PHAESTOS3 BIS
Public Security Target

CONTENT

FIGURES

TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

ST Title:	PHAESTOS3 BIS Security Target
ST Reference:	D1267149
Version:	1.0p
Origin:	GEMALTO
ITSEF	SERMA
Certification scheme:	French (ANSSI)

1.2 TOE REFERENCE

Product: MultiApp ID Tachograph 1.3

TOE name: Tacho V1.3 applet

TOE version: T1018062

TOE documentation: Guidance [AGD]

TOE hardware part: P5CC081 security controller

Developer: Gemalto

1.3 TOE OVERVIEW

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

The **MultiApp** platform(including hardware and the operating system).

The Tachograph application TACHO V1.3

All ROMed applets are deactivated; **TACHO V1.3** application is installed in EEPROM.

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 plastic card is outside the scope of this Security Target.

The Tachograph V13 MultiApp ID V2.1 product is a “contact-only” smartcard compliant with [ISO7816], and supporting T=0 and T=1 communication protocols.

TOE Components	Identification	Constructor
IC	P5CC081 Version V1A	NXP
Platform	MultiApp version 2.1	Gemalto
Tachograph application	TACHO version 1.3	Gemalto
ROMed out-of-TOE Components	Identification	Constructor
Deactivated non-instanciable applications	IAS XL IAS Classic V3 MPCOS v4.1 MOCA Server 1.0 MOCA Client 1.0	Gemalto Gemalto Gemalto Gemalto Gemalto
EEPROmed out-of-TOE Component	Identification	Constructor
Instanciable application	N/A	
Non-instanciable application	N/A	

Table 1. MultiApp Tacho Card components

The TOE defined in this Security Target is the Tachograph application provided by the TACHO V1.3 application, and is supported by the MultiApp Java Card platform.
The other applications are locked and cannot be instantiated or personalized. They are not in the TOE scope and therefore not part of the evaluation.
The TOE will be designed and produced in a secure environment and used by each user in a hostile environment.

The functional requirements for a Tachograph card are specified in [EEC/A1B] body text and Appendix 2.

The product provides the following services:

Storing of Activity data(events, control activities data, faults data)

Storing of card identification and card holder identification data

Downloading of User Data

Personalization of the product

The product is compliant with:
Java Card 2.2.2

Global Platform 2.1.1

The Tachograph security functions take advantage of the platform security functions:

Hardware Tamper Resistance is managed by the chip security layer that meets the Security IC Platform Protection Profile [PP/BSI-0035].

Secure operation of the MultiApp platform managed inside platform component.

1.3.1 TOE type

The TOE is the micro-module made of the Integrated Circuit (IC) and its embedded software (ES). The ES encompasses MultiApp and the Tachograph Application. 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.

1.3.2 TOE boundaries and out of TOE

The TOE is composed of the IC, the software platform and the Tachograph application:

P5CC081 IC which has been certified separately according to [ST-IC] claiming [PP/BSI-0035]
MultiApp platform

TACHO V1.3 application

The **TSFs** are composed of:

1. The Tachograph related functions of the **TACHO V1.3** application: Authentication, Verify PIN, Verify Certificate, Select/read/Update files, Manage Security Environment, Hash file generation, Generation/Verification Signature,
2. Personalization commands. (Other functions are out of the TOE)
3. **The P5CC081 IC** that supports the MultiApp platform.

Figure 1 represents the product. The TOE is bordered with bold and un-continuous line. The architecture of MultiApp inside the TOE is presented in platform description chapter below.

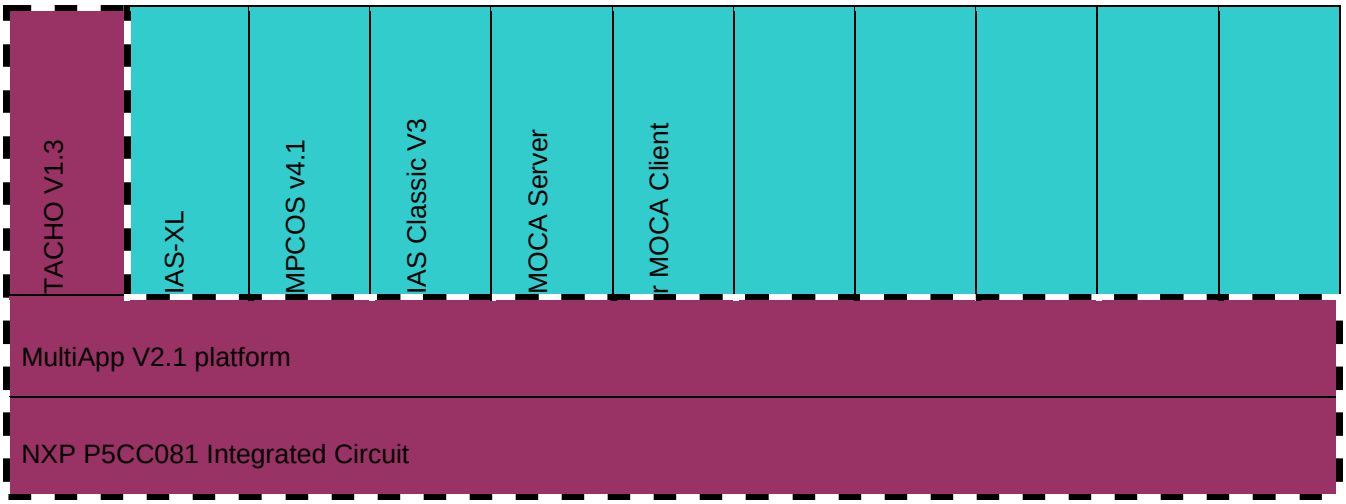


Figure 1 - MultiApp TACHO V13 Card

Beside the TOE, the product also contains the following Java Card applications:

These ROMed applications are all **deactivated (entry point deactivated)**

IAS XL: digital signature application compatible with IAS ECC v1.01 specification defined by Gixel (French smartcard industry association)

IAS Classic V3: digital signature application with RSA up to 2048 and SHA256

MPCOS: secure data storage 3DES based and PIN protection

MOCA server: offers a match on card services to applications

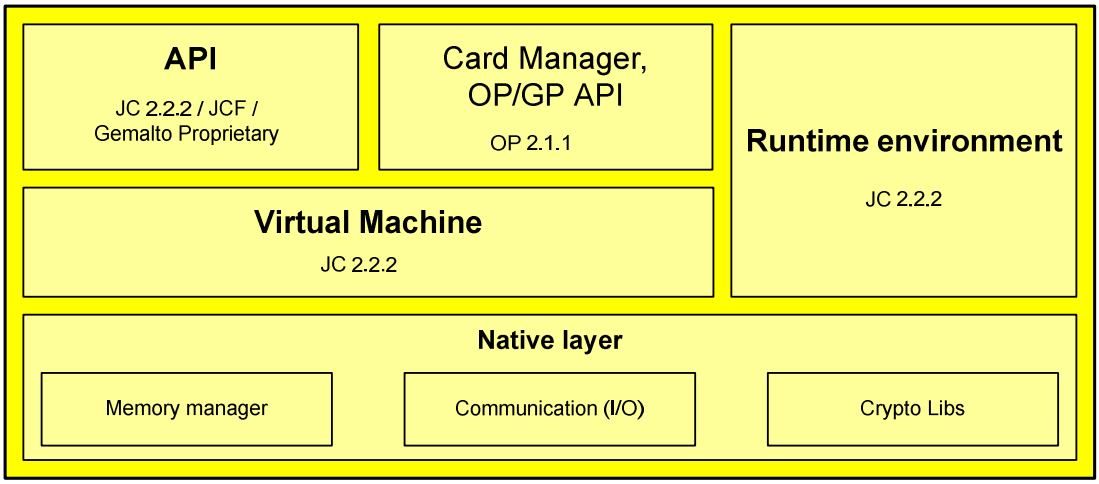
MOCA client: match on card application using MOCA server

1.4 TOE DESCRIPTION

1.4.1 Platform description

MultiApp ID V2.1 platform is a Java Open Platform that complies with two major industry standards:

- Sun's Java Card 2.2.2, which consists of the Java Card 2.2.2 Virtual Machine [JVCM222], Java Card 2.2.2 Runtime Environment [JCRE222]and the Java Card 2.2.2 Application Programming Interface[JCAPI222].
- The GlobalPlatform Card Specification version 2.1.1[GP211]
-



-

Figure 2: MultiApp ID V2.1 javacard platform architecture

-

As described in figure 3, the MultiApp ID V2.1 platform contains the following components :

The *Native Layer* provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the dedicated IC. The cryptographic features implemented in the native layer, and which support the Tacho V13 functionality, are:

Triple-DES

RSA 1024

OBKG (RSA key pair)

SHA1

Pseudo-Random Number Generation (PRNG)

The *Java Card Runtime Environment*,

It conforms to [JCRE222] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).

Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management, SCP01 and SCP02 ;

The *Java Card Virtual Machine*,
It conforms to [JCVM222] and provides the secure interpretation of bytecodes.

The *API*
It includes the standard Java Card API [JCAPI222] and Gemalto proprietary API.

The *Open Platform Card Manager*
It conforms to [GP211] and provides card, key and applet management functions (contents and life-cycle) and security control.

The MultiApp ID V2.1 platform provides the following services:

Remark: Points 2, 3 and 4 are services available in development environment phase and no available in operational environment (not part of the evaluation scope).

1. Initialization of the Card Manager and management of the card life cycle,
2. Secure loading and installation of the application under Card Manager control,
3. Extradition services to allow several applications to share a dedicated security domain,
4. Deletion of applications under Card Manager control,
5. Secure operation of the applications through the API
6. Management and control of the communication between the card and the CAD
7. Card basic security services as follows:
    a. Checking environmental operating conditions using information provided by the IC,
    b. Checking life cycle consistency,
    c. Ensuring the security of the PIN and cryptographic keys objects,
    d. Generating random number,
    e. Handling secure data object and backup mechanisms,
    f. Managing memory content
    g. Ensuring Java Card firewall mechanism

1.4.2 TACHO V13 Application description

A Tachograph card is a smart card 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), only vehicle units may write user data to the card.

The functional requirements for a Tachograph card are specified in [5] and [7].

"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 [5]

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

1.4.3 TOE life-cycle

The Smart card product life cycle, as defined in [PP/BSI-0035], 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.

Table 2. Smart Card Product Life Cycle

The Tachograph Card life as described in [PP/BSI0035] can be matched as shown in Figure 3 – Tachograph Card Life Cycle “Micro-module delivery”.

OS design, **application design and Tacho V13 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** correspond to life phase 6 “Smart card personalisation”.

Storing of Activity data and **Downloading of user data** correspond to life phase 7 “Smart card usage”.

