full read access right on any user data.
During the end-usage phase of a tachograph card life cycle (phase 7 of life-cycle as described in [PP/9911]), only vehicle units may write user data to the card.
The functional requirements for a tachograph card are specified in [EEC/A1B] body text and Appendix 2.

“tachograph card” means:
smart card 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;

“company card” means:
a tachograph card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment;
the company card identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company;

“control card” means:
a tachograph card issued by the authorities of a Member State to a national competent control authority;
the control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading;

“driver card” means:
a tachograph card issued by the authorities of a Member State to a particular driver;
the driver card identifies the driver and allows for storage of driver activity data;

“workshop card” means:
a tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State.
The workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recording equipment;

Further description can be found in [EEC/A1B]

The TOE is designed for the four types of cards. The personalization process differentiates these types of cards.

2.2 SMART CARD PRODUCTS LIFE-CYCLE

The Smart card product life cycle, as defined in [PP/BSI-0002], is split up into 7 phases where the following authorities are involved:

Phase 1	Smart card software development	**The smart card embedded software developer** is in charge of the smart card embedded software development and the specification of IC pre-personalisation requirements.
Phase 2	IC Development	**The IC designer** designs the integrated circuit, develops IC firmware if applicable, provides information, software or tools to the smart card software developer, and receives the software from the developer, through **trusted delivery and verification procedures**. From the IC design, IC firmware and smart card embedded software, he constructs the smart card IC database, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and testing	**The IC manufacturer** is responsible for producing the IC through three main steps: IC manufacturing, testing, and IC pre-personalisation.
Phase 4	IC packaging and testing	**The IC packaging manufacturer** is responsible for the IC packaging and testing.
Phase 5	Smart card product finishing process	**The smart card product manufacturer** is responsible for the smart card product finishing process and testing, and the smart card pre-personalisation
Phase 6	Smart card personalisation	**The Personaliser** is responsible for the smart card personalisation and final tests.
Phase 7	Smart card end-usage	**The smart card issuer** is responsible for the smart card product delivery to **the smart card end-user**, and for the end of life process.

Refinement:
In Phase 4, the IC packaging includes the pre-personalization of the micro-module.

The Tachograph Card life as described in [PP/BSI0002] can be matched as shown in Figure 2: Tachograph Card Life Cycle.
OS design and **application design** correspond to life phase 1 “Smart card software development”.
Hardware design corresponds to life phase 2 “IC development”.
Hardware fabrication OS and Application implementation correspond to life phase 3 “IC manufacturing and testing”, phase 4 “IC packaging and testing”, phase 5 “Smart card product finishing process”.
Loading of general application data and **Signature key import** corresponds to life phase 6 “Smart card personalisation”.
Storing of Activity data and **Downloading of user data** correspond to life phase 7 “Smart card usage”.

The global security requirements of the TOE mandate to consider, during the development phase, the threats to security occurring in the other phases. This is why this ST addresses the functions used in phases 5, 6 and 7 but developed during phases 1 to 4.
The limits of the evaluation process correspond to phases 1 to 4 including the TOE under development delivery from the party responsible for each phase to the parties responsible of the following phases. These different phases may be performed at different sites. This implies that procedures on the delivery process of the TOE must exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from any phase between 1 and 4 to subsequent phases. This includes

- Intermediate delivery of the TOE or the TOE under construction within a phase,
- Delivery of the TOE or the TOE under construction from one phase to the next.

These procedures must be compliant with the security assurance requirements developed in section 5.2.

