PHAESTOS3
Public Security Target

CONTENT

FIGURES

TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

ST Title:	PHAESTOS V3 Security Target
ST Reference:	D1189203
Version:	1.1p
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

Context

The Commission of the European Communities has adopted a council regulation concerning a recorded equipment in road transport. The annex 1B of this document ([EEC/A1B]) gives the requirements for construction, testing, installation and inspection of this recording equipment.

The purpose of the recording equipment is to record, store, display, print, and output data related to driver activities.

[EEC/A1B] defines the tachograph card that is used in this equipment and [EEC/A1B] Appendix 10 gives a generic Security Target for this tachograph card.

In [JIL/Tacho], ANSSI and other Certification bodies have given an interpretation that defines the rules to be applied for the evaluation of the Tachograph Card.

The product to be evaluated complies with the requirements of [EEC/A1B], as interpreted by [JIL/Tacho].

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.

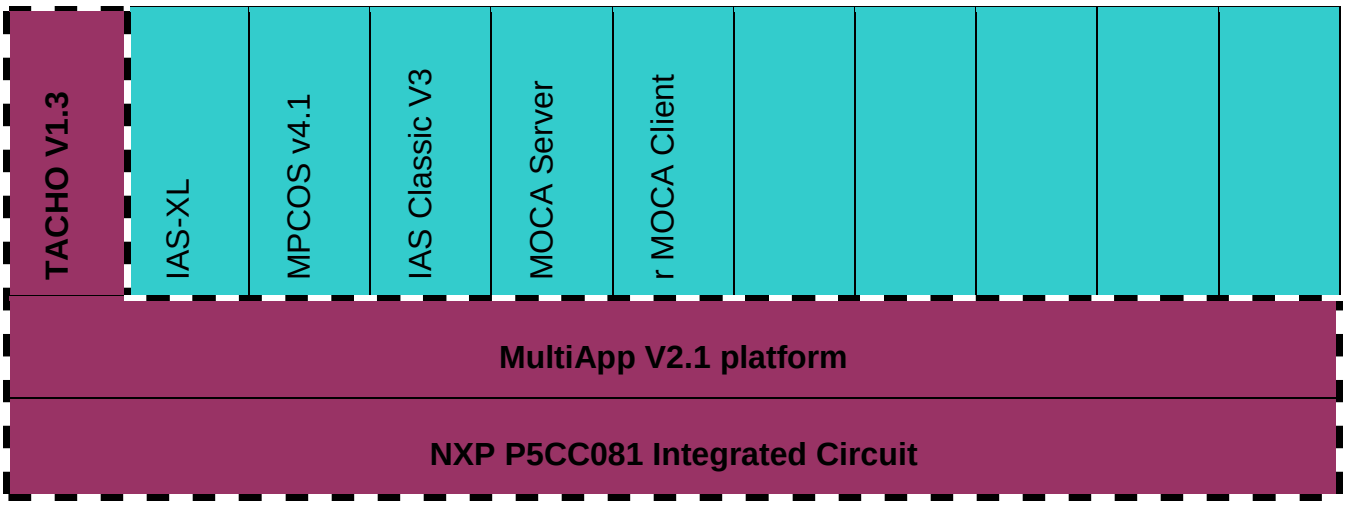

Figure 1 - MultiApp TACHO V13 Card

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

These ROMed applications are 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:

1. 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].
2. The GlobalPlatform Card Specification version 2.1.1[GP211]

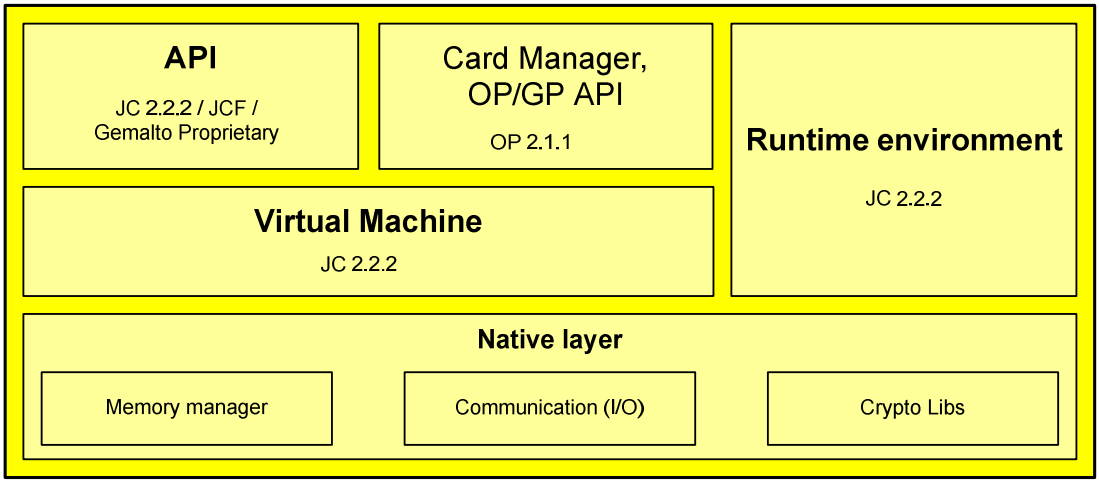

Figure 2: MultiApp ID V2.1 javacard platform architecture

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:
   - Checking environmental operating conditions using information provided by the IC,
   - Checking life cycle consistency,
   - Ensuring the security of the PIN and cryptographic keys objects,
   - Generating random number,
   - Handling secure data object and backup mechanisms,
   - Managing memory content
   - Ensuring Java Card firewall mechanism

1.4.2 TACHO V13 Application description

A Tachograph card is a smart card, as described in [PP/BSI-0035] and [PP/9911], carrying an application intended for its use with the recording equipment.