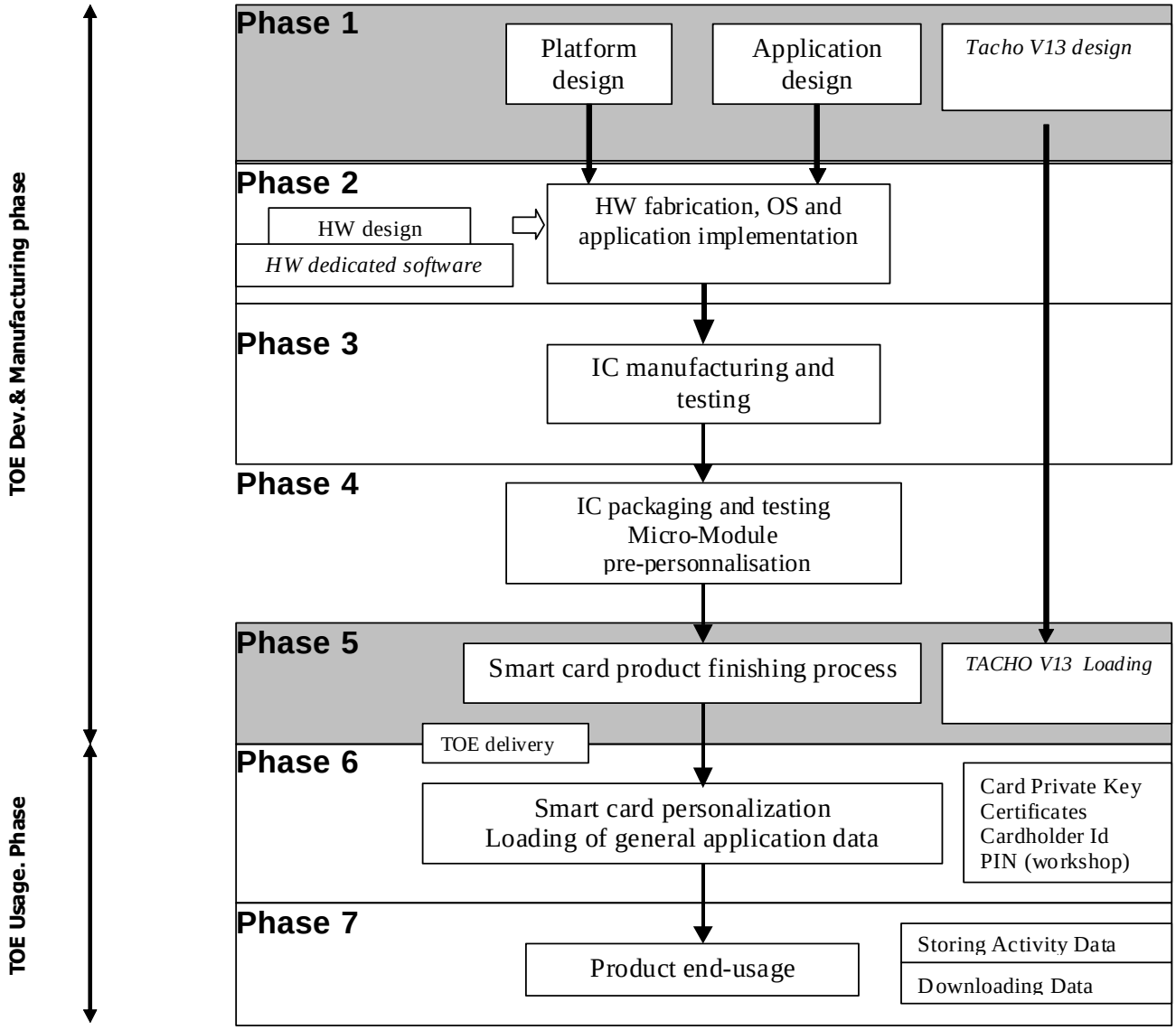


Figure 3 – Tachograph Card Life Cycle "Micro-module delivery"

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 6 and 7 but developed during phases 1 to 5.

The limits of the evaluation process correspond to phases 1 to 5 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 5 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 TOE "Security Assurance Requirements".

1.4.4 TOE Environment

The TOE environment is defined as follow:

For TOE development phase:

Development environment corresponding to the software developer environment (phase1), and the hardware fabrication environment (phase 2);

Production environment corresponding to the generation of the masked Integration Circuit (phase 3), the manufacturing of the card (phase 4), the initialization of the JavaCard (phase 5) and the installation of the applet (phase 5), the test operations, and initialization of the JavaCard.

For TOE operational phase

Personalization environment corresponding to the card personalization: loading of TOE application data (phase 6).

User environment corresponding to card usage: the card stores and downloads data in files (phase 7). End of life environment which is the physical destruction of the card. (End of the phase 7).

1.4.4.1 TOE Development & Production Environment

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

Phase 1	Secure OS Design (MultiApp)	Gemalto Meudon site (all development) Gemalto La Ciotat site (MKS servers) Gemalto Gémenos site (Component team
	Tacho V1.3 design	Gemalto Singapore site (dev team) Gemalto La Ciotat site (MKS servers)
	Pre-personalization design	Gemalto Singapore
Phase 2	IC design Hardware fabrication	NXP development site(s) mentioned in [CR-IC]
Phase 3	IC manufacturing & testing	NXP development site(s) mentioned in [CR-IC]
Phase 4	IC packaging & testing Module assembling Module packaging(embedding)	Gemalto Gemenos Gemalto Gemenos/Singapore
Phase 5	Pre-personalization	Gemalto Gemenos/Singapore

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 authorized 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 unauthorized access) to make the conception, the design, the implementation and the 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, 4and 5, 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 Initialization is performed in NXP development site(s) mentioned in [CR-IC] phase 3; in Gemalto sites for phase 4 and phase 5.

In the initialization environment of the TOE, module pre-personalization takes place.

During module pre-personalization the applet is loaded. Then the applet is instantiated. At the end of this phase, the loader of executable files is blocked.

Initialization requires a secure environment, which guarantees the integrity and confidentiality of operations

1.4.4.2 Card manufacturing Environment

The Card manufacturing can take place outside Gemalto. The micro-module is inserted in a plastic card. In this environment, the personalization 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.

1.4.4.3 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.

If the Signature Key is disclosed, the PKI enters it in the revocation list and the whole PKI knows that this key cannot be trusted anymore.

1.4.4.4 End of life Environment.

The end of life is the physical destruction of the card.

1.4.5 The actors and roles

The actors can be divided in:

Developers

The IC designer and Dedicated Software (DS) developer designs the chip and its DS. For this TOE, it is NXP.

The Embedded Software developer designs the OS according to IC/DS specifications, the Tacho V1.3 application. For this TOE, it is GEMALTO.

Manufacturers

The IC manufacturer -or founder- designs the photomask, manufactures the IC with its DS and hardmask from the Product Developer. For this TOE, the founder is NXP.

The IC die bonding manufacturer is responsible for the die bonding the ICs provided by the founder. For this TOE, the IC die bonding manufacturer is GEMALTO.

The Smart Card product manufacturer (or Card manufacturer) is responsible to obtain a pre-personalized card from a packaged IC. In the phase 5, the card manufacturer is also responsible for loading additional code belonging to the Developer and Manufacturer of the Card (applet). For this TOE, the Smart Card product manufacturer is GEMALTO.

At the end of this phase, no more applets may be loaded on the card (post-issuance is not allowed). The card is issued in OP_SECURED state.

Personnalisater

The Smart Card Personalizer personalizes the card (TOE Life cycle Phase 6) by loading the cardholder data as well as cryptographic keys and PIN. For this TOE, the personalizer is the Card Issuer/Administrator.

At the end of this phase, the card is in OP_SECURED state.

Card Issuer, Administrator

The Card issuer creates the user's PIN and imports the Card private key into the TOE or generates this key in the TOE..

End-user,User

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

The roles (administration and usage) are defined in the following tables.

Phase	Administrator	Environment
6 and 7	Card Issuer	Personalization and Usage Environment

Phase	User	Environment
7	End-User	Usage Environment

During the delivery between phases the responsibility is transferred from the current phase administrator to the next phase administrator.

1.4.6 TOE intended usage

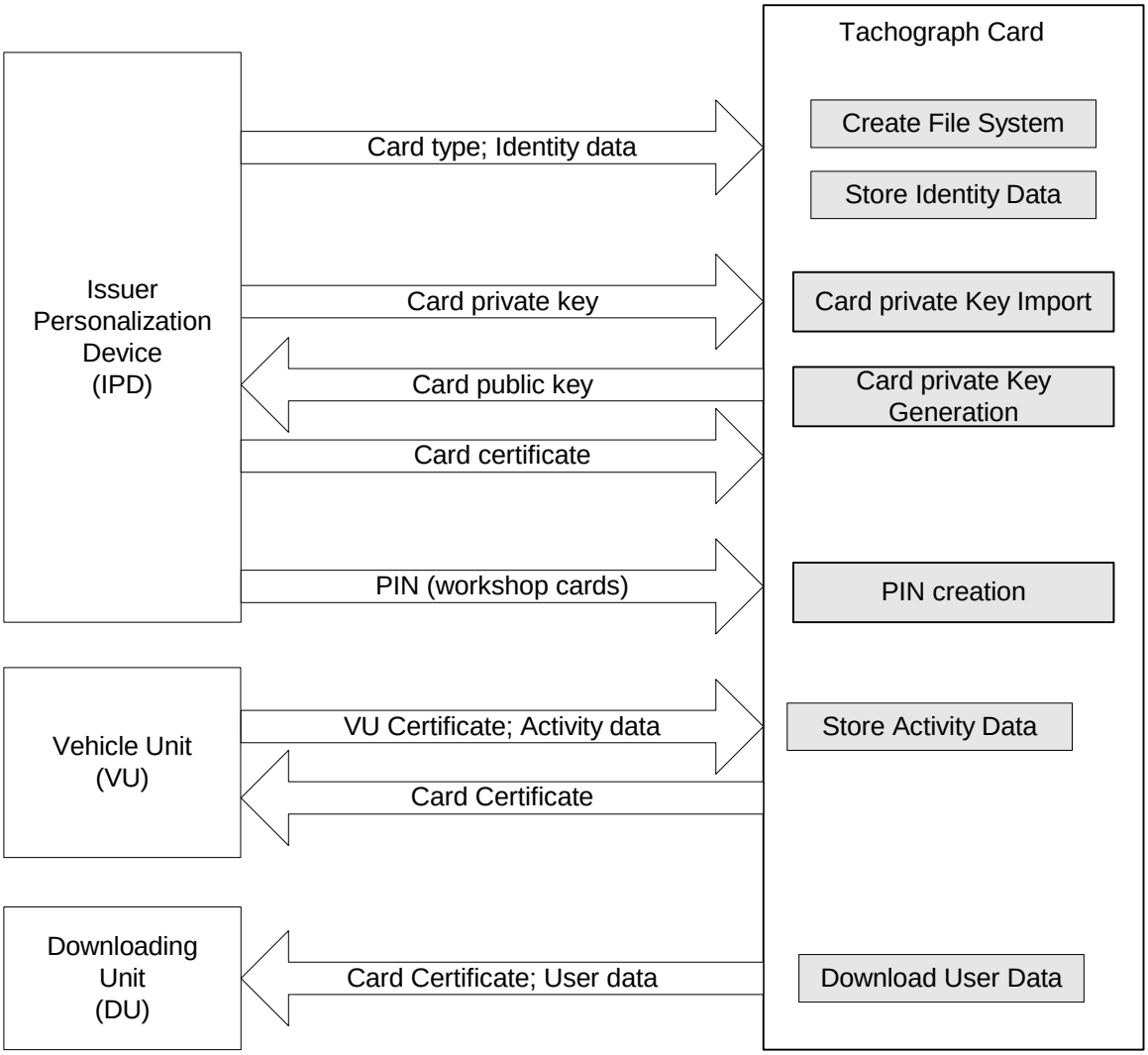


Figure 4: TOE Usage

Personalization ,

The IPD authenticates itself to the TOE. (mutual authentication)
The IPD sends the following data to the TOE:

- Cardholder identification
- Card private key (if it is loaded)
- European public key; Member state Certificates: Card certificate
- PIN (workshop cards)

Storing of Activity Data

The VU authenticates itself to the TOE. (mutual authentication)
The VU sends Activity Data to the card.
The TOE stores these data in the appropriate files.