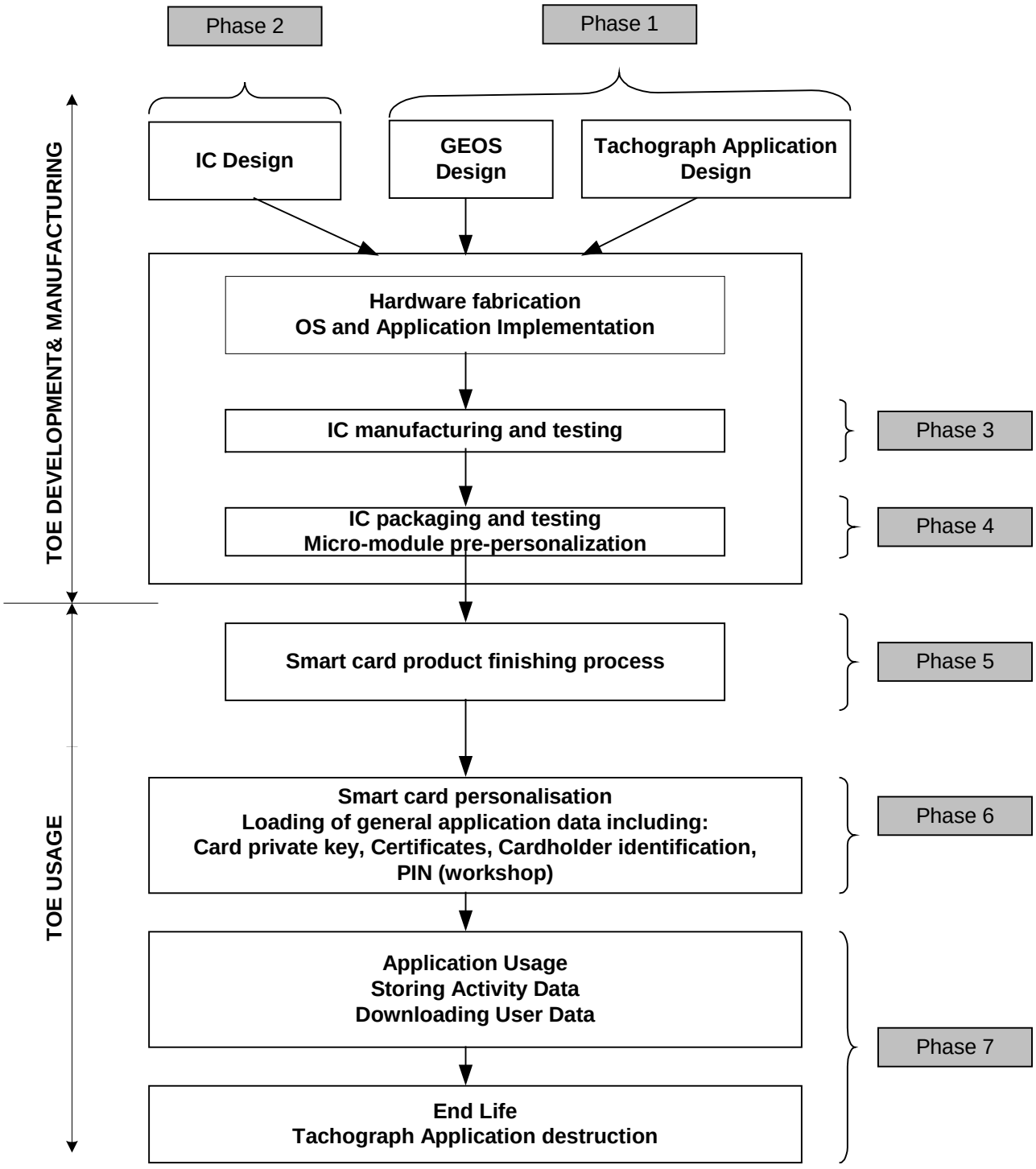

Figure 2: Tachograph Card Life Cycle

2.3 TOE ENVIRONMENT

Considering the TOE, four types of environment are defined:

- Development and fabrication environment (phase 1 to 4),
- Initialisation environment corresponding to Smart card product finishing (phase 5)
- Card personalization: loading of TOE application data (phase 6),
- User environment, during which the card stores and downloads data in files (phase 7),
- End of life environment, during which the TOE is made inapt for storing and downloading data in files (end of the phase 7).

2.3.1 TOE DEVELOPMENT & PRODUCTION ENVIRONMENT

The TOE described in this ST is developed in different places as indicated below:

IC design	Infineon München
Secure OS Design	Schlumberger Louveciennes
Tachograph Application design	Schlumberger Louveciennes
IC manufacturing and Testing	Infineon München
IC packaging and testing	Schlumberger Orleans

In order to ensure security, the environment in which the development takes place must be made secure with access control tracing entries. Furthermore, it is important that all authorised personnel feels involved and fully understands the importance and the rigid implementation of the defined security procedures.
The development begins with the TOE specification. All parties in contact with sensitive information are required to abide by Non-disclosure Agreement.
Design and development of the ES then follows. The engineers use a secure computer system (preventing unauthorised access) to make the conception, design, implementation and test performances.
Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).
Testing, programming and deliveries of the TOE then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.
During the electronic transfer of sensitive data, procedures must be established to ensure that the data arrive, only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies). It must also be ensured that transfer is done without modification or alteration.
During fabrication, phases 3, and 4, all the persons involved in the storage and transportation operations should fully understand the importance of the defined security procedures.
Moreover, the environment in which these operations take place must be secured.
The TOE Initialisation is performed in [Infineon München phase 3; Orleans phase 4].
In the initialisation environment of the TOE, module pre-personalisation takes place.
During module pre-personalisation the applet is instantiated. At the end of this phase, the loader of executable files is blocked.
Initialisation requires a secure environment, which guarantees the integrity and confidentiality of operations.

2.3.2 CARD MANUFACTURING ENVIRONMENT

The Card manufacturing takes place in the Imprimerie Nationale. The micro-module is inserted in a plastic card. In this environment, the personalisation takes place (phase 6). Additional data such as Cardholder Identification data is loaded and the Private key is imported or generated by the TOE. Then the Tachograph card is issued to the end User.

2.3.3 USAGE ENVIRONMENT

Once delivered to the end user (phase 7), the TOE can store activity data and download user data.
The TOE is owned by the end user who cannot impose strict security rules. It is the responsibility of the TOE to ensure that the security requirements are met.

2.3.4 END OF LIFE ENVIRONMENT.

End of life must be considered for several reasons:
The Signature Key can be compromised.
The TOE physical support can come to the end of its useful life.
In all these cases, it must be ensured that the TOE cannot be used any more for downloading valid signed user data.

2.3.5 THE ACTORS AND ROLES

For the tachograph application, two roles have been identified, the Administrator, also called Issuer and the User also called the owner.
The Administrator acts during the personalisation phase (TOE life cycle phase 6). He creates the User's PIN and imports the Card private key into the TOE or generates this key in the TOE.
The User that owns the TOE is the End-User in the usage phase (phase 7). He can store Activity data and download User data.

2.4 TOE INTENDED USAGE

The TOE intended usage is the Storing and Downloading of data related to a person and his activity, as defined previously.

3 TOE SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE is to be used. It describes the assets to be protected, the threats, the organisational security policies and the assumptions.