The basic functions of the Tachograph card are:

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

A Tachograph card is therefore intended to be used by a card interface device of a vehicle unit. It may also be used by any card reader (e.g. of a personal computer) who shall have full read access right on any user data.

During the end-usage phase of a Tachograph card life cycle (phase 7 of life-cycle as described in [PP/9911]), only vehicle units may write user data to the card.

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

“Tachograph card” means:

smart card intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage.

A Tachograph card may be of the following types:

- driver card,
- control card,
- workshop card,
- company card;

"company card" means:

A Tachograph card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment;

The company card identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company;

"control card" means:

A Tachograph card issued by the authorities of a Member State to a national competent control authority;

the control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading;

"driver card" means:

A Tachograph card issued by the authorities of a Member State to a particular driver;

the driver card identifies the driver and allows for storage of driver activity data;

"workshop card" means:

A Tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State.

The workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recording equipment;

Further description can be found in [EEC/A1B]

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

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".

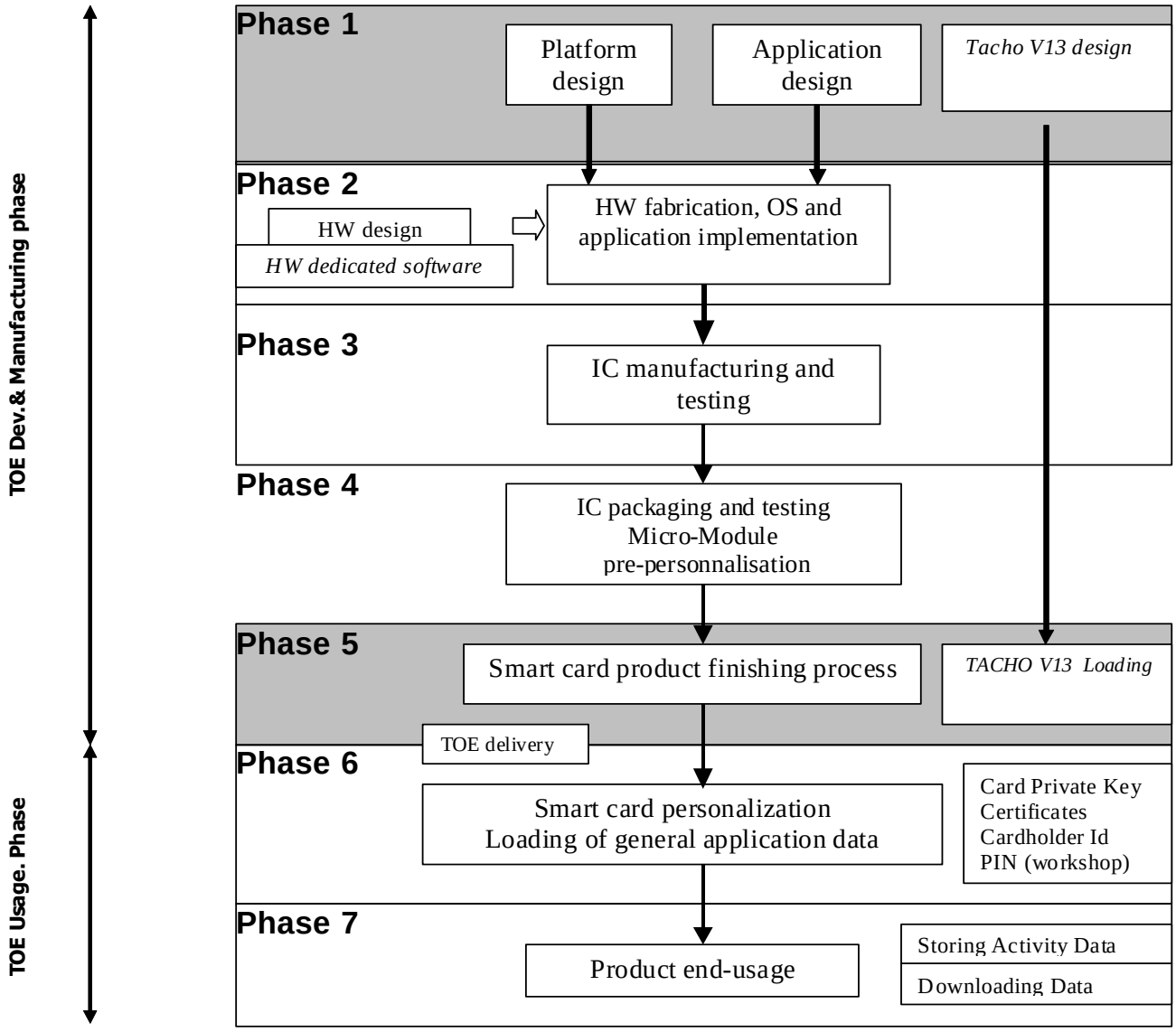

Figure 3 – Tachograph Card Life Cycle "Micro-module delivery"