Downloading of User Data

The VU or another DU authenticates itself to the TOE. (mutual authentication)
The TOE retrieves User Data from the requested files.
The TOE sends these data to the DU.

1.5 REFERENCES, GLOSSARY AND ABBREVIATIONS

1.5.1 External references

Reference	Title - Reference
[CC]	Common Criteria references
[CCPART1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001, version 3.1 Revision 3, July 2009 (conform to ISO 15408).
[CCPART2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components CCMB-2009-07-002, version 3.1 Revision 3, July 2009 (conform to ISO 15408).
[CCPART3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCMB-2009-07-003, version 3.1 Revision 3, July 2009 (conform to ISO 5408).
[CEM]	Common Methodology for Information Technology Security Evaluation CCMB-2009-07-004, version 3.1 Revision 3, July 2009.
[CCDB]	Common Criteria mandatory technical document – Composite product evaluation for smart cards and similar devices, CCDB-2007-09-001, Version 1.0 Revision 1, September 2007.
[ISO]	ISO references
[ISO 7816]	ISO 7816-X documents
[PP]	Protection Profiles
[PP/BSI-0070]	Digital Tachograph –Smart Card (Tachograph Card) Protection Profil BSI-CC-PP-0070 Version 1.02, 15th of November 2011
[PP/BSI-0035]	Security IC Platform Protection Profile - BSI-PP-0035-2007; Version 1.0, 15 June 2007
[TACHO]	Tachograph references
[5]	Annex I(B) of Commission Regulation (EEC) No. 1360/2002 'Requirements for Construction, Testing, Installation and Inspection', 05.08.2002 and last amended by CR(EC) No. 432/2004 and corrigendum dated as of 13.03.2004(OJ L 71)
[6]	Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport, Official Journal of the European Communities L 71-86, 13.03.
[7]	Appendix 2 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5]– Tachograph Cards Specification
[8]	Appendix 10 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] - Generic Security Targets
[9]	Appendix 11 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5]– Common Security Mechanisms
[NXP]	Protection Profiles

[ST-IC]	NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A - Security Target Lite — Rev. 1.3 — 21 September 2009.
[CR-IC]	Certification Report for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A, each with IC dedicated software BSI-DSZ-CC-0555-2009, November 10th 2009
[MA-IC]	Assurance Continuity Maintenance Report BSI-DSZ-CC-0555-2009-MA-01, December 30th 2010 Reassessment of BSI-DSZ-CC-0555-2009, November,3 2011
[JCS]	Javacard references
[JCVM222]	Java Card ™ 2.2.2 Virtual Machine Specification - 15 March 2006 Sun Microsystems
[JCRE222]	Java Card ™ 2.2.2 Runtime Environment Specification, 15 March 2006, Sun Microsystems, Inc.
[JCAPI222]	Java Card ™ 2.2.2 Application Programming Interface, March 2006 Sun Microsystems.
[GP]	Global Platform references
[GP211]	Global Platform - Card specification v2.1.1 - 2.1.1 - March 2003
[MISC]	Miscellaneous
[RSA-PKCS#1]	PKCS#1 v2.1 RSA Cryptography Standard
[SHA-1]	FIPS PUB 180-1 Secure Hash Standard
[SP800-67]	SP800-67 Triple Data Encryption Algorithm (TDEA)
[SP800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation

1.5.2 Internal references

Reference	Title - Reference
[ADV]	**PHAESTOS3 ADV Documentation**
[FSP_PHAESTOS3]	**PHAESTOS3 Bis Functional Specification** Ref: D1267713 (ADV_FSP_D1267713)
[ARC_PHAESTOS3]	**PHAESTOS3 Security architecture description** Ref: D1190955 (ADV_ARC_D1190955)
[TDS_PHAESTOS3]	**PHAESTOS3 TOE design** Ref: D1190956 (ADV_TDS_D1190956)
[IMP_PHAESTOS3]	**PHAESTOS3 Implementation representation** Ref: D1190957 (ADV_IMP_D1190957)
[AGD]	**PHAESTOS3 Guidance Documentation**
[OPE_PHAESTOS3]	**PHAESTOS3 Operational user Guidance** Ref: D1190958 (AGD_OPE_D1190958)
[PRE_PHAESTOS3]	**PHAESTOS3 Preparative procedures** Ref: D1190960 (AGD_PRE_D1190960)
[ALC]	**PHAESTOS3 ALC Documentation**

Reference	Title - Reference
[CMC_PHAESTOS3]	**PHAESTOS3 Production support, acceptance procedures and automation** Ref: D1190961 (CMC_D1190961)
[CMS_PHAESTOS3]	**PHAESTOS3 Problem tracking CM coverage** Ref: D1190962 (CMS_D1190962)
[DEL_PHAESTOS3]	**PHAESTOS3 Delivery procedures** Ref: D1190963 (DEL_D1190963)
[DVS_PHAESTOS3]	**PHAESTOS3 Identification of security measures** Ref: D1190964 (DVS_ D1190964)
[LCD_PHAESTOS3]	**PHAESTOS3 Developer defined life-cycle model** Ref: D1190965 (LCD D1190965)
[TAT_PHAESTOS3]	**PHAESTOS3 Documentation of development tools** Ref: D1190966 (TAT_ D1190966)
[ATE]	**PHAESTOS3 ATE Documentation**
[COV_PHAESTOS3]	**PHAESTOS3 Analysis of test coverage** Ref: D1190967 (ATE_COV_ D1190967)
[DPT_ PHAESTOS3]	**PHAESTOS3 Bis Testing: security enforcing modules** Ref: D1267714 (ATE_DPT_ D1267714)
[FUN_PHAESTOS3]	**PHAESTOS3 Test Documentation** Ref: D1190969 (ATE_FUN_ D1190969)

1.5.3 Glossary

Activity data	Activity data include cardholder activities data, events and faults data and control activity data.
Card identification data	User data related to card identification
Cardholder activities data	User data related to the activities carried by the cardholder:
Cardholder identification data	User data related to cardholder
Control activity data	User data related to law enforcement controls
Digital tachograph	Recording equipment
Events and faults data	User data related to events or faults
Identification data	Identification data include card identification data and cardholder identification data.
Sensitive data	Data stored by the tachograph card that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data

Security data	The specific data needed to support security enforcing functions (e.g. crypto keys)
System	Equipment, people or organisations involved in any way with the recording equipment
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (when not used in the expression “user data”).
User data	Sensitive data stored in the tachograph card, other than security data. User data include identification data and activity data.

1.5.4 Abbreviations

CC	Common Criteria version 3.1
CSP	Certification-Service Provider
EAL	Evaluation Assurance Level
ES	Embedded Software
HI	Human Interface
HW	Hardware
IC	Integrated Circuit
ICC	Integrated Circuit Card
IT	Information Technology
NVM	Non Volatile Memory
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
SF	Security function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security functions
TSFI	TSF Interface
TSP	TOE Security Policy
VIN	Vehicle Identification Number
VRN	Vehicle Registration Number
VU	Vehicle Unit

2 CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This Security Target is built with CC V.3.1 Revision 3

This ST is [CCPART2] extended with FPT_EMS TOE emanation.

This ST is [CCPART3] conformant.

Evaluation type

This is a composite evaluation, which relies on the P5CC081 chip certificate and evaluation results.

P5CC081 chip certificate:

Certification done under the BSI scheme
Certification reports [CR-IC] , [MA-IC]
Security Target [ST-IC] strictly conformant to IC Protection Profile [PP/0035]
Common criteria version: 3.1
Assurance level: EAL5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document "Composite product evaluation for smart cards and similar devices" [CCDB].

2.2 PP CLAIM, PACKAGE CLAIM

This ST claims strict conformance to the Protection Profile [PP-BSI-0070].

[ST-IC] refines the assets, threats, objectives and SFR of [PP/BSI-0035].

This TOE claims conformance to Package EAL4 augmented (+) with:

ALC_DVS.2: Sufficiency of security measures.

ATE_DPT.2: Testing Enforcing modules

AVA_VAN.5: Advanced methodical vulnerability analysis

2.3 CONFORMANCE RATIONALE

The ST security objectives and requirements are identical to those of the claimed PP [PP-BSI-0070].].

in the ST.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the TOE environment and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions.

3.1 ASSETS

Asset name	Description	Generic security property to be maintained by the TOE
Identification data (IDD)	Primary asset: card identification data, cardholder identification data (see Glossary for more details)	Integrity
Activity data (ACD)	Primary asset: cardholder activities data, events and faults data and control activity data (see Glossary for more details)	Integrity, Authenticity, for parts of the activity data also Confidentiality

Asset name	Description	Generic security property to be maintained by the TOE
Signature creation data (SCD)	Secondary asset: private key used to perform an electronic signature operation	Confidentiality, Integrity
Secret messaging keys (SMK)	Secondary asset: session keys (TDES) used to protect the Tachograph Card communication by means of secure messaging	Confidentiality, Integrity
Signature verification data (SVD)	Secondary asset: public keys certified by Certification Authorities, used to verify electronic signatures	Integrity, Authenticity
Verification authentication data (VAD)	Secondary asset: authentication data provided as input for authentication messaging attempt as authorised user (PIN)	Confidentiality (This security property is not maintained by the TOE but by the TOE environment)
Reference authentication data (RAD)	Secondary asset: data persistently stored by the TOE for verification of the authentication attempt as authorized user	Confidentiality, Integrity
Data to be signed (DTBS)	Secondary asset: the complete electronic data to be signed (including both user message and signature attributes)	Integrity, Authenticity
TOE File system incl. specific identification data	Secondary asset: file structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalization	Integrity

All primary assets represent User Data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF and TSF-data in the sense of the CC. The GST [8] defines “sensitive data” which include security data and user data as data stored by the Tachograph Card, which integrity, confidentiality and protection against unauthorized modification need to be enforced. User data include identification data and activity data (see Glossary for more details) and match User Data in the sense of the CC. Security data are defined as specific data needed to support security enforcement and match the TSF data in the sense of the CC.