3.1 ASSETS

Asset name	Data type	Description
D.IC_DESIGN	TSF DATA	the IC specifications, design, development tools and technology
D.IC_CODE	TSF executable code	the IC Dedicated software
D.ES_CODE	TSF executable code	the Smart Card Embedded Software including specifications, implementation and related documentation
D.AP_DATA	USER DATA or TSF DATA	the application data of the TOE (such as IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data,)

The TOE itself is therefore an asset.
Assets have to be protected in terms of confidentiality, and integrity

Refinement:
D.AP_DATA can be refined as follows:

Asset name	Data type	Description
TDES master Keys VOP	TSF DATA	TDES master keys used to compute TDES session keys
TDES session Keys VOP	TSF DATA	TDES session keys VOP derived from TDES master keys VOP
TDES session Keys A1B	TSF DATA	TDES session keys computed for the A1B Secure Channel
Euro public key	TSF DATA	Public key to verify countries' certificates
Card private key	TSF DATA	Private RSA key to sign data
User data	USER DATA	User data as defined in [DEF_PHAESTOS]
PIN	USER DATA	User PIN (Workshop card)

3.2 ASSUMPTIONS

3.2.1 ASSUMPTIONS ON PHASE 1

The current TOE' development include phase 1. Therefore the assumptions on phase 4 have been translated into Organisational Security Policies.

3.2.2 ASSUMPTIONS ON THE TOE DELIVERY PROCESS (PHASES 5 TO 7)

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following assumptions:

Assumption name	Description
A.DLV_PROTECT	Procedures shall ensure protection of TOE material/information under delivery and storage.
A.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
A.DLV_RESP	Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

Note: in [PP/9911], these assumptions also covered phase 4. The current TOE' development include phase 4. Therefore the TOE is protected by objectives on the environment: O.DLV_PROTECT, O.DLV_AUDIT and O.DLV_RESP.
However, we keep the assumptions on phase 4 to keep the rationale of [PP/9911].

3.2.3 ASSUMPTIONS ON PHASES 5 TO 6

Assumption name	Description
A.USE_TEST	It is assumed that appropriate functionality testing of the TOE is used in phases 5 and 6.
A.USE_PROD	It is assumed that security procedures are used during all manufacturing and test operations through phases 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

Note: in [PP/9911], these assumptions also cover phase 4. The current TOE' development include phase 4. Therefore the assumptions on phase 4 have been translated into Organisational Security Policies.

3.2.4 ASSUMPTIONS ON PHASE 7

Assumption name	Description
A.USE_DIAG	It is assumed that secure communication protocols and procedures are used between Smart Card and terminal.

3.3 THREATS

A threat agent wishes to abuse the assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.
Threats have to be split in:
- threats against which specific protection within the TOE is required (class I),
- threats against which specific protection within the environment is required (class II).

3.3.1 THREATS FROM [PP/9911]

3.3.1.1 Unauthorized full or partial cloning of the TOE

Threat name	Description
T.CLON	Functional cloning of the TOE (full or partial) appears to be relevant to all phases of the TOE life-cycle, from phase 1 to phase 7, but only phases 1 and 4 to 7 are considered here, since functional cloning in phases 2 and 3 are purely in the scope of Smart Card IC PP. Generally, this threat is derived from specific threats combining unauthorized disclosure, modification or theft of assets at different phases.

3.3.1.2 Threats on phase 1

During phase 1, three types of threats have to be considered:
a) threats on the Smart Cards Embedded Software and its development environment, such as unauthorized disclosure, modification or theft of the Smart Card Embedded Software and/or initialization data at phase 1.
b) threats on the assets transmitted from the IC designer to the Smart Card software developer during the Smart Card ES development ;
c) threats on the Smart Card Embedded Software and initialization data transmitted during the delivery process from the Smart Card software developer to the IC designer.

Unauthorized disclosure of assets
This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

Threat name	Description
T.DIS_INFO (type b)	Unauthorized disclosure of the assets delivered by the IC designer to the Smart Card Embedded Software developer, such as sensitive information on IC specification, design and technology, software and tools if applicable.
T.DIS_DEL* (type c)	Unauthorized disclosure of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery to the IC designer.
T.DIS_ES1 (type a)	Unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or Application Data(such as secrets, or control parameters for protection system, specification and implementation for security

Threat name	Description
	mechanisms).
T.DIS_TEST_ES (type a and c)	Unauthorized disclosure of the Smart Card ES test programs or any related information.

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such an attacker may personalize, modify or influence the product in order to gain access to the Smart Card application system.

Threat name	Description
T.T_DEL (type c)	Theft of the Smart Card Embedded Software and any additional application data (such as pre-personalization requirements) during the delivery process to the IC designer.
T.T_TOOLS (type a and b)	Theft or unauthorized use of the Smart Card ES development tools (such as PC, development software, data bases).
T.T_SAMPLE2 (type a)	Theft or unauthorized use of TOE samples (e.g. bond-out chips with the Embedded Software).

Unauthorized modification of assets

The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementation of malicious Trojan horses.

Threat name	Description
T_MOD_DEL (type c)	Unauthorized modification of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.
T.MOD (type a)	Unauthorized modification of ES and/or Application Data or any related information (technical specifications).

3.3.3. Threats on delivery for/from phase 1 to phases 4 to 6

Threats on data transmitted during the delivery process from the Smart Card developer to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.
These threats are described hereafter:

Threat name	Description
T.DIS_DEL1	Unauthorized disclosure of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

Threat name	Description
T.DIS_DEL2	Unauthorized disclosure of Application Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
T.MOD_DEL1	Unauthorized modification of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.
T.MOD_DEL2	Unauthorized modification of Application Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

3.3.4. Threats on phases 4 to 7

During these phases, the assumed threats could be described in three types:

- unauthorized disclosure of assets,
- theft or unauthorized use of assets,
- unauthorized modification of assets.