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	Gemalto Gemenos

	Module packaging(embedding)	Gemalto Gemenos/Vantaa/Singapore
Phase 5	Pre-personalization	Gemalto Gemenos/Vantaa/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; Gemenos/Vantaa/Singapore 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

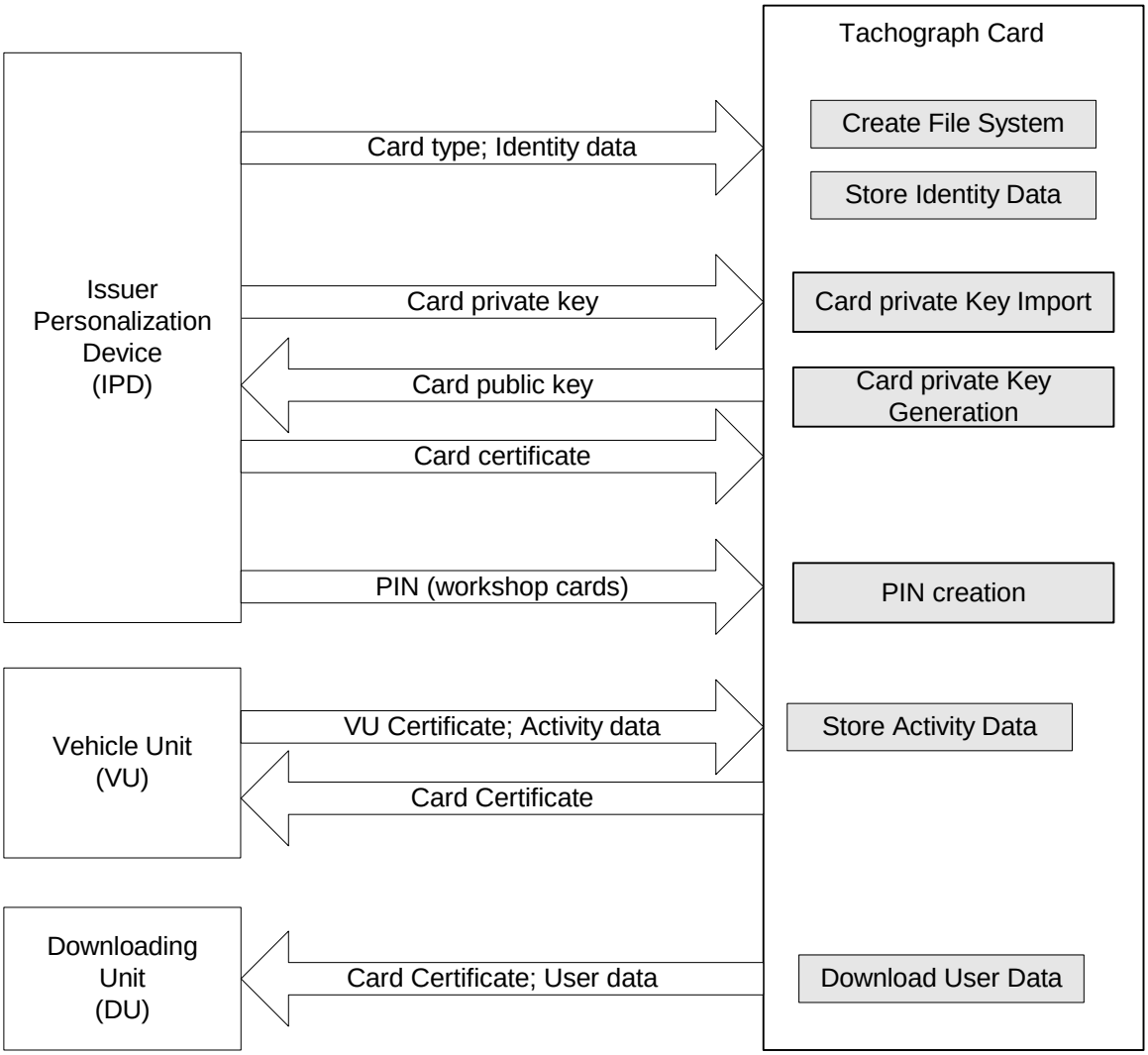

Figure 4: TOE Usage

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.
[ISO]	**ISO references**
[ISO 7816]	ISO 7816-X documents
[PP]	**Protection Profiles**
[PP/9806]	Protection Profile - Smart Card Integrated Circuit
[PP/9911]	Protection Profile - Smart Card Integrated Circuit With Embedded Software
[PP/BSI-0035]	Security IC Platform Protection Profile - BSI-PP-0035-2007; Version 1.0, 15 June 2007
[TACHO]	**Tachograph references**
[EEC/A1B]	Council Regulation No 3821/85 on recording equipment in road transport – Annex 1B Requirements for construction, Installation and Inspection
[JIL/Tacho]	Joint Interpretation Library – Security Evaluation and Certification of Digital Tachograph
[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
[ST_PHAESTOS3]	**PHAESTOS3 Security Target** Ref: D1189203(ST_D1189203)
[ADV]	**PHAESTOS3 ADV Documentation**
[FSP_PHAESTOS3]	**PHAESTOS3 Functional Specification** Ref: D1190952 (ADV_FSP_D1190952)
[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**
[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)