3.2 SUBJECTS AND EXTERNAL ENTITIES

Role	Definition
Administrator	S.Administrator: the subject is usually active only during Initialization/Personalization (Phase 6) – listed here for the sake of completeness..
Vehicle Unit	S.VU: Vehicle Unit (with a UserID), which the Tachograph Card is connected to.
Other devices	S.Non-VU: Other device (without UserID) which the Tachograph Card is connected to.
Attacker	It is a human or process acting on his behalf being located outside the TOE. For example, a driver could be an attacker if he misuses the driver card. An attacker is a threat agent (a person with the aim to manipulate the user data or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the maintained assets. The attacker is assumed to possess an at most *high* attack potential.

3.3 THREATS

Threat name	Description
T.Identification_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. The threat agent for T.Identification_Data is Attacker.
T.Activity_Data	A successful modification of activity data stored in the TOE would be a threat to the security of the TOE. The threat agent for T.Activity_Data is Attacker.
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. The threat agent for T.Data_Exchange is Attacker
T.Personalisation_Data	A successful modification of personalization data (such as TOE file system, cryptographic keys, RAD) to be stored in the TOE or disclosure of cryptographic material during the personalization would be a threat to the security of the TOE. The threat addresses the execution of the TOE's personalization process and its security. The threat agent for T.Personalisation_Data is Attacker.

3.4 ASSUMPTIONS

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

Assumption Name	Description
A.Personalisation_Phase	All data structures and data on the card produced during the Personalization Phase, in particular during initialization and/or personalization are correct according to the Tachograph Card Specification [7] and are handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalization Service Provider controls all materials, equipment and information, which is used for initialization and/or personalization of authentic smart cards, in order to prevent counterfeit of the TOE.

3.5 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policy name	Description
P.EU_Specifications	All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents [5] to [9]. To ensure the interoperability between the components all Tachograph Card and Vehicle Unit requirements concerning handling, construction and functionality inclusive the specified cryptographic algorithms and key length have to be fulfilled.

3.6 COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

3.6.1 Statement of Compatibility – Threats part

The following table lists the relevant threats of the P5CC081 security target [ST-IC], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
T.Leak-Inherent	Inherent Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets. No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.	T.Data_Exchange T.Personalisation_Data
T.Phys-Probing	Physical Probing	An attacker may perform physical probing of the TOE in order (i) to disclose User Data (ii) to disclose/reconstruct the Security IC Embedded Software or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Data_Exchange T.Personalisation_Data
T.Malfunction	Malfunction due to Environmental Stress	An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks	T.Identification_Data T.Activity_Data T.Data_Exchange T.Personalisation_Data

		disclosing or manipulating the User Data or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions.	
T.Phys-Manipulation	Physical Manipulation	An attacker may physically modify the Security IC in order to (i) modify User Data (ii) modify the Security IC Embedded Software (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Identification_Data T.Activity_Data T.Personalisation_Data
T.Leak-Forced	Forced Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets even if the information leakage is not inherent but caused by the attacker.	T.Identification_Data T.Activity_Data T.Data_Exchange T.Personalisation_Data
T.Abuse-Func	Abuse of Functionality	An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate User Data (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the User Data or the Security IC Embedded Software.	T.Identification_Data T.Activity_Data T.Personalisation_Data
T.RND	Deficiency of Random Numbers	An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.	T.Identification_Data T.Activity_Data T.Data_Exchange T.Personalisation_Data

3.6.2 Statement of Compatibility – OSPs part

The following table lists the relevant OSPs of the P5CC081 security target [ST-IC], and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.

IC OSP label	IC OSP content	Link to the composite product
P.Process-TOE	Protection during TOE Development and Production: An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.	No contradiction with the present evaluation; the chip traceability information is used to identify the composite TOE.
P.Add-Components	Additional Specific Security Components: The TOE shall provide the following additional security functionality to the Security IC Embedded Software: Triple-DES encryption and decryption AES encryption and decryption Area based Memory Access Control Memory separation for different software parts (including IC Dedicated Software and Security IC Embedded Software) Special Function Register Access control	Cryptographic services: the hardware Triple-DES encryption and decryption services are used by the composite TOE. The hardware AES encryption and decryption services is not used by the composite TOE. The Memory Separation and Area Based Memory Access Control IC services are used by the composite TOE. Special Function Register Access Control IC service is not used by the composite TOE.

3.6.3 Statement of Compatibility – Assumptions part

The following table lists the relevant assumptions of the P5CC081 security target [ST-IC] and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

IC assumption label	IC assumption title	IC assumption content	IrPA	CfPA	SgPA	Link to the composite product
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer 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). This means that the Phases after TOE Delivery (refer to Sections 19H1.2.2 and 120H7.1) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 121H92 (page 12H30).		X	X	Fulfilled by the composite ALC_DVS.2 and ALC_DEL.1 SARs until the end of phase 5 (TOE delivery point). Covered by the assumption A.USE_PROD after the TOE delivery point.
.Plat-Appl	Usage of Hardware Platform	The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware		X		Fulfilled by the composite-SAR ADV_COMP.1 (cf [CCDB], Appendix 1.2, §72 and §73)

		application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC ,Embedded Software as documented in the certification report.				
A.Resp-Appl	Treatment of User Data	All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.		X		OT.Data_Access,OT.Card_Activity_Storage,OT.Card_Identification_Data, OT.Secure_Communications

A.Check-Init	Check of initialization data by the Security IC Embedded Software	The Security IC Embedded Software must provide a function to check initialization data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability.		X		Fulfilled through the transport key verification at the beginning of phases 4 and 5.
A.Key-Function	Usage of key-dependent functions	Key-dependent functions (if any) shall be implemented in the Security IC Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys when being executed are part of the Security IC Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.		X		OT.Secure_Communications

4 SECURITY OBJECTIVES

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

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

This section describes the security objectives for the TOE, which address the aspects of identified threats to be countered by the TOE independently of the TOE environment and organizational security policies to be met by the TOE independently of the TOE environment.

Security Objectives	Description
OT.Card_Identification_Data	The TOE must preserve card identification data and cardholder identification data stored during card personalization process as specified by the EU documents [5] to [9]
OT.Card_Activity_Storage	The TOE must preserve user data stored in the card by Vehicle Units as specified by the EU documents [5] to [9]
OT.Data_Access	The TOE must limit user data write access rights to authenticated Vehicle Units as specified by the EU documents [5] to [9]
OT.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 as specified by the EU documents [5] to [9]

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the TOE's operational environment address the security properties which have to be provided by the TOE environment independently of the TOE itself.

The TOE's operational environment has to implement security measures in accordance with the following security objectives:

Objective	Description
OE.Personalisation_Phase	All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation must be correct according to the Tachograph Card Specification [7] and must be handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider must control all materials, equipment and information, which is used for personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality..
OE.Tachograph_Components	All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents [5] to [9]. To ensure the interoperability between the components all Vehicle Unit requirements concerning handling, construction and functionality inclusive the specified cryptographic algorithms and key length have to be fulfilled.

4.3 SECURITY OBJECTIVES RATIONALE

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

	Security objectives of the TOE	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Card_Data_Access	OT.Secure_Communications	Security objectives of the TOE's operational environment	OE.Personalisation_Phase	OE.Tachograph_Composants
Threats								
T.Identification_Data		X						
T.Activity_Data			X	X				
T.Data_Exchange					X			
T.Personalisation_Data							X	
OSPs								
P.EU_Specifications		X	X	X	X			X
Assumptions								
A.Personalisation_Phase							X	

Table 3: Security Objective Rationale

T.Identification_Data is addressed by OT.Card_Identification_Data. The unalterable storage of personalised identification data of the TOE (cardholder identification data, card identification data) as defined in the security objective OT.Card_Identification_Data counters directly the threat T.Identification_Data.

T.Activity_Data is addressed by OT.Card_Activity_Storage and OT.Data_Access. The unalterable storage of Activity data as defined in the security objective OT.Card_Activity_Storage counters directly the threat T.Activity_Data. In addition, the security objective OT.Data_Access limits the user data write access to authenticated Vehicle Units so that the modification of activity data by regular card commands can be conducted only by authenticated card interface devices.

T.Data_Exchange is addressed by OT.Secure_Communications. The security objective OT.Secure_Communications provides the support for secure communication protocols and procedures between the TOE and card interface devices. This objective supports the securing of the data transfer between the TOE and card interface devices with the goal to prevent modifications during data import and export and counters directly the threat T.Data_Exchange.

T.Personalisation_Data is addressed by the security objective of the operational environment OE.Personalisation_Phase which requires correct and secure handling of the personalisation data regarding integrity and confidentiality. It prevents the modification and disclosure of the personalisation data as well as the disclosure of cryptographic material during the execution of the personalisation process.

The OSP **P.EU_Specifications** is covered by all objectives of the TOE and the objective for the environment OE.Tachograph_Components. The security objectives of the TOE OT.Card_Identification_Data, OT.Card_Activity_Storage, OT.Data_Access and OT.Secure_Communications require that the corresponding measures are implemented by the Tachograph Cards as specified by the EU documents. The objective for the environment OE.Tachograph_Components requires this for the Vehicle Unit.

The Assumption **A.Personalisation_Phase** is covered directly by the security objective of the operational environment OE.Personalisation_Phase. At this point, the focus of OE.Personalisation_Phase lies in the overall security of the personalisation environment and its technical and organisational security measures.