Unauthorized disclosure of assets

This type of threat covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

Threat name	Description
T.DIS_ES2	Unauthorized disclosure of ES and Application Data (such as data protection systems, memory partitioning, cryptographic programs and keys).

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operation for which they are not allowed. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulently access to the Smart Card system

Threat name	Description
T.T_ES	Theft or unauthorized use of TOE. (e.g. bound out chips with embedded software).
T.T_CMD	Unauthorized use of instructions or commands or sequence of commands sent to the TOE.

Unauthorized modification of assets

The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threat includes the implementation of malicious Trojan horses, Trapdoors, downloading of viruses or unauthorized programs.

Threat name	Description
T.MOD_LOAD	Unauthorized loading of programs.
T.MOD_EXE	Unauthorized execution of programs.

Threat name	Description
T.MOD_SHARE	Unauthorized modification of program behavior by interaction of different programs.
T.MOD_SOFT	Unauthorized modification of Smart Card Embedded Software and Application Data.

3.3.2 THREATS FROM [EEC/A1B]

TOE's assets may be attacked by:

- trying to gain illicit knowledge of TOE's hardware and software design and especially of its security functions or security data. Illicit knowledge may be gained though attacks to designer or manufacturer material (theft, bribery, …) or through direct examination of the TOE (physical probing, inference analysis, …),
- taking advantage of weaknesses in TOE design or realisation (exploit errors in hardware, errors in software, transmission faults, errors induced in TOE by environmental stress, exploit weaknesses of security functions such as authentication procedures, data access control, cryptographic operations, …),
- modifying the TOE or its security functions through physical, electrical or logical attacks or combination of these.

Threat name	Description
T.Ident_Data	A successful modification of identification data held by the TOE (e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.
T.Activity_Data	A successful modification of activity data stored in the TOE would be a threat to the security of the TOE.
T.Data_Exchange	A successful modification of activity data (addition, deletion, modification) during import or export would be a threat to the security of the TOE.

3.3.3 CLASSIFICATION OF THREATS

Threats	Phase 1	Phase 4	Phase 5	Phase 6	Phase 7
T.CLON	Class II	Class I	Class I	Class I	Class I
T.DIS_INFO	Class II				
T.DIS_DEL	Class II				
T.DIS_DEL1	Class II				
T.DIS_DEL2		Class II	Class II	Class II	
T.DIS_ES1	Class II				
T.DIS_TEST_ES	Class II				
T.DIS_ES2		Class I	Class I	Class I	Class I
T.T_DEL	Class II				
T.T_TOOLS	Class II				
T.T_SAMPLE2	Class II				
T.T_ES		Class I	Class I	Class I	Class I
T.T_CMD		Class I	Class I	Class I	Class I
T.MOD_DEL	Class II				
T.MOD_DEL1	Class II				
T.MOD_DEL2		Class II	Class II	Class II	
T.MOD	Class II				
T.MOD_SOFT		Class I	Class I	Class I	Class I
T.MOD_LOAD		Class I	Class I	Class I	Class I
T.MOD_EXE		Class I	Class I	Class I	Class I
T.MOD_SHARE		Class I	Class I	Class I	Class I
T.Ident_Data				Class I	Class I
T.Activity_Data					Class I
T.Data_Exchange					Class I

3.4 ORGANIZATIONAL SECURITY POLICIES

3.4.1 ORGANIZATIONAL SECURITY POLICIES FROM [PP/9911]

Organisational Security Policy name	Description
OSP.DEV_ORG	Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity, of Smart Card Embedded Software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation ...) shall exist and be applied in software development
OSP.DLV_PROTECT	Procedures shall ensure protection of TOE material/information under delivery and storage.
OSP.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
OSP.DLV_RESP	Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.
OSP.USE_TEST	It is assumed that appropriate functionality testing of the TOE is used in phases 4.
OSP.USE_PROD	It is assumed that security procedures are used during all manufacturing and test operations through phases 4 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

3.4.2 ADDITIONAL ORGANIZATIONAL SECURITY POLICIES

Organisational Security Policy name	Description
OSP.Secret_Private_Keys	The Issuer must ensure that Secret & Private keys, when outside the TOE, are handled securely. The disclosure of these keys may give hackers access to the TOE. The Private Keys include the European private Key, the Countries' Private keys and the VU private keys. The Secret Keys include VOP TDES keys.
OSP.Qualified certificates	The Issuer must ensure that all certificates used in the Tachograph system are handled properly inside a reliable PKI. This includes the revocation of a certificate when the corresponding key is not secure.

4 SECURITY OBJECTIVES

The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation and environment during development and production phases.

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 SECURITY OBJECTIVES OF [PP/9911]

The TOE shall use state of art technology to achieve the following IT security objectives, and for that purpose, when IC physical security features are used, the specification of those IC physical security features shall be respected. When IC physical security features are not used, the Security Objectives shall be achieved in other ways:

Security Objectives	Description
O.TAMPER_ES	The TOE must prevent tampering with its security critical parts. Security mechanisms have especially to prevent the unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys. The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.
O.CLON	The TOE functionality must be protected from cloning.
O.OPERATE	The TOE must ensure continued correct operation of its security functions
O.FLAW	The TOE must not contain flaws in design, implementation or operation.
O.DIS_MECHANISM2	The TOE shall ensure that the ES security mechanisms are protected against unauthorized disclosure.
O.DIS_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against unauthorized disclosure.
O.MOD_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.