Reference	Title - Reference
[DPT_ PHAESTOS3]	**PHAESTOS3 Testing: security enforcing modules** Ref: D1190968 (ATE_DPT_ D1190968)
[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] conformant.

This ST is [CCPART3] conformant.

The TOE includes the Integrated Circuit certified with CC V3.1 EAL5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5.This IC has its own ST [ST-IC]. The assets, threats, objectives, SFR and security functions specific to the IC are described in [ST-IC] and are not repeated in the current ST.

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]

2.2 PP CLAIM, PACKAGE CLAIM

The PP [PP/9911] is included except for the parts regarding the IC.

This ST does not claim any strict or demonstrable conformance to a PP.

This ST is built on [EEC/A1B], [PP/9911] and [PP/BSI-0035]. It is conformant to [EEC/A1B] as interpreted by [JIL/Tacho]. It is based on [PP/9911]: it includes all assets, threats, assumptions, objectives and SFR of this PP but it includes an IC which claims [PP/BSI-0035], not the older [PP/9806] required by [PP/9911].

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

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

- ALC_DVS.2: Sufficiency of security measures.
- AVA_VAN.5: Advanced methodical vulnerability analysis

Equivalence between CC v2.3 EAL4 augmented (+) and CC v3.1 EAL4 augmented (+)

- ADV_IMP.2 (Development – Implementation of the FSP) in CC v2.3 is equivalent to ADV_IMP.1 in CC v3.1 managed by EAL4 (augmentation not required)
- ALC_DVS.2 (Sufficiency of security measures) augmentation is maintained in CC v3.1 EAL4 augmented
- AVA_MSU.3 (Analysis and testing for insecure states) this CC V3.1 assurance family moved in AGD families in CC3.1 managed by EAL4

- AVA_VLA.4 (Highly resistant) en CC v2.3 is equivalent to AVA_VAN.5 in CC v3.1, augmentation maintain in CC v3.1 EAL4 augmented

2.3 CONFORMANCE RATIONALE

In this ST the TOE is under development from phase 1 to phase 5 whereas in [PP/9911], the TOE is under development from phase 1 to phase 3. Therefore the assumptions on phase 4 and 5 are not necessary. Keeping these assumptions allows keeping the rationales of [PP/9911].

The ST security objectives and requirements are identical to those of the claimed PP [EEC/A1B] and [PP/9911].

2.4 PP REFINEMENTS

Refinements of [PP/BSI-0035] are described in [ST-IC] and are not repeated here.

The table below shows the functional requirements refined in PP and in ST.

PP / Security requirements	Refined in PP/9911	Refined in [EEC/A1B]	Refined in ST
FAU_SAA.1	_	**X**	**(X)**
FCO_NRO.1		**X**	**(X)**
FCS_CKM.1		**X**	**X**
FCS_CKM.2		**X**	**X**
FCS_CKM.3	_	**X**	**X**
FCS_CKM.4	_	**X**	**X**
FCS_COP.1	_	**X**	**X**
FDP_ACC.2	_	**X**	**X**
FDP_ACF.1	_	**X**	**X**
FDP_DAU.1	_	**X**	**(X)**
FDP_ETC.1	_		**X**
FDP_ETC.2		**X**	**(X)**
FDP_ITC.1	_		**X**
FDP_RIP.1	_		**X**
FDP_SDI.2	_	**X**	**X**
FIA_AFL.1	_	**X**	**(X)**
FIA_ATD.1	_	**X**	**(X)**
FIA_UAU.1	_	**X**	**(X)**
FIA_UAU.3	_	**X**	**(X)**
FIA_UAU.4	_	**X**	**(X)**
FIA_UID.1	_	**X**	**(X)**
FIA_USB.1	**NA**		**NA**
FMT_MOF.1	_		**X**

PP / Security requirements	Refined in PP/9911	Refined in [EEC/A1B]	Refined in ST
FMT_MSA.1	_		**X**
FMT_MSA.2	**NA**		**NA**
FMT_MSA.3	_		**X**
FMT_MTD.1	_		**X**
FMT_SMF.1	_		**X**
FMT_SMR.1	_		**X**
FPR_UNO.1	_		**X**
FPT_FLS.1	_	_	**X**
FPT_PHP.3	_		**X**
FPT_TDC.1	_		**X**
FPT_TST.1	_	**X**	**X**
FTP_ITC.1		**X**	**X**

Table 3. PP functional requirements that have been refined

The functional requirements are both refined in the claimed PP and in this ST. This section demonstrates the compatibility of the refinements done in both documents.

-: No refinement

(X): no additional refinement has been made in the ST.