4.4 COMPOSITION TASKS – OBJECTIVES PART

4.4.1 Statement of compatibility – TOE objectives part

The following table lists the relevant TOE security objectives of the P5CC081 chip and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
O.Leak-Inherent	Protection against Inherent Information Leakage	The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC - by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and - by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines). This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access
O.Phys-Probing	Protection against Physical Probing	The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Security IC Embedded Software or against the disclosure of other critical information about the operation of the TOE. This includes protection against - measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or - measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access

		with a prior reverse-engineering to understand the design and its properties and functions.	
O.Malfunction	Protection against Malfunctions	The TOE must ensure its correct operation. The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.	OT.Card_Activity_Data OT.Data_Access
O.Phys-Manipulation	Protection against Physical Manipulation	The TOE must provide protection against manipulation of the TOE (including its software and Data), the Security IC Embedded Software and the User Data. This includes protection against - reverse-engineering (understanding the design and its properties and functions), - manipulation of the hardware and any data, as well as - controlled manipulation of memory contents (Application Data).	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access
O.Leak-Forced	Protection against Forced Information Leakage	The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker - by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or - by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”. If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access
O.Abuse-Func	Protection against Abuse of Functionality	The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical User Data, (ii) manipulate critical User Data of the Security IC Embedded Software, (iii) manipulate Soft-coded Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access
O.Identification	TOE Identification	The TOE must provide means to store Initialization Data and Pre-personalisation Data in its non-volatile memory. The Initialization Data (or parts of them) are used for TOE identification.	No direct link to the composite-product TOE objectives, however chip traceability information stored

			in NVM is used by the TOE to answer identification CC assurance requirements.
O.RND	Random Numbers	The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.	No direct link to the composite-product TOE objectives; This objective is ensure by the platform MultiApp ID V2.1
O.HW_DES3	Triple DES Functionality	The TOE shall provide the cryptographic functionality to calculate a Triple DES encryption and decryption to the Security IC Embedded Software. The TOE supports directly the calculation of Triple DES with up to three keys	No direct link to the composite-product TOE objectives. This objective is ensure by the platform MultiApp ID V2.1
O.HW_AES	AES Functionality	The TOE shall provide the cryptographic functionality to calculate an AES encryption and decryption to the Security IC Embedded Software. The TOE supports directly the calculation of AES with three different key lengths.	Not used by the composite TOE
O.MF_FW	MIFARE Firewall	The TOE shall provide separation between the “MIFARE Operating System” as part of the IC Dedicated Support Software and the Security IC Embedded Software. The separation shall comprise software execution and data access.	Not used by the composite TOE
O.MEM_ACCESS	Area based Memory Access Control	Access by processor instructions to memory areas is controlled by the TOE. The TOE decides based on the CPU mode (Boot Mode, Test Mode, MIFARE Mode, System Mode or User Mode) and the configuration of the Memory Management Unit if the requested type of access to the memory area addressed by the operands in the instruction is allowed;	OT.Card_Activity_Data OT.Card_Identification_Data OT.Data_Access
O.SFR_ACCESS	Special Function Register Access Control	The TOE shall provide access control to the Special Function Registers depending on the purpose of the Special Function Register or based on permissions associated to the memory area from which the CPU is currently executing code. The access control is used to restrict access to hardware components of the TOE; The possibility to define access permissions to specialized hardware components of the TOE shall be restricted to code running in System Mode.	Not used by the composite TOE.

4.4.2 Statement of compatibility – TOE ENV objectives part

The following table lists the relevant ENV security objectives related to the P5CC081 chip, and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

IC ENV security objective label	IC ENV security objective title	IC ENV security objective content	Link to the composite-product
OE.Plat-Appl	Usage of Hardware Platform	To ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: – (i) hardware data sheet for the TOE, – (ii) data sheet of the IC Dedicated Software of the TOE, – (iii) TOE application notes, other guidance documents, and – (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.	Fulfilled by ADV_COMP.1 (cf [CCDB], Appendix 1.2, §72 and §73)
OE.Resp-Appl	Treatment of User Data	Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant User Data to unauthorized users or processes when communicating with a terminal.	Covered by TOE Security Objectives: OT.Card_Activity_Data ,OT.Card_Identification_Data ,OT.Data_Access, OT.Secure_Communications,
OE.Process-Sec-IC	Protection during composite product manufacturing	Security procedures shall be used after TOE Delivery up to delivery to the end-consumer 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).	Fulfilled by ALC.DVS.2 and ALC_DEL.1 during phases 4 and 5. After phase 5, covered by O.USE_DIAG,; OT.Secure_Communications OE.Personalisation_Phase

		This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately.	
OE.Check-init	Check of initialization data by the Security IC Embedded Software	To ensure the receipt of the correct TOE, the Security IC Embedded Software shall check a sufficient part of the pre-personalization data. This shall include at least the FabKey Data that is agreed between the customer and the TOE Manufacturer.	Fulfilled through the transport key verification at the beginning of phases 4 and 5, as stated in ALC_DEL.1

5 EXTENDED COMPONENTS DEFINITION

5.1 FPT_EMS (TOE EMANATION)

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation.

The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE.

Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which ere not directly addressed by any other component of CC part 2.

FPT_EMS TOE Emanation

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS.1 TOE Emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be .

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: no dependencies

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6 SECURITY REQUIREMENTS

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

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP/BSI-0070]

[ST-IC] deals with the security functional requirements of [PP/BSI-0035].

6.1.1Security Function Policy

The SFP AC_SFP is only relevant for the end-usage phase of the Tachograph Card, i.e. after the personalisation of the card has been completed.

Subjects:

·S.VU (in the sense of the Tachograph Card specification)

·S.Non-VU (other card interface devices)

Security attributes for subjects:

· USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

·USER_ID Vehicle Registration Number (VRN) and Registering Member State Code (MSC), exists only for subject S.VU

Objects:

-·user data:

- •identification data (card identification data, cardholder identification data)
- •activity data (cardholder activities data, events and faults data, control activity data)

-·security data:

- •cards´s private signature key
- •public keys (in particular card´s public signature key; keys stored permanently on the card or imported into the card using certificates)
- •session keys
- •PIN (for workshop card only)

-·TOE software code

-·TOE file system (incl. file structure, additional internal structures, access conditions)

-·identification data of the TOE concerning the IC and the Smartcard Embedded Software (indicated as identification data of the TOE in the following text)

- identification data of the TOE`s personalisation concerning the date and time of the personalisation (indicated as identification data of the TOE`s personalisation in the following text)

Security attributes for objects:

·Access Rules based on defined Access Conditions (see below) for:

- •user data
- •security data
- •identification data of the TOE
- •identification data of the TOE's personalisation

·Digital signature for each data to be signed

Operations:

user data:

- •identification data: selecting (command Select), reading (command Read Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)
- •activity data: selecting (command Select), reading (command Read Binary), writing / modification (command Update Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)

·security data:

- •card´s private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication (command External Authenticate)
- •public keys (in particular card´s public signature key): referencing over a MSE-command (for further usage within cryptographic operations as authentication, verification of a digital signature etc.)
- •session keys: securing of commands with Secure Messaging
- •PIN (only relevant for Workshop Card): verification (command Verify PIN)

·TOE software code: No Operations

TOE file system (incl. file structure, additional internal structures, access conditions): No Operations

·identification data of the TOE: selecting and reading

·identification data of the TOE's personalisation (date and time of personalisation): selecting and reading.

Access Rules:

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object. The possible commands are described in the Tachograph Card specification [7], sec. 3.6. Following Access Conditions are defined in the Tachograph Card specification [7], sec. 3.3:

- **NEV (Never)** - The command can never be executed.
- **ALW (Always)** - The command can be executed without restrictions.
- **AUT (Key based authentication)** - The command can be executed only if the preceding external authentication (done by the command External Authenticate) has been conducted successfully.
- **PRO SM (Secure Messaging providing data integrity and authenticity for command resp. response)** - The command can be executed and the corresponding response can be accepted only if the command/response is secured with a cryptographic checksum using Secure Messaging as defined in the Tachograph Card Specification [7], sec. 3.6 and Tachograph Common Security Mechanisms [9], sec. 5.
- **AUT and PRO SM** (combined, see description above)

For each type of Tachograph Card the Access Rules (which make use of the Access Conditions described above) for the different objects are implemented according to the requirements in the Tachograph Card Specification [7], sec. 4 and GST [8], sec. 4.3. These access rules cover in particular the rules for the export and import of data.

For the Tachograph Card type Workshop Card an additional AC is necessary. A mutual authentication process between the card and the external world is only possible if a successful preceding verification process with the PIN of the card has been taken place.

6.1.1 Security functional requirements list

Identification	Description
FAU	Security Audit
FAU_SAA.1	Security Audit Analysis
FCO	Communication
FCO_NRO.1	Non-repudiation of origin
FCS	Cryptographic support
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	User data protection
FDP_ACC.2	Complete Access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic Data Authentication

FDP_ETC.1	Export of user data without security attributes
FDP_ETC.2	Export of user data with security attributes
FDP_ITC.1	Import of User Data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FIA	Identification and Authentication
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.3	Unforgeable authentication
FIA_UAU.4	Single use authentication mechanisms
FIA_UID.1	Timing of identification
FIA_USB.1	User subject binding
FPR	Privacy
FPR_UNO.1	Unobservability
FPT	Protection of the TOE Security Function
FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_TDC.1	Inter-TSF TSF data consistency
FPT_TST.1	TSF testing
FTP	Trusted path/Channel
FTP_ITC.1	Inter-TSF trusted channel

Table 3 Tacho V1.3 security functional requirements list

6.1.2 FAU: Security Audit

6.1.2.1 FAU_SAA Security Audit Analysis

Hierarchical to: No Other component

FAU_SAA.1.1 The TSF shall be able **to detect failure events as cardholder authentication failures, self test errors, stored data integrity errors and activity data input integrity errors**, to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs

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

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

known to indicate a potential security violation;

No other rules[1]

Dependencies: FAU.GEN.1 Audit Data Generation Not applicable for a smart card

The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE ; the FAU_GEN.1 component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable in a SmartCard since many of these events result in card being in an insecure state where recording of the event itself could cause a security breach. It is then assumed that the function FAU_SAA.1 may still be used and the specific audited events will have to be defined in the ST independently with FAU_GEN.1. »

6.1.3 FCO: Communication

6.1.3.1 FCO_ NRO Non-repudiation of origin

FCO_NRO.1 Selective proof of origin

Hierarchical to: No other component

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

FCO_NRO.1.2 The TSF shall be able to relate the **card holder identity by means of digital signature** of the originator of the information, and **the hash value over the data to be downloaded to external media** of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to recipient given **in accordance with the Tachograph Common Security Mechanisms [9], sec 6, CSM_035**.

Dependencies: FIA_UID.1 Timing of identification

6.1.4 FCS – Cryptographic support

Remark: To be in the context of the French qualification RSA key shall use 1536 or 2048 bits.

6.1.4.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other component

[1] [assignment: any other rules]

FCS_CKM.1.1 / Session GP	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 **[GP Session keys SCP01, cf. [GP211]]**
FCS_CKM.1.1 / Session A1B	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic two-keys TDES derivation algorithms]** and specified cryptographic key sizes **[128 bits with 112 effective bits]** that meet the following **[Tachograph Common Security Mechanisms [9], sec 3,CSM_012,CSM_013,CSM_015,CSM_020].**
FCS_CKM.1.1 / Card private 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 **[None]**

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

FCS_COP.1 Cryptographic operations]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other component

FCS_CKM.2.1 / Session A1B	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **TDES session key agreement by an internal-external authentication mechanism** that meets the following **Tachograph Common Security Mechanisms [9], sec. 3, CSM_012, CSM_013, CSM_015, CSM_020 and Tachograph Card Specification [7], sec 3.6**
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]**

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other component

FCS_CKM.4.1 / Session GP	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: **[Tachograph Common Security Mechanisms [9] sec. 3, CSM_013 and Tachograph Card Specification [7], sec 3.6]]**. Application note : The session keys will be destroyed at the end of the session (withdrawal of the card or reset of the card) and /or after 240 use.