4.1.2 SECURITY OBJECTIVES OF [EEC/A1B]

The main security objectives of the TOE, contributing to the global security objective of the entire digital Tachograph are the following:

Security Objectives	Description
O.Card_Identification_Data	The TOE must preserve card identification data and cardholder identification data stored during card personalisation process,
O.Card_Activity_Storage	The TOE must preserve user data stored in the card by vehicle units.

In addition to the smart card general security objectives listed in (ES PP) and (IC PP), the specific IT security objectives of the TOE that contributes to its main security objectives during its end-usage life-cycle phase are the following:

Security Objectives	Description
O.Data_Access	The TOE must limit user data write access rights to authenticated vehicle units,
O.Secure_Communications	The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

This section describes the security objectives for the environment.

4.2.1 SECURITY OBJECTIVES OF [PP/9911]

4.2.1.1 Objectives on phase 1

Security Objectives	Description
O.DEV_TOOLS	The Smart Card ES shall be designed in a secure manner, by using exclusively software development tools (compilers assemblers, linkers, simulators, etc.) and software-hardware integration testing tools (emulators) that will result in the integrity of program and data.
O.DEV_DIS_ES	The Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that tools are only delivered and accessible to the parties authorized personnel. It must be ensured that confidential information on defined assets are only delivered to the parties authorized Personnel on a need to know basis.
O.SOFT_DLV	The Smart Card embedded software must be delivered from the Smart Card embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.INIT_ACS	Initialization Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).
O.SAMPLE_ACS	Samples used to run tests shall be accessible only by authorized personnel.

4.2.1.2 Objectives on the TOE delivery process (phases 4 to 7)

Security Objectives	Description
O.DLV_PROTECT	Procedures shall ensure protection of TOE material/information under delivery including the following objectives : • non-disclosure of any security relevant information, • identification of the element under delivery, • meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment), • physical protection to prevent external damage • secure storage and handling procedures (including rejected TOE's) • traceability of TOE during delivery including the following parameters: • origin and shipment details

Security Objectives	Description
	• reception, reception acknowledgement, • location material/information.
O.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.
O.DLV_RESP	Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

4.2.1.3 Objectives on delivery from phase 1 to phases 4, 5 and 6

Security Objectives	Description
O.DLV_DATA	The Application Data must be delivered from the Smart Card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.

4.2.1.4 Objectives on phases 4 to 6

Security Objectives	Description
O.TEST_OPERATE	Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

4.2.1.5 Objectives on phase 7

Security Objectives	Description
O.USE_DIAG	Secure communication protocols and procedures shall be used between the Smart Card and the terminal.

4.2.2 SECURITY OBJECTIVES OF [EEC/A1B]

There is no security objective for the environment in [EEC/A1B].

4.2.3 ADDITIONAL SECURITY OBJECTIVES

The use of secret keys, private keys and Certificates as described in [EEC/A1B] induces the following objectives.

Objective	Description
OE.Secret_Private_Keys	The Issuer must ensure that Secret & Private keys, when outside the TOE, are handled securely. The disclosure of these keys may give hackers access to the TOE. The Private Keys include the European private Key, the Countries' Private keys and the VU private keys. The Secret Keys include VOP TDES keys.
OE.Qualified certificates	The Issuer must ensure that all certificates used in the Tachograph system are handled properly inside a reliable PKI. This includes the revocation of a certificate when the corresponding key is not secure.

5 IT SECURITY REQUIREMENTS

5.1 TOE IT SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP/9911] and [EEC/A1B].
[ST/Infineon] deals with the security functional requirements of [PP/BSI-0002].

5.1.1 FAU: SECURITY AUDIT

5.1.1.1 FAU_SAA Security Audit Analysis

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [**audited events listed below**] known to indicate a potential security violation;
b) No other rules

Audited events:

- Cardholder authentication failure (5 consecutive unsuccessful PIN checks)
- Self test error
- Stored data integrity error
- Activity data input integrity error

5.1.2 FCO: COMMUNICATION

5.1.2.1 FCO_NRO Non-repudiation of origin

FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1	The TSF shall be able to generate evidence of origin for transmitted **[User data]** at the request of the **[recipient].**
FCO_NRO.1.2	The TSF shall be able to relate the **[Public key]** of the originator of the information, and the **[User data]** of the information to which the evidence applies.
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to **[recipient]** given **[validity of the certificate].**

5.1.3 FCS: CRYPTOGRAPHIC SUPPORT

5.1.3.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 / Session VOP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Triple DES key generation]** and specified cryptographic key sizes **[112 bits]** that meet the following **[VOP Session keys, cf. [OP2.0.1']]**
FCS_CKM.1.1 / Session A1B	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Triple DES key generation]** and specified cryptographic key sizes **[112 bits]** that meet the following **[A1B Session keys, cf. [EEC/A1B]]**
FCS_CKM.1.1 / Card private & public key	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA key generation]** and specified cryptographic key sizes **[1024 bits]** that meet the following **[No Standard]**

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 / Public Key	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **["Generate RSA key" command]** that meets the following **[None]**
FCS_CKM.2.1 / Certificate	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **["Read Binary" command]** that meets the following **[None]**

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 / Session VOP	The TSF shall perform **[Access to session keys]** in accordance with a specified cryptographic key access method **[Secure reading in Memory]** that meets the following **[None].**
FCS_CKM.3.1 / Session A1B	The TSF shall perform **[Access to session keys]** in accordance with a specified cryptographic key access method **[Secure reading in Memory]** that meets the following **[None].**
FCS_CKM.3.1 / Card private key	The TSF shall perform **[Access to signature keys]** in accordance with a specified cryptographic key access method **[Secure reading in Memory]** that meets the following **[None].**

Note: as the Card Private Key is a TSF Data, a new dependency from FCS_CKM.3.1 / Card private key to FDP_TDC.1 and FMT_MTD.1 has been added to the nominal dependency from FCS_CKM.3.1 / Card private key to FDP_ITC.1.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 / Session VOP	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.
FCS_CKM.4.1 / Session A1B	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.