X: Refinement

NA: the functional requirement requires no refinement.

The functional requirements are refined in this ST.

FAU_SAA.1: Potential violation analysis

This functional requirement has been refined as requested in [EEC/A1B] and no other refinement has been added in the ST.

FCO_NRO.1: Selective proof of origin

This functional requirement has been refined as requested in [EEC/A1B] and no other refinement has been added in the ST.

FCS_CKM.1: Cryptographic key generation

This functional requirement partially refined in [EEC/A1B] has been completed in the ST with a specific list of approved algorithms that gives the cryptographic key generation algorithms and key sizes used by the TOE.

FCS_CKM.2: Cryptographic key distribution

This functional requirement partially refined in [EEC/A1B] has been completed in the ST with a description of the key distribution method used that follows [no specific standard].

FCS_CKM.3: Cryptographic key access

This functional requirement partially refined in [EEC/A1B] has been completed in the ST with a description of the key access method used that follows [no specific standard].

FCS_CKM.4: Cryptographic key destruction

This functional requirement partially refined in [EEC/A1B] has been completed in the ST with a description of the key destruction method used that follows [no specific standard].

FCS_COP.1: Cryptographic operation

This functional requirement partially refined in [EEC/A1B] has been completed in the ST with a specific list of cryptographic algorithms and key sizes that are used by the TOE.

FDP_ACC.2: Complete access control

This functional requirement partially refined in [EEC/A1B] has been completed in the ST.

FDP_ACF.1: Security based access control functions

This functional requirement partially refined in [EEC/A1B] has been completed in the ST.

FDP_DAU.1: Basic data authentication

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FDP_ETC.1: Export of user data without security attributes

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the Card certificate SFP.

FDP_ETC.2: Export of user data with security attributes

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FDP_ITC.1: Import of user data without security attributes

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the VU Certificate SFP.

FDP_RIP.1: Subset residual information protection

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the Card private key.

FDP_SDI.2: Stored data integrity monitoring and action

This functional requirement partially refined in [EEC/A1B], with the actions to be taken, has been completed in the ST with the integrity checked stored data.

FIA_AFL.1: Basic authentication failure handling

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_ATD.1: User-attribute definition

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_UAU.1: Timing of authentication

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_UAU.3: Unforgeable authentication

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_UAU.4: Single-use authentication mechanism

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_UID.1: Timing of identification

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FIA_USB.1: User-subject binding

No refinement.

FMT_MOF.1: Management of security functions behavior

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the functions PIN Creation, Import card private key, generate card private key.

FMT_MSA.1: Management of security attributes

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with AC_SFP SFP.

FMT_MSA.2: Secure security attributes

There is no refinement required for this security requirement.

FMT_MSA.3: Static attributes initialization

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with AC_SFP SFP.

FMT_MTD.1: Management of TSF data

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the deletion of the Card private key.

FMT_SMF.1: Specification of Management functions

This functional requirement is a new dependency of FMT.MOF.1, FMT_MSA.1 and FMT_MTD.1 that are requested by [PP/9911]. In the ST, this SFR is refined with the following functions:

PIN Creation, Import card private key, Generate card private key, Read User data, Write Identification data, Write Activity data, Create File Structure.

FMT_SMR.1: Security roles

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the roles Issuer and User.

FPR_UNO.1: Unobservability

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the card holders and card issuers.

FPT_FLS.1: Failure with preservation of secure state

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FPT_PHP.3: Resistance to physical attacks

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the clock frequency, voltage tampering and penetration of protection layer.

FPT_TDC.1: Inter-TSF TSF basic data consistency

This functional requirement is only requested by [PP/9911]. In the ST, it is refined with the Card private key.

FPT_TST.1: TSF Testing

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added in the ST.

FTP_ITC.1: Inter-TSF trusted channel

This functional requirement is already refined in [EEC/A1B] and no other refinement has been added 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	Data type	Description
D.IC_DESIGN	TSF DATA	the IC specifications, design, development tools and technology
D.IC_CODE	TSF executable code	the IC Dedicated software
D.ES_CODE	TSF executable code	the Smart Card Embedded Software including specifications, implementation and related documentation
D.AP_DATA	USER DATA or TSF DATA	the application data of the TOE (such as IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data,)

The TOE itself is therefore an asset.

Assets have to be protected in terms of confidentiality, and integrity

Refinement:

D.AP_DATA can be refined as follows:

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

3.2 THREATS

A threat agent wishes to abuse the assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

Threats have to be split in:

- threats against which specific protection within the TOE is required (class I),

- threats against which specific protection within the environment is required (class II).

3.2.1 Threats from [PP/9911]

3.2.1.1 Unauthorized full or partial cloning of the TOE

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

3.2.1.2 Threats on phase 1

In CCV3 it is not possible to define threats along the development environment of the TOE. The Security Assurance Class ALC: Life Cycle Support and particularly DVS family is designed to check that all the security measures for protecting the confidentiality and the integrity of the TOE design and its implementation are taken.