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.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

6.1.4.2 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

Hierarchical to: No other component

FCS_COP.1.1/RSA	The TSF shall perform **the cryptographic operations (encryption, decryption, signature creation and signature verification as well as certificate verification for the authentication between the Tachograph Card and the Vehicle Unit and signing for downloading to external media]** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits** that meet the following: **Tachograph Common Security Mechanisms [9] sec 2.6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_016, CSM_017, CSM_018, CSM_019, CSM_020,CSM_033, CSM_034, CSM_035 and Tachograph Card Specification [7], sec 3.**
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**: [FIPS180-2]**.
FCS_COP.1.1/TDES	The TSF shall perform **the cryptographic operations (encryption and decryption respective Retail-MAC generation and verification) concerning symmetric cryptography** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **128 bits with 112 effective bits** that meet the following:

	Tachograph Common Security Mechanisms [9] sec 2, CSM_005, sec 3, CSM_015, sec 5,CSM_021,CSM_031 and Tachograph Card Specification [7], sec 3.
FCS_COP.1.1/GP MAC	The TSF shall perform **[MAC computation in GP session]** in accordance with a specified cryptographic algorithm **[TDES-CBC]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]**.
FCS_COP.1.1/GP ENC	The TSF shall perform **[Encryption and decryption in GP session]** in accordance with a specified cryptographic algorithm **[TDES-ECB]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

6.1.5 FDP: User data protection

6.1.5.1 FDP_ACC Access Control policy

FDP_ACC.2 Complete access control
Hierarchical to: No other component

FDP_ACC.2.1/ SFP	AC_SFP	The TSF shall enforce the **AC_SFP** on **[** **subjects:** **- S.VU (in the sense of the Tachograph Card specification)** **- S.Non-VU (other card interface devices)** **objects:** **- user data:** **- identification data** **- activity data** **- security data:** **- cards´s private signature key** **-public keys** **-session keys** **-PIN (for workshop card)** **- TOE software code** **- TOE file system** **- identification data of the TOE** **- identification data of the TOE`s personalisation** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/ SFP	AC_SFP	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.5.2 FDP_ACF access control function

FDP_ACF.1 Security attributes based access control

Hierarchical to: No other component

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** to objects based on the following:

subjects:
- **S.VU (in the sense of the Tachograph Card specification)**
- **S.Non-VU (other card interface devices)**

objects:
- **user data:**
  - **identification data**
  - **activity data**
- **security data:**
  - **cards´s private signature key**
  - **public keys**
  - **session keys**
  - **PIN (for workshop card)**
- **TOE software code**
- **TOE file system**
- **identification data of the TOE**
- **identification data of the TOE`s personalisation**
- **security attributes for subjects:**
  - **USER_GROUP**
  - **USER_ID**
- **security attributes for objects:**
  - **Access Rules.**

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:

- GENERAL_READ:
driver card, workshop card: user data may be read from the TOE by any user
control card, company card: user data may be read from the TOE by any user, except cardholder identification data which may be read by S.VU only;

- IDENTIF_WRITE: all card types: identification data may only be written once and before the end of Personalisation; no user may write or modify identification data during end-usage phase of card's life-cycle;

- ACTIVITY_WRITE: all card types: activity data may be written to the TOE by S.VU only;

- SOFT_UPGRADE: all card types: no user may upgrade TOE's software;

- FILE_STRUCTURE: all card types: files structure and access conditions shall be created before the Personalisation is completed and then locked from any future modification or deletion by any user

- IDENTIF_TOE_READ: all card types: identification data of the TOE and identification data of the TOE's personalisation may be read from the TOE by any user;

- IDENTIF_TOE_WRITE: all card types: identification data of the TOE may only be written once and before the Personalisation; no user may write or modify these identification data during the Personalisation;

- IDENTIF_TOE_PERS_WRITE: all card types: identification data of the TOE's personalisation may only be written once and within the Personalisation ; no user may write or modify these identification data during end-usage phase of card's life-cycle.

FDP_ACF.1.3/ AC_SFP SFP — The TSF shall explicitly authorize 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 following additional rules: **none**

.

Dependencies: FDP_ACC.1 Subset access control
FDP_MSA.3 Static attribute initialization

6.1.5.3 FDP_DAU: Data Authentication

FDP_DAU.1: Basic Data Authentication

Hierarchical to: No Other component

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 **S.VU and S.Non-VU** with the ability to verify evidence of the validity of indicated information.

Dependencies: No dependency

6.1.5.4 FDP_ETC :Export from the TOE

FDP_ETC.1: Export of user data without security attributes

Hierarchical to: No other component

FDP_ETC.1.1 — The TSF shall enforce the **AC_SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

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** when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: **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 is the signature of the file.

6.1.5.5 FDP_ITC Import From outside of the TOE

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

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

6.1.5.6 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

6.1.5.7 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"

Identification data

Activity data

Card private key

Euro public key

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for **[integrity errors]** 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

6.1.6 FIA: Identification and authentication

6.1.6.1 FIA_AFL Authentication failure

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other component

FIA_AFL.1.1 / Card interface GP	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 GP	When the defined number of unsuccessful authentication attempts has been **met** , 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 / C — The TSF shall detect when ***1*** unsuccessful authentication attempts occur related to **authentication of a card interface device**.

FIA_AFL.1.2 C — When the defined number of unsuccessful authentication attempts has been **met , or surpassed** the TSF shall warn **the entity connected assume the user as S.Non-VU**

FIA_AFL.1.1 / WSC — The TSF shall detect when ***5*** unsuccessful authentication attempts occur related to **PIN verification of Workshop Card.**

FIA_AFL.1.2 / WSC — When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **warn the entity connected block the PIN check procedure such that any subsequent PIN check attempt will fail be able to indicate to subsequent users the reason of the blocking.**

Dependencies: FIA_UAU.1 Timing of authentication

.

6.1.6.2 FIA_ATD User attribute definition

FIA_ATD.1 User attribute definition

Hierarchical to: No other component

FIA_ATD.1.1 — The TSF shall maintain the following list of security attributes belonging to individual users **[**

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

- USER_ID (VRN and Registering MSC for subject S.VU).

Dependencies: No dependency

6.1.6.3 FIA_UAU User authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other component

Driver & Workshop Cards

FIA_UAU.1.1 — The TSF shall allow

driver card, workshop card: export of user data with security attributes (card data download function),
control card, company card: export of user data without security attributes except export of cardholder identification data

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other component

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

Hierarchical to: No other component

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **key based authentication mechanisms.**

6.1.6.4 FIA_UID User Identification

FIA_UID.1Timing of identification

Hierarchical to: No other component

FIA_UID.1.1 / Driver & Workshop Cards The TSF shall allow **[Download of User Data]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 / Driver & Workshop Cards The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1.1 / Control & company Cards	The TSF shall allow **[Download of User Data except cardholder identification data]** 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.

Dependencies: No dependency

Note: In the smart card, Identification and authentication are a single process.

6.1.6.5 FIA_USB User-Subject Binding

FIA_USB.1 User-subject binding

Hierarchical to: No Other component

FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: - **USER_GROUP (VEHICLE_UNIT for S.VU, NON_VEHICLE_UNIT for S.Non-VU)** **- USER_ID (VRN and Registering MSC for subject S.VU)**
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**none].**
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[none].**

Dependencies: FIA_ATD.1 User attribute definition

6.1.7 FPR:Privacy

6.1.7.1 FPR_UNO Unobservability

FPR_UNO.1 Unobservability

Hierarchical to: No other component

FPR_UNO.1.1	The TSF shall ensure that **Attackers** are unable to observe the operation **with involved authentication and/or cryptographic operations** on **security and activity data** by **any user**.

Dependencies: no dependency

6.1.8 FPT: Protection of the TSF

6.1.8.1 FPT_EMS TOE Emanation

FPT_EMS.1 TOE Emanation

Hierarchical to: No other component

FPT_EMS.1.1	The TOE shall not emit [**Side channel current**] in excess of [**State of the art limits**] enabling access to **privates key(s) and session keys** and [**activity data**].
FPT_EMS.1.2	The TOE shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **private key(s) and session keys and [activity data]**

Dependencies: No dependency

6.1.8.2 FPT_FLS Failure secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other component

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **- Reset** **- power supply cut-off** **- power supply variations** **Unexpected abortion of the TSF execution due to external or internal events (esp. break of a transaction before completion)**

Dependencies: No dependency

6.1.8.3 FPT_PHP TSF physical Protection

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other component

FPT_PHP.3.1	The TSF shall resist **physical manipulation and physical probing** to the **all TOE components implementing the TSF** by responding automatically such that the SFRs are always enforced.

Dependencies: No dependency

6.1.8.4 FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1 Inter-TSF TSF basic data consistency

Hierarchical to: No Other component

FPT_ TDC.1.1	The TSF shall provide the capability to consistently interpret **key material (session keys and certificates** when shared between the TSF and another trusted IT product.

FPT_ TDC.1.2	The TSF shall use **rules for the interpretation of key material (session keys and certificates) as defined in Tachograph Security Mechanisms [9], and Tachograph Card Specification [7], sec 3.6** when interpreting the TSF data from another trusted IT product.

Dependencies: No dependency

6.1.8.5 FPT_TST TSF self test

FPT_TST.1 TSF testing
Hierarchical to: No other component

FPT_TST.1.1	The TSF shall run a suite of self-tests 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 authorized users with the capability to verify the integrity of **TSF data**.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of **the TSF**.

Dependencies: No dependency

6.1.9 FTP: Trusted Path / Channel

6.1.9.1 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted Channel

Hierarchical to: No other component

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another 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 **another trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for a**ctivity data import from a remote trusted product.**

Refinement: The mentioned remote trusted IT product is the Vehicle Unit.
Dependencies: No dependency

6.2 SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CCPART3].

The assurance level is **EAL4** augmented on:

ALC_DVS.2: Sufficiency of security measures.

ATE_DPT.2: Testing : Security enforcing modules

AVA_VAN.5: Advanced methodical vulnerability analysis

6.2.1 TOE security assurance requirements list

Table below shows equivalence between SAR in CC V2.3 and SAR CC V3.1.

CC V3.1 will be followed on this part.