Note:
There is no iteration for the Card private key. Disabling the signature function is performed by invalidating the Card certificate. So there is no need to delete the card private key.

5.1.3.2 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/ SIGN	The TSF shall perform **[Digital signature generation and verification]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[1024 bits]** that meet the following**: [[RSA-PKCS#1] -v1_5]**.
FCS_COP.1.1/ HASH	The TSF shall perform **[Hashing of data file]** in accordance with a specified cryptographic algorithm **[SHA-1]** and cryptographic key sizes **[not applicable]** that meet the following**: [SHA-1]**.
FCS_COP.1.1/ MAC	The TSF shall perform **[MAC computation]** in accordance with a specified cryptographic algorithm **[TDES-CBC]** and cryptographic key sizes **[112 bits]** that meet the following**: [FIPS 46-3]**.
FCS_COP.1.1/ ENC	The TSF shall perform **[Encryption and decryption]** in accordance with a specified cryptographic algorithm **[TDES-ECB]** and cryptographic key sizes **[112 bits]** that meet the following**: [FIPS 46-3]**.

5.1.4 FDP : USER DATA PROTECTION

5.1.4.1 FDP_ACC Access Control policy

FDP_ACC.2 Complete access control

FDP_ACC.2.1/ AC_SFP SFP	The TSF shall enforce the **[AC_SFP SFP]** on **[Read User data by Owner, Write Identification data by Issuer, Write Activity data by Owner Create File Structure by Issuer]** and all operations among subjects and objects covered by the SFP.

Note: If the date & time are inserted in the personalization phase, they are regarded as identification data and are subject to the same rules as identification data.

5.1.4.2 FDP_ACF access control function

FDP_ACF.1 Security attribute based access control

The only security attribute related to Access Control is **User_Group**. It is an attribute of the User. It can have the following values: Vehicle_Unit, Non_Vehicle_Unit.

FDP_ACF.1.1/ AC_SFP SFP	The TSF shall enforce the **[AC_SFP SFP]** to objects based on **[User_Group]**
FDP_ACF.1.2/ AC_SFP SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User data may be read from the TOE by any user, except cardholder identification data, which may be read from control cards by VEHICLE_UNIT only. Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle. Activity data may be written to the TOE by VEHICLE_UNIT only. No User may upgrade TOE's software Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.
FDP_ACF.1.3/ AC_SFP SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules **[none]**.

FDP_ACF.1.4/ AC_SFP SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **[none]**.

5.1.4.3 FDP_DAU :Data Authentication

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 [**activity data**].
FDP_ DAU.1.2/	The TSF shall provide [**any user]** with the ability to verify evidence of the validity of indicated information.

5.1.4.4 FDP_ETC :Export to outside TSF control

FDP_ETC.1: Export of user data without security attributes

FDP_ETC.1.1	The TSF shall enforce the **[AC_SFP SFP]** when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
Refinement: The certificate is exported without security attribute.

FDP_ETC.2: Export of user data with security attributes
Hierarchical to: No other component

FDP_ETC.2.1	The TSF shall enforce the **[AC_SFP SFP]** 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: **[none]**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
Refinement: The User data are exported with a security attribute, which the signature of the file.

5.1.4.5 FDP_ITC Import From outside TSF control

FDP_ITC.1: Import of user data without security attributes
Hierarchical to: No other component

FDP_ITC.1.1	The TSF shall enforce the **[AC_SFP SFP]** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[none]**.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation.

5.1.4.6 FDP_RIP Residual information protection

FDP_RIP.1: Subset residual information protection
Hierarchical to: No other component

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: **[Card Private Key].**

Dependencies: No dependency

5.1.4.7 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action
Hierarchical to: FDP_SDI.1

The following data persistently stored by TOE have the user data attribute “integrity checked stored data”

1. PIN
2. TDES master keys
3. Activity data
4. Card private key
5. Euro public key

FDP_SDI.2.1	The TSF shall monitor user data stored within the TSC for **[integrity error]** on all objects, based on the following attributes: **[integrity checked stored data]**.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall **[warn the entity connected].**

Dependencies: No dependency

5.1.5 FIA: IDENTIFICATION AND AUTHENTICATION

5.1.5.1 FIA_AFL Authentication failure

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 / Card interface VOP	The TSF shall detect when **[*3*]** unsuccessful authentication attempts occur related to **[authentication of a card interface device in personalization]**.
FIA_AFL.1.2 / Card interface VOP	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[** • **warn the entity connected** • **block the authentication mechanism** • **be able to indicate to subsequent users the reason of the blocking]**
FIA_AFL.1.1 / Card interface A1B	The TSF shall detect when **[*1*]** unsuccessful authentication attempts occur related to **[authentication of a card interface device in usage phase]**.
FIA_AFL.1.2 / Card interface A1B	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[** • **warn the entity connected** • **assume the user as NON_VEHICLE_UNIT]**
FIA_AFL.1.1 / PIN check	The TSF shall detect when **[*5*]** unsuccessful authentication attempts occur related to **[PIN check (workshop card)]**.
FIA_AFL.1.2 / PIN check	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[** • **warn the entity connected** • **block the PIN** • **be able to indicate to subsequent users the reason of the blocking]**

5.1.5.2 FIA_ATD User attribute definition

FIA_ATD.1User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users **[USER_ID, USER_GROUP]**

Refinement:

USER_GROUP is either VEHICLE_UNIT or NON_VEHICLE_UNIT
USER_ID, defined only for VEHICLE_UNIT is composed of the Vehicle Registration Number (VRN) and the registering Member State Code.