By consequence the following threats are not included in this ST:

T.DIS_INFO, T.DIS_DEL, T.DIS_ES1, T.DIS_TEST_ES, T.T_DEL, T.T_TOOLS, T.T_SAMPLE2 , T_MOD_DEL, T.MOD.

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

Threats on data transmitted during the delivery process from the Smart Card developer to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.

These threats are described hereafter:

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

3.2.1.4 Threats on phases 4 to 7

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

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

Unauthorized disclosure of assets

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

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

Theft or unauthorized use of assets

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

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

Unauthorized modification of assets

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

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

3.2.2 Threats from [EEC/A1B]

TOE's assets may be attacked by:

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

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

3.2.3 Classification of Threats

Threats	Phase 1	Phase 4	Phase 5	Phase 6	Phase 7
T.CLON		Class I	Class I	Class I	Class I
T.DIS_DEL2		Class II	Class II	Class II	
T.DIS_ES2		Class I	Class I	Class I	Class I
T.T_ES		Class I	Class I	Class I	Class I
T.T_CMD		Class I	Class I	Class I	Class I
T.MOD_DEL2		Class II	Class II	Class II	
T.MOD_SOFT		Class I	Class I	Class I	Class I
T.MOD_LOAD		Class I	Class I	Class I	Class I
T.MOD_EXE		Class I	Class I	Class I	Class I
T.MOD_SHARE		Class I	Class I	Class I	Class I
T.Ident_Data				Class II	Class I & Class II
T.Activity_Data					Class I
T.Data_Exchange					Class I

- class I : threats against which specific protection within the TOE is required.
- class II : threats against which specific protection within the environment is required.

3.3 ASSUMPTIONS

3.3.1 Assumptions on phase 1

In CCV3 it is not possible to define assumptions during the development environment of the TOE. The Security Assurance Class ALC: Life Cycle Support and particularly DVS family is designed to check that all the security measures for protecting the confidentiality and the integrity of the TOE design and its implementation are taken.

By consequence the following assumptions are not included in this ST:

A.DEV_ORG

3.3.2 Assumptions on the TOE delivery process (phases 4 to 7)

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

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

Note: in [PP/9911], these assumptions also covered phase 4 and 5. The current TOE development include phase 4 and 5. Therefore the TOE is protected by objectives on the environment: O.DLV_PROTECT, O.DLV_AUDIT and O.DLV_RESP.

However, we keep the assumptions on phase 4 and 5 to keep the rationale of [PP/9911].

3.3.3 Assumptions on phases 4 to 6

Assumption name	Description
A.USE_TEST	It is assumed that appropriate functionality testing of the TOE is used in phases 4, 5 and 6.
A.USE_PROD	It is assumed that security procedures are used during all manufacturing and test operations through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

Note: in [PP/9911], these assumptions also cover phase 4 and 5. The current TOE development include phase 4 and 5. Therefore the TOE is protected by objectives on the environment: O.DLV_PROTECT, O.DLV_AUDIT and O.DLV_RESP.

However, we keep the assumptions on phase 4 and 5 to keep the rationale of [PP/9911].

3.3.4 Assumptions on phase 7

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

3.4 ORGANIZATIONAL SECURITY POLICIES

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

3.5 COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

3.5.1 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.DIS_ES2
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.DIS_ES2
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 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.DIS_ES2

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.DIS_ES2
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.DIS_ES2
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.DIS_ES2
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.DIS_ES2

3.5.2 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.

3.5.3 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 Personalisation	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 application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.		X		Fulfilled by the composite-SAR ADV_COMP.1 (cf [CCDB], Appendix 1.2, §72 and §73)
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		O.TAMPER_ES,O.CARD_ACTIVITY,O.CARD_IDENTIFICATION_DATA

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**		O.TAMPER_ES

4 SECURITY OBJECTIVES

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

- Integrity and confidentiality of assets,

- Protection of the TOE and associated documentation and environment during development and production phases.

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 Security objectives of [PP/9911]

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

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

4.1.2 Security objectives of [EEC/A1B]

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

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

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

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

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.2.1 Security objectives of [PP/9911]

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

Security Objectives	Description

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

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

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

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

4.2.1.3 Objectives on phases 4 to 6

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

4.2.1.4 Objectives on phase 7

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

4.2.2 Security objectives of [EEC/A1B]

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

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

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Objectives [PP/9911] vs. Threats- Assumptions - Policies [PP/9911]

The rationale of [PP/9911] section 8.2 demonstrates that the security objectives it specifies are suitable to counter all the identified threats, assumptions and organizational security policies it describes. This rationale is not repeated there.

4.3.2 Objectives [EEC/A1B] vs. Threats - Assumptions - Policies [EEC/A1B]

O.Card_Identification addresses the threat of unauthorized modification of identification data, T.Ident_Data.

O.Card_Activity_Storage & O.Data_Access address the threat of unauthorized modification of stored activity data, T.Activity_Data.

O.Secure_Communication addresses the threat of unauthorized modification of activity data during communication, T.Data_Exchange.

OE.Secret_Private_Key addresses the OSP on Secret keys and Private keys OSP.Secret_Private_Key.

OE.Qualified_Certificates_Key addresses the OSP on Certificates OSP.Qualified_Certificates.