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
Configuration Management	ACM_AUT	--
	ACM_CAP	ALC_CMC
	ACM_SCP	ALC_CMS
Delivery and operation	ADO_DEL	ALC_DEL partially AGD_PRE [1.1C]
	ADO_IGS	installation: AGD_PRE [1.2C] start-up: part of ADV_ARC [1.3C]
Development	ADV_LLD	ADV_TDS partially ADV_ARC [1.2C, 1.4C, 1.5C]
	ADV_FSP	ADV_FSP
	ADV_IMP	ADV_IMP
	ADV_HLD	ADV_TDS
Guidance documents	AGD_USR	AGD_OPE

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
	AGD_ADM	AGD_OPE
Life-cycle support	-- (ACM_CAP)	ALC_CMC
	-- (ACM_SCP)	ALC_CMS
	-- (ADO_DEL)	ALC_DEL
	ALC_DVS	ALC_DVS
	ALC_LCD	ALC_LCD
	ALC_TAT	ALC_TAT
Security Target evaluation	ASE	ASE
Tests	ATE_COV	ATE_COV
	ATE_DPT	ATE_DPT
	ATE_FUN	ATE_FUN
	ATE_IND	ATE_IND
Vulnerability assessment	AVA_CCA	AVA_VAN
	AVA_VLA	AVA_VAN
	AVA_SOF	AVA_VAN
	AVA_MSU	AGD_OPE [1.5C – 1.8C] AGD_PRE.1.2C (WU AGD_PRE.1-4) AGD_PRE.1.2E

Table 4. SAR CC V2.3 versus CC V3.1

Identification	Description
ADV	Development
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD	Guidance documents
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC	Life cycle support
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	**Sufficiency of security measures**
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE	Tests
ATE_COV.2	Analysis of coverage
ATE_DPT.2	**Testing : Security enforcing modules**
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA	Vulnerability assessment
AVA_VAN.5	**Methodical vulnerability analysis,**

Table 5. TOE security assurance requirements list

6.3 SECURITY REQUIREMENTS RATIONALE

The aim of this section is to demonstrate that the combination of the security functional requirements and assurance measures is suitable to satisfy the identified security objectives.

6.3.1 Security Functional Requirements Rationale

The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one objective.

	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication
FAU_SAA.1	X	X		X
FCO_NRO.1				X
FCS_CKM.1 / Session GP				X
FCS_CKM.1 /Session A1B				X
FCS_CKM.1 / Card Private Key				X
FCS_CKM.2/ Session GP				X
FCS_CKM.2/Session A1B				X
FCS_CKM.2/ Card Private Key				X
FCS_CKM.4				X
FCS_COP.1/RSA				X
FCS_COP.1/TDES				X
FCS_COP.1/GP MAC				X
FCS_COP.				X

	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication
1/GP ENC				
FDP_ACC.2	X	X	X	X
FDP_ACF.1	X	X	X	X
FDP_DAU.1				X
FDP_ETC.1				X
FDP_ETC.2				X
FDP_ITC.1				X
FDP_RIP.1				X
FDP_SDI.2	X	X		
FIA_AFL.1/C			X	
FIA_AFL.1/WSC			X	
FIA_AFL.1 Interface GP			X	
FIA_ATD.1			X	
FIA_UAU.1			X	
FIA_UAU.3			X	X
FIA_UAU.4				X
FIA_UID.1			X	
FIA_USB.1			X	
FPR_UNO.1				X
FPT_EMS.1	X	X	X	X
FPT_FLS.1	X	X	X	X
FPT_PHP.3	X	X	X	X
FPT_TDC.1				X

	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication
FPT_TST.1	X	X	X	X
FTP_ITC.1				X

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

According to the security objective **OT.Card_Identification_Data**, the TOE preserves card identification data and cardholder identification data stored during card personalisation process as specified by the EU documents. The access to the TOE's data, especially to the identification data is regulated by the security function policy AC_SFP. This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1, explicitly denies the write access to personalised identification data. The integrity of the stored data within the TOE, especially the integrity of the identification data is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1 (as single failure event or in combination with other failure events), the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the stored identification data and their modification.

According to the security objective **OT.Card_Activity_Storage**, the TOE preserves user data stored in the card by Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP. This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1, explicitly restricts the write access to user data to authenticated Vehicle Units. The integrity of the stored data within the TOE, especially the integrity of the user data written by Vehicle Units is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1, the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the user data written by Vehicle Units and their modification.

According to the security objective **OT.Data_Access**, the TOE limits the user data write access in the TOE's end-usage phase to authenticated Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP.

This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1, explicitly restricts the write access to user data to authenticated Vehicle Units. The components FIA_USB.1 and FIA_ATD.1 with its definition of the user security attributes supply a distinction between Vehicle Units and other card interface devices. The components FIA_UID.1 and FIA_UAU.1 ensure that especially the write access to user data is not possible without a preceding successful authentication process. If the authentication fails, the component FIA_AFL.1/C resp. FIA_AFL.1/WSC reacts with a warning to the connected entity, and the user will be assumed as different from a Vehicle Unit. The component FIA_UAU.3 prevents the use of forged authentication data. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to user data write access.

According to the security objective **OT.Secure_Communication**, the TOE supports secure communication protocols and procedures between the card and the card interface device when required by the application as specified by the EU documents.

The component FTP_ITC.1 together with FDP_ETC.1 and FDP_ITC.1 offers the possibility to secure the data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel assuring identification of its end points and protection of the data transfer from modification and disclosure. Hereby, both parties are capable of verifying the received data with regard to their integrity and authenticity. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys which is covered by the

components FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1/RSA for cryptographic support. The cryptographic component FCS_COP.1/TDES realise the securing of the data exchange itself.

The cryptographic components FCS_COP.1/GP MAC and FCS_COP.1/GP ENC realise the securing of the data exchange during the personalization in phase 6

The components FPR_UNO.1 guarantees for the unobservability of the establishing process of the trusted channel and for the unobservability of the data exchange itself which both contributes to a secure data transfer. The components FIA_UAU.3 and FIA_UAU.4 support the security of the trusted channel as the TOE prevents the use of forged authentication data and as the TOE's input for the authentication tokens and for the session keys within the preceding authentication process is used only one time. During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will send a warning to the entity sending the data, which is realised by the component FAU_SAA.1;

Furthermore, within the TOE's end-usage phase, the TOE offers a data download functionality with specific properties. The TOE provides the capability to generate an evidence of origin for the data downloaded to the external media, to verify this evidence of origin by the recipient of the data downloaded and to download the data to external media in such a manner that the data integrity can be verified. All these requirements are covered by FDP_ETC.2, FCO_NRO.1 and FDP_DAU.1. The corresponding cryptographic components for conducting the data download process with its security features are given with FCS_COP.1/RSA.

For each secure communication described above, the component FPT_TDC.1 ensures for a consistent interpretation of the security related data shared between the TOE and the external world. The necessity for the usage of a secure communication protocol as well as the access to the relevant card´s keys is deposited in the security function policies AC_SFP defined in chap. 6.1.1. These policies correspond directly to the SFRs FDP_ACC.2 and FDP_ACF.1. Finally, the components FDP_RIP.1, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the secure communication protocols.

6.3.2 DEPENDENCIES

6.3.2.1 SFRs dependencies

Requirements	CC dependencies	Satisfied dependencies
FAU_SAA.1	FAU_GEN.1	justification 1 for non-satisfied dependencies
FCO_NRO.1	FIA_UID.1	FIA_UID.1/Driver & Workshop cards FIA_UID.1/Control & Company Cards
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP1, FCS_CKM.4
FCS_CKM.2	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2	FCS_CKM.1
FCS_COP.1/RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	justification 2 for non-satisfied dependencies
FCS_COP.1/TDES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/GP MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/GP ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.2/AC_SFP SFP	FDP_ACF.1	FDP_ACF.1/AC_SFP SFP
FDP_ACF.1/AC_SFP SFP	FDP_ACC.1. FMT_MSA.3	FDP_ACC.1/AC_SFP SFP, justification 3 for non-satisfied dependencies
FDP_DAU.1	none	
FDP_ETC.1	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/AC_SFP SFP
FDP_ETC.2	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/AC_SFP SFP
FDP_ITC.1	(FDP_ACC.1 or FDP_IFC.1), FMT_MSA.3	FDP_ACC.2/AC_SFP SFP, justification 3 for non-satisfied dependencies

Requirements	CC dependencies	Satisfied dependencies
FDP_RIP.1	none	
FDP_SDI.2	none	
FIA_AFL.1/ interface GP	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1C	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/ WSC	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	none	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.3	none	
FIA_UAU.4	none	
FIA_UID.1/Driver & Workshop Card	none	
FIA_UID.1/Control & company Cards	none	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FPR_UNO.1	none	
FPT_EMS.1	none	
FPT_FLS.1	none	
FPT_PHP.3	none	
FPT_TDC.1	none	
FPT_TST.1	none	
FTP_ITC.1	none	

Justification for non-satisfied dependencies:

No.1: The dependency FAU_GEN.174 (Audit Data Generation) is not applicable to the TOE. Tachograph cards do not generate an audit record but reacts with an error response resp. reset. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.

No.2: The SFR FCS_COP.1/RSA uses keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1/RSA.

No.3: The access control TSF according to FDP_ACF.1 uses security attributes (access rules, refer to sec. 6.1.1) which are defined during the Personalisation Phase respective initialisation (for the terms refer to sec. 1.2.3) and are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, neither during the personalisation nor within the usage phase of the TOE. This argument holds for FDP_ACF.1 as well as for FDP_ITC.1.

6.3.2.2 Assurance measures rationale

6.3.2.2.1 ADV Development

6.3.2.2.1.1 ADV_ARC: Security architecture description

ADV_ARC.1 done in [ARC_PHAESTOS3].

6.3.2.2.1.2 *ADV_FSP: Complete functional specification*

ADV_FSP.4 done in [FSP_PHAESTOS3].

6.3.2.2.1.3 *ADV_IMP: Implementation representation of the TSF*

ADV_IMP.1 done in [IMP_PHAESTOS3].

6.3.2.2.1.4 *ADV_TDS: Basic modular design*

ADV_TDS.3 done in [TDS_PHAESTOS3].

6.3.2.2.2 AGD Guidance documents

6.3.2.2.2.1 AGD_OPE: Operational user guidance

AGD_OPE.1 done in [OPE_PHAESTOS3].

6.3.2.2.2.2 AGD_PRE: Preparative procedures

AGD_PRE.1 done in [PRE_PHAESTOS3].

6.3.2.2.3 ALC Life cycle support

6.3.2.2.3.1 ALC_ CMC: Production support, acceptance procedures and automation

ALC_ CMC.4 done in [CMC_PHAESTOS3].

6.3.2.2.3.2 ALC_ CMS: Problem tracking CM coverage

ALC_ CMS.4 done in [CMS_PHAESTOS3].

6.3.2.2.3.3 ALC_ DVS: Identification of security measures

ALC_DVS.2 done in [DVS_PHAESTOS3].

6.3.2.2.3.4 ALC_ DEL: Delivery procedures

ALC_DEL.1 done in [DEL_PHAESTOS3].

6.3.2.2.3.5 ALC_ LCD: Developer defined life-cycle model

ALC_LCD.1 done in [LCD_PHAESTOS3].

6.3.2.2.3.6 ALC_ TAT: Well-defined development tools

ALC_TAT.1 done in [TAT_PHAESTOS3].

6.3.2.2.4 ATE Tests

6.3.2.2.4.1 ATE_COV: Coverage

ATE_COV.2 done in [COV_PHAESTOS3].