5.1.5.3 FIA_UAU User authentication

FIA_UAU.1 Timing of authentication

Driver & Workshop Cards

FIA_UAU.1.1 / Driver & Workshop Cards	The TSF shall allow **[Export user data with security attributes (card data download function)]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 / Driver & Workshop Cards	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Control & Company cards

FIA_UAU.1.1 / Control & Company Cards	The TSF shall allow **[Export user data without security attributes except cardholder identification data]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 / Control & Company Cards	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 **[prevent]** use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall **[prevent]** use of authentication data that has been copied from any user of the TSF.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to **[any authentication mechanisms].**

5.1.5.4 FIA_UID User Identification

FIA_UID.1Timing of identification

FIA_UID.1.1 / Driver & Workshop Cards	The TSF shall allow **[No operation]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 / Driver &	The TSF shall require each user to be successfully identified before allowing

Workshop Cards	any other TSF-mediated actions on behalf of that user.
FIA_UID.1.1 / Control & company Cards	The TSF shall allow **[No operation]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 / Control & company Cards	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note: In the Tachograph card, The identification is the insertion of the card into the card reader.

5.1.5.5 FIA_USB User-Subject Binding

FIA_USB.1 User-subject binding

FIA_USB.1.1	The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user

5.1.6 FMT: SECURITY MANAGEMENT

5.1.6.1 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1	The TSF shall restrict the ability to **[disable]** the functions **[PIN Creation, Import card private key, generate card private key]** to **[Issuer].**

5.1.6.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the **[AC_SFP SFP]** to restrict the ability to **[modify]** the security attributes **[User_Group]** to **[Owner]**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1/	The TSF shall enforce the **[AC_SFP SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/	The TSF shall allow the **[none]** to specify alternative initial values to override the default values when an object or information is created.

5.1.6.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1	The TSF shall restrict the ability to **[Import]** the **[Card private key]** to **[Issuer]**.

5.1.6.4 FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1	The TSF shall be able of performing the following security management functions: **[PIN Creation, Import card private key, Generate card private key, Read User data, Write Identification data, Write Activity data, Create File Structure]**.

5.1.6.5 FMT_SMR Security management roles

FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles **[Issuer]** and **[Owner]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.1.7 FPR: PRIVACY

5.1.7.1 FPR_UNO Unobservability

FPR_UNO.1 Unobservability

FPR_UNO.1.1	The TSF shall ensure that **[card holders and card issuers]** are unable to observe the operation **[file management, key management, software cryptographic computation, access control requirements]** on **[resources]** by **[terminals and card users]**.

5.1.8 FPT: PROTECTION OF THE TSF

5.1.8.1 FPT_FLS Failure secure

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[power cut-off or variations, unexpected reset].**

5.1.8.2 FPT_PHP TSF physical Protection

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1	The TSF shall resist **[clock frequency, voltage tampering and penetration of protection layer]** to the **[integrated circuit]** by responding automatically such that the TSP is not violated

5.1.8.3 FPT_SEP Domain Separation

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.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.8.4 FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1 Inter-TSF TSF basic data consistency

FPT_ TDC.1.1	The TSF shall provide the capability to consistently interpret **[Card private key]** when shared between the TSF and another trusted IT product.
FPT_ TDC.1.2	The TSF shall use **[Extract from message and decipher]** when interpreting the TSF data from another trusted IT product.

5.1.8.5 FPT_TST TSF self test

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self-tests **[during initial start-up, periodically 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.

5.1.9 FTP: TRUSTED PATH / CHANNEL

5.1.9.1 FTP_ITC Inter-TSF trusted channel

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 Vehicle Unit]** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for **[Storage of Activity Data]**

Refinement: The mentioned remote trusted IT product is the Vehicle Unit.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Assurance requirements is EAL 4 augmented by components:
ADO_IGS.2 : Generation log,
ADV_IMP.2 : Implementation of the TSF,
ALC_DVS.2 : Sufficiency of security measures,
ATE_DPT.2 : Testing low-level design,
AVA_MSU.3 : Analysis of insecure states,
AVA_VLA.4 : Highly resistant.

5.2.1 CONFIGURATION MANAGEMENT (ACM)

EAL4 augmented claimed level requires the following ACM class components:
ACM_AUT.1 Partial CM automation
ACM_CAP.4 Generation support and acceptance procedures
ACM_SCP.2 Problem tracking CM coverage
Refer to CC Part 3 for description.

5.2.2 DELIVERY AND OPERATION (ADO)

EAL4 augmented claimed level requires the following ADO class components:
ADO_DEL.2 Detection of modification
ADO_IGS.2 generation log
Refer to CC Part 3 for description.

5.2.3 DEVELOPMENT (ADV)

EAL4 augmented claimed level requires the following ADV class components:
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
ADV_SPM.1 Informal TOE security policy model
Refer to CC Part 3 for description.

5.2.4 GUIDANCE DOCUMENTS (AGD)

EAL4 augmented claimed level requires the following AGD class components:
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
Refer to CC Part 3 for description.

5.2.5 LIFE CYCLE SUPPORT (ALC)

EAL4 augmented claimed level requires the following ALC class components:
ALC_DVS.2 Sufficiency of security measures
ALC_LCD.1 Developer defined life-cycle model
ALC_TAT.1 Well-defined development tools
Refer to CC Part 3 for description.