	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication	OE.Secret_Private_Key	OE.Qualified_Certificates
T.Ident_Data	X					
T.Activity_Data		X	X			
T.Data_Exchange				X		
OSP.Secret_Private_Key					X	
OSP.Qualified_Certificates						X

We can conclude that the security objectives specified in [EEC/A1B] are suitable to counter all the identified threats it describes.

4.3.3 Objectives [PP/BSI-0035] vs. Threats - Assumptions - Policies [PP/BSI-0035]

The rationale for [PP/BSI-0035] is done in [ST-IC].

4.3.4 Objectives [PP/9911] vs. Threats- Assumptions - Policies [EEC/A1B]

Objectives of [PP/9911] vs. Threats of [EEC/A1B]	O.TAMPER_ES	O.CLON	O.OPERATE	O.FLAW	O.DIS_MECHANISM2	O.DIS_MEMORY	O.MOD_MEMORY						O.DLV_PROTECT – ph4-7	O.DLV_AUDIT – ph4-7	O.DLV_RESP – ph4-7	O.DLV_DATA – ph1->ph4-6	O.TEST_OPERATE – ph4-6	O.USE_DIAG – ph7
T.Ident_Data							**X**											
T.Activity_Data							**X**											
T.Data_Exchange																		**X**

T.Ident_Data & T.Activity_Data deal with the modification of information in the TOE. This threat is addressed by O.MOD_MEMORY

T.Data_Exchange deals with the security of communications with the TOE. This threat is addressed by O.USE_DIAG

4.3.5 Objectives [EEC/A1B] vs. Threats- Assumptions [PP/9911]

Objectives of [EEC/A1B]Vs. Threats of [PP/9911]	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
T.CLON				
T.DIS_DEL2 – ph1->ph4-6				
T.MOD_DEL2 – ph1->ph4-6				
T.DIS_ES2 – ph4-7				
T.T_ES – ph4-7				
T.T_CMD – ph4-7				
T.MOD_LOAD – ph4-7				
T.MOD_EXE – ph4-7				
T.MOD_SHARE – ph4-7				
T.MOD_SOFT – ph4-7	**X**	**X**	**X**	
A.DLV_PROTECT				
A.DLV_AUDIT				
A.DLV_RESP				
A.USE_TEST				
A.USE_PROD				
A.USE_DIAG				**X**

T.MOD_SOFT deals with the modification of information in the TOE. This threat is partly addressed by O.Card_Identification_Data, O.Card_Activity_Storage & O.Data_Access.

A.USE_DIAG deals with the communications. This assumption is partly addressed by O.Secure_Communication

4.3.6 Objectives [PP/9911] vs. Threats- Assumptions - Policies [PP/BSI-0035]

Threats - Assumptions - Policies [PP/BSI-0035] / Security objectives [PP/9911]	O.TAMPER_ES	O.CLON	O.OPERATE	O.FLAW	O.DIS_MECHANISM2	O.DIS_MEMORY	O.MOD_MEMORY	O.DEV_TOOLS - ph1	O.DEV_DIS_ES - ph1	O.SOFT_DLV - ph1	O.INIT_ACS - ph1	O.SAMPLE_ACS - ph1	O.DLV_PROTECT – ph4-7	O.DLV_AUDIT – ph4-7	O.DLV_RESP – ph4-7	O.DLV_DATA – ph1->ph4-6	O.TEST_OPERATE – ph4-6	O.USE_DIAG – ph4-6
T.Leak-Inherent	X				X	X												
T.Phys-Probing	X				X	X												
T.Malfunction	X						X											
T.Phys-Manipulation	X						X											
T.Leak-Forced	X				X	X												
T.Abuse-Func			X															
T.RND																		
A.Process-Card													X	X	X			
A.Plat-Appl																		
A.Resp-Appl											X							
P.Process-TOE																		

T.Leak-Inherent, T.Phys-Probing and T.Leak-Forced deal with leakage of information. These threats are addressed by O.TAMPER_ES, O.DIS_MECHANISM2 and O.DIS_MEMORY.

T.Malfunction & T.Phys-Manipulation deal with the modification of information. These threats are addressed by O.TAMPER_ES & O.MOD_MEMORY.

T.Abuse-Func deals with unauthorized use of functions. This threat is addressed by O.OPERATE.

A.Process-Card deals with environmental protection during phases 4 to 7. This assumption is addressed by O.DLV_PROTECT, O.DLV_AUDIT & O.DLV_RESP.