6.3.2.2.4.2 ATE_DPT Testing: security enforcing modules

ATE_DPT.2 done in [DPT_PHAESTOS3].

6.3.2.2.4.3 ATE_FUN: Functional tests

ATE_FUN.1 done in [FUN_ PHAESTOS3].

6.3.2.2.4.4 ATE_IND: Independent testing

ATE_IND.2 [IND_ PHAESTOS3] will be provided by the ITSEF (Evaluation Laboratory).

6.3.2.2.5 AVA Vulnerability assessment

6.3.2.2.5.1 AVA_VAN: Vulnerability analysis

AVA_VAN.5 No evidence element is required (except the TOE samples).

6.4 COMPOSITION TASKS – SFR PART

The following table (see next page) lists the SFRs that are declared in the P5CC081 security target [ST-IC] and separates them in relevant platform[2]-SFRs (RP_SFR) and irrelevant platform-SFRs (IP_SFR), as requested in [CCDB]. The table also provides the link between the relevant platform-SFRs and the composite product SFRs.

[2] In the present ST, the platform is the P5CC081 chip.

Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
FAU_SAS.1	The TSF shall provide the test process before TOE Delivery with the capability to store the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software in the EEPROM.	None	X		No link to TOE SFRs but used for the composite-product identification.
FCS_COP.1 / DES	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Triple Data Encryption Algorithm (TDEA) and cryptographic key sizes of 112 or 168 bit that meet the following list of standards: FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25, keying options 1 and 2.	None	X		FCS_COP.1 / GP ENC FCS_COP.1 / GP MAC
FCS_COP.1 / AES	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) algorithm and cryptographic key sizes of 128, 192 or 256 bit that meet the following list of standards: FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26.	None		X	Not used by the composite TOE
FCS_RNG.1	The TSF shall provide a physical random number generator that implements total failure test of the random source.	None	X		FCS_CKM.1 / Card private key FCS_CKM.1 / Session GP FCS_CKM.1 / Session A1B

Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
FDP_ACC.1 / MEM	The TSF shall enforce the Access Control Policy on all code running on the TOE, all memories and all memory Operations.	SFP_3: Access Control Policy The hardware shall provide different CPU modes to the IC Dedicated Software and Security IC Embedded Software. The TOE shall separate IC Dedicated Software and Security IC Embedded Software from each other by both, partitioning of memory and different CPU modes. The management of access to code and data as well as the configuration of the hardware shall be performed each in a dedicated CPU mode. The hardware shall enforce a separation between different applications (i.e.	X		FPT_TST.1
FDP_ACC.1 / SFR	The TSF shall enforce the Access Control Policy on all code running on the TOE, all Special Function Registers, and all Special Function Register operations.			X	Not used by the composite TOE
FDP_ACF.1 / MEM	The TSF shall enforce the Access Control Policy to objects based on the following: all subjects and objects and the attributes CPU mode, the MMU Segment Table, the Special Function Registers to configure the MMU segmentation and the Special Function Registers related to system Management.		X		FPT_TST.1
FDP_ACF.1 / SFR	The TSF shall enforce the Access Control Policy to objects based on the following: all subjects and objects and the attributes CPU mode, the MMU Segment Table and the Special Function Registers FWCTRLL and FWCTRLH.			X	Not used by the composite TOE
FMT_MSA.1 /	The TSF shall enforce the Access Control Policy to restrict the ability		X		FPT_TST.1

MEM	to modify the security attributes Special Function Registers to configure the MMU segmentation to code executed in the System Mode.	parts of the Security IC Embedded Software) running on the TOE. An application shall not be able to access hardware components without explicitly granted permission.			
FMT_MSA.1 / SFR	The TSF shall enforce the Access Control Policy to restrict the ability to modify the security attributes defined in Special Function Registers to code executed in a CPU mode which has write access to the respective Special Function Registers.			X	Not used by the composite TOE
FMT_MSA.3 / MEM	The TSF shall enforce the Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. The TSF shall allow no subject to specify alternative initial values to override the default values when an object or information is created.		X		FPT_TST.1
FMT_MSA.3 / SFR	The TSF shall enforce the Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. The TSF shall allow no subject to specify alternative initial values to override the default values when an object or information is created.			X	Not used by the composite TOE

Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
FMT_SMF.1	The TSF shall be capable of performing the following security management functions: Change of the CPU mode by calling a system call vector (SVEC) or configuration vector (CVEC) address, change of the CPU mode by invoking an exception or interrupt, change of the CPU mode by finishing an exception/interrupt (with a RETI instruction), change of the CPU mode with a special LCALL/ACALL/ECALL address, change of the CPU mode by writing to the respective bits in the PSWH Special Function Register and		X		FPT_TST.1

	modification of the Special Function Registers containing security attributes, and modification of the MMU Segment Table.				
FDP_IFC.1	The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TSF or by the Security IC Embedded Software.	SFP_2: Data Processing Policy User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.	X		FPR_UNO.1
FDP_ITT.1	The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.		X		FPR_UNO.1 FPT_PHP.3
FPT_ITT.1	The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE. The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.		X		FPR_UNO.1 FPT_PHP.3
FMT_LIM.1	The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Limited capability and availability Policy.	SFP_1: Limited capability and availability Policy Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.	X		No direct link to a specific composite SFR. However, participates to the TSF enforcement.
FMT_LIM.2	The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Limited capability and availability Policy.		X		No direct link to a specific composite SFR. However, participates to the TSF enforcement.

latform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs

FPT_FLS.1	**Failure with preservation of secure state**: The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.		X		FPT_PHP.3 FPT_FLS.1
FRU_FLT.2	**Limited fault tolerance**: The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).	None	X		FPT_PHP.3
FPT_PHP.3	The TSF shall resist physical manipulation and physical probing, to the TSF by responding automatically such that the SFRs are always enforced.	None	X		FPT_PHP.3

7 TOE SUMMARY SPECIFICATION

The security functionalities provided by the IC are described in [ST-IC]. The TOE Security Functionalities are described below.

7.1 TOE SECURITY FUNCTIONALITIES : BASIC

SF.TEST Self test

The TSF performs the following tests:

When starting a work session,

working condition of the work memory (RAM),

integrity of code in EEPROM,

Dependencies: SF.INTEGRITY

SF.EXCEPTION Error Messages and exceptions

The TOE reports the following errors:

Message format errors,

Integrity errors,

Life cycle status errors,

Errors in authentication attempt.

The card becomes mute (secure Fail State) when one of the following errors occurs:

Error on integrity of keys or PINs,

Out of range in frequency or voltage,

Life cycle status errors,

Dependencies: SF.DRIVER

SF.ERASE Data erasure

The whole RAM is erased after reset.

When a new mutual authentication is performed, the former session key set is destroyed without any possibility of even partial recovery.

Dependencies: No dependency

SF.INTEGRITY Data Integrity

The function provides the ability to check the integrity of the following data elements stored in the card:

Cryptographic keys including card private key, Euro public key and corresponding attributes,

Authentication data including PIN and corresponding attributes,

Data contained in the File System, including Identification data, Activity data.

Dependencies: No dependency

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

Dependencies: No dependency

SF.CARD_MGR Card manager

This function controls the execution of the card internal process when command messages are sent to the card. The messages handled are defined as specified in ISO 7816. Controls include:

CM Format verification

Identification: the instruction code of the message is supported,

Format analysis: the class is consistent with the instruction code, P1/P2/P3 parameter values are supported by the identified command.

CM Access checking

Life cycle analysis: the identified command shall be enabled in the current TOE life cycle phase of the TOE.

Check that the command sequence is respected,

Check that the authenticated user is allowed to send the command.

CM Execution

Execution: activation of the executable code corresponding to the card internal process for the command message.

CM Response

Control the build-up of the response.

Dependencies: SF.ACC

7.2 TOE SECURITY FUNCTIONALITIES : CRYPTOGRAPHIC

SF.KEY_GEN Key generation

The TOE can generate the Card private/public key pair, RSA 1024, in personalization phase.

The TOE generates Session keys, using TDES with 2 keys, according to the SCP01 and SCPi 05, see [GP211], in personalization phase. The generation process includes the distribution to the remote IT.

The TOE generates Session keys, using triple DES with 2 keys, according to the rules defined in [5], in usage phase. The generation process includes the distribution to the remote IT.

Dependencies: No dependency

SF.SIG Signature creation and verification

The TOE can sign a message digest, which is the result of a hash operation performed on a Tachograph data file, stored in the TOE. This hashing is performed by SF.HASH and the result is stored in the card.

The TOE can verify the signature of a message imported into the card.

The TOE uses a RSA PKCS#1 signature scheme with a 1024 bit modulus, as defined in [RSA SHA PKCS#1].

Dependencies: SF.KEY_GEN, SF.HASH

SF.ENC TDES encryption and decryption

The TOE encrypts and decrypts messages.

The encryption uses TDES with 2 keys, in CBC mode according to [SP800-67] and [SP800-38 A].

Dependencies: SF.KEY_GEN

SF.HASH Message hashing

The TOE can generate a hash of a file stored in the card.

Hashing is done using SHA_1 algorithm as specified in [FIPS180-2].

Dependencies: No dependency

SF.MAC MAC generation and verification

The TOE generates and verifies the MAC of messages.

The MAC computation uses TDES with 2 keys, in CBC according to [SP800-67] and [SP800-38 A].

Dependencies: SF.KEY_GEN

SF.TRUSTED Trusted Path

This function establishes a secure channel, using a mutual authentication.

The secure channel is GP in Personalization phase and A1B in Usage phase.

In GP, a ratification counter limits the number of failed consecutive authentication attempts. The counter initial value is 3. When the authentication fails, the counter is decremented. When the authentication succeeds, the counter is set to its initial value. 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.

Dependencies: SF.HASH, SF.MAC, SF.ENC

SF.PIN PIN management

This SF controls all the operation 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. After 5 consecutive unsuccessful verification of the PIN, it is blocked. When the PIN is blocked, then it cannot be used anymore.

Dependencies: No dependency

7.3 TOE SECURITY FUNCTIONALITIES: CARD MANAGEMENT

SF.ACC Access Authorization

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.

Dependencies: No dependency

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.

RSA keys have their own RAM space.

Dependencies: No dependency

7.4 TOE SECURITY FUNCTIONALITIES: PHYSICAL MONITORING

SF.DRIVER Chip driver

This function ensures the management of the chip security features:

Enforce shield protection,

physical integrity of the IC,

physical environment parameters,

Dependencies: No dependency

SF.ROLLBACK Safe fail state recovery

The function shall ensure that the TOE returns to its previous secure state when following events occur.
power cut-off or variations,

unexpected reset,

Dependencies: SF.DRIVER

7.5 TOE SUMMARY SPECIFICATION RATIONALE

Chapter content has been removed in Public Version

7.6 COMPOSITION RATIONALE

Chapter content has been removed in Public Version