5.2.6 TESTS (ATE)

EAL4 augmented claimed level requires the following ATE class components:
ATE_COV.2 Analysis of coverage
ATE_DPT.2 Testing low-level design
ATE_FUN.1 Functional testing

ATE_IND.2 Independent testing- sample
Refer to CC Part 3 for description.

5.2.7 VULNERABILITY ASSESSMENT (AVA)

EAL4 augmented claimed level requires the following AVA class components:
AVA_MSU.3 Analysis and testing of insecure states
AVA_SOF.1 Strength of TOE security function evaluation
AVA_VLA.4 Highly resistant
Refer to CC Part 3 for description.

6 TOE SUMMARY SPECIFICATION

6.1 STATEMENT OF TOE SECURITY FUNCTIONS

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirements.

6.1.1 BASIC SECURITY FUNCTIONS

SF.TEST Self test
When starting a work session, the TSF tests the RAM, the IC and its environment. When required, the TSF tests the integrity of EEPROM and random number generator.

SF.EXCEPTION Error Messages and exceptions
The TOE reports the errors on Message format, Integrity, range of environment conditions, Life cycle status.
Upon detection of a fault that could lead to a potential security violation, the card enters a secure Fail State. In this state, the card is mute.

SF.ERASE Residual information protection
The TOE erases its working memory when starting a working session and before allocation/deallocation of sensitive data.
The TOE destroys the cryptographic session keys.

SF.INTEGRITY Data Integrity
The TOE checks the integrity of the cryptographic keys, the authentication data, data contained in the File System.

SF.HIDE Data and operation hiding
The TOE hides sensitive data transfers and operations from outside observations.
The TOE is protected against SPA, DPA, DFA & timing attacks

SF.CARD_MGR Card manager
This function controls the execution of the card internal process corresponding to management command messages sent by the user to the card. The messages that it handles are defined as specified in ISO 7816.
This SF

- analyses the format of the command and the consistency of the instruction code and the P1/P2/P3 parameters
- Checks that the command sequence is respected and that the command is allowed in the current TOE life phase.
- Executes the command.
- Controls the modification of the TOE life cycle phase.

6.1.2 CRYPTOGRAPHIC RELATED FUNCTIONS

SF.KEY_GEN Key generation and distribution
The TOE can generate the Card private/public key pair, RSA 1024, according to the standard RSA PKCS#1_1.5, in personalization phase. The public key is then exported to enable the generation of the certificate.
In Personalization phase, the TOE generates Session keys, triple DES with 2 keys, according to the standard VOP. The generation uses triple DES with 2 keys.
In usage phase, The TOE generates Session keys, triple DES with 2 keys, according to the rules defined in [EEC/A1B].

SF.SIG Signature creation and verification
The TOE signs a hash of data, which is the result of a hash of file performed in the card or imported into the card.
The TOE can verify the signature of a hash of data imported into the card.
The TOE uses an RSA PKCS#1_1.5 signature scheme with a 1024 bit modulus.

SF.ENC TDES encryption and decryption
The TOE encrypts messages to be exported out of the card.
The TOE decrypts messages imported into the card.
The TOE uses Triple DES with 2 keys, in ECB mode.

SF.HASH Message hashing
The TOE generates a hash of a file stored in the card.
Hashing is done using SHA_1 algorithm.

SF.MAC MAC generation and verification
The TOE generates the MAC of exported data.
The TOE verifies the MAC of imported data.
The MAC computation uses Triple DES with 2 keys, in CBC mode.

SF.TRUSTED Trusted Path
This function establishes a secure channel, using a mutual authentication.
In Personalization phase, the secure channel is VOP (cf [OP.2.0.1']).
In Usage phase, the secure channel is A1B (cf [EEC/A1B] Appendix 11).
In VOP, a ratification counter limits the number of authentication attempts. The counter is decremented each time the authentication fails. The authentication mechanism is blocked and cannot be used any longer if the counter reaches zero.
When the secure channel is established, the messages may be MACed and Encrypted, depending on the function performed. The imported keys are encrypted.

SF.PIN PIN management
This SF controls all the operations relative to the PIN management, including the Cardholder authentication:
- PIN creation: the PIN is stored and is associated to a maximum presentation number.
- PIN verification: the PIN can be accessed only if its format and integrity are correct. If the PIN is blocked, then it cannot be used anymore.

The strength of this function is SOF_High.

6.1.3 SECURITY MANAGEMENT FUNCTIONS

SF.ACC Access Authorisation
The function controls the access conditions of a file.
This SF puts the access conditions on a file when it is created. It checks that the AC are met before accessing a file in the card.

This SF maintains the roles of the user.

This SF also maintains the security attributes USER_GROUP and USER_ID.

SF.DOMAIN Domain Separation
This SF maintains the Security Domains.
It ensures that the Tachograph application has its own security environment, separate from the security environment of the OS.
This SF also ensures that the right security environment is used when dealing with PIN and cryptographic keys.

6.1.4 PHYSICAL MONITORING

SF.DRIVER Chip driver
This function ensures the management of the chip security features. It starts the state analysis, audits events, performs shield actions according to violation severity and control random clock generation.

SF.ROLLBACK Safe fail state recovery
The function ensures that the TOE returns to its previous secure state when following events occurs: Power cut-off or variations, unexpected reset.

7 PP CLAIMS

The PP [PP/BSI-0002] is claimed.
The PP [PP/9911] is included except for the parts regarding the IC.

END OF SECURITY TARGET