A.Resp-Appl deals with environmental protection of user data during phase 1. This assumption is addressed by O.INIT_ACS

P.Process-TOE deals with environmental protection during phases 2 & 3. This Policy is addressed by [ST-IC]

4.3.7 Objectives [PP/BSI-0035] vs. Threats- Assumptions [PP/9911]

Threats - Assumptions - Policies [PP/9911] / Security objectives [PP/BSI-0035]	O.Identification	O.Leak-inherent	O.Phys-Probing	O.Malfunction	O.Phys-	O.Leak-Forced	O.Abuse-Func	O.RND	OE.Plat-Appl	OE.Resp-Appl	OE.Process-	OE.Process-
T.CLON												
T.DIS_DEL2 – ph1->ph4-6										X		
T.MOD_DEL2 – ph1->ph4-6										X		
T.DIS_ES2 – ph4-7		X	X			X						X
T.T_ES – ph4-7							X					X
T.T_CMD – ph4-7							X					X
T.MOD_LOAD – ph4-7				X								X
T.MOD_EXE – ph4-7							X					X
T.MOD_SHARE – ph4-7												
T.MOD_SOFT – ph4-7					X							X
A.DEV_ORG – ph1												
A.DLV_PROTECT – ph4-7												X
A.DLV_AUDIT – ph4-7												X
A.DLV_RESP – ph4-7												X
A.USE_TEST – ph4-6												X
A.USE_PROD – ph4-6												X
A.USE_DIAG – ph7												

T.DIS_DEL2 & T.MOD_DEL2 deal with the protection of information during delivery from phase 1. These threats are addressed by OE.Resp-Appl.

T.DIS_ES2 deals with unauthorized disclosure during phases 4 to 7. This threat is addressed by O.Leak-inherent, O.Phys-Probing & O.Leak-Forced during phases 5 to 7.

T.T_ES, T.T_CMD, T.MOD_EXE deal with unauthorized use of assets during phases 4 to 7. These threats are addressed by O.Abuse-Func during phases 5 to 7, by OE.Process-TOE in phase 4.

T.MOD_LOAD deals with unauthorized loading of code during phases 4 to 7. This threat is addressed by O.Malfunction, OE.Process-CARD during phases 5 to 7.

T.MOD_SOFT deals with unauthorized modification of assets during phases 4 to 7. This threat is addressed by O.Phys-Manipulation and OE.Process-CARD during phases 5 to 7.

A.DLV_PROTECT, A.DLV_AUDIT, A.DLV_RESP, A.USE_TEST & A.USE_PROD deal with environmental protection during phases 4 to 6 or phases 4 to 7. These assumptions are addressed by OE.Process-Card during phases 5 to 7.

4.3.8 Objectives [EEC/A1B] vs. Threats- Assumptions - Policies [PP/BSI-0035]

Objectives of [EEC/A1B] Vs. Threats of [PP/BSI-0035]	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
T.Leak-Inherent				
T.Phys-Probing				
T.Malfunction	X	X	X	
T.Phys-Manipulation	X	X	X	
T.Leak-Forced				
T.Abuse-Func				
T.RND				
A.Plat-Appl				
A.Resp-Appl				
A.Process-Card				
P.Process-TOE				

T.Malfunction & T.Phys-Manipulation deal with unauthorized modification of assets during usage phase. These threats are partly addressed by O.Card_Identification_Data, O.Card_Activity_Storage & O.Data_Access

4.3.9 Objective [PP/BSI-0035] vs. Threats- Assumptions - Policies [EEC/A1B]

Threats - Assumptions - Policies [EEC/A1B] / Security objectives [PP/BSI-0035]	O.Identification	O.Leak-inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.RND	OE.Plat-Appl	OE.Resp-Appl	OE.Process-TOE	OE.Process-Card
T.Ident_Data				X	X							
T.Activity_Data				X	X							
T.Data_Exchange				X								

T.Ident_Data & T.Activity_Data deal with unauthorized modification of assets during usage phase. These threats are addressed by O.Malfunction & O.Phys-Manipulation.

T.Data_Exchange deals with unauthorized modification of assets during import or export. This threat is addressed by O.Malfunction.

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.	O.TAMPER_ES O.DIS_MEMORY
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) with a prior reverse-engineering to understand the design and its properties and functions.	O.TAMPER_ES O.CLONING
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.	O.TAMPER_ES O.OPERATE

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).	O.TAMPER_ES O.CLONING O.DIS_MECHANISM O.DIS_MEMORY
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.	O.TAMPER_ES O.DIS_MEMORY
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.	O.TAMPER_ES O.DIS_MECHANISM
O.Identification	TOE Identification	The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation 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.	O.OPERATE
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: O.TAMPER_ES, O.CARD_ACTIVITY, O.CARD_IDENTIFICATION, O.SECURE_COMMUNICATIONS, O.DATA_ACCESS
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). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately.	Fulfilled by ALC.DVS.2 and ALC_DEL.1 during phases 4 and 5. After phase 5, covered by O.USE_DIAG,OE.SECRET_PRIVATE_KEYS,OE.QUALIFIED_CERTIFICATE;
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 prepersonalization 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

No extended component defined in this ST.

6 SECURITY REQUIREMENTS

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP/9911] and [EEC/A1B].

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

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.3	Cryptographic key access
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
FMT	**Security management**

FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPR	**Privacy**
FPR_UNO.1	Unobservability
FPT	**Protection of the TOE Security Function**
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 4 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 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:

a) Accumulation or combination of **[audited events listed below]** known to indicate a potential security violation;

b) No other rules

Audited events:

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

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

From [PP/9911] "*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 Smart Card 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 **[User data]** at the request of the **[recipient].**
FCO_NRO.1.2	The TSF shall be able to relate the **[Public key]** of the originator of the information, and the **[User data]** of the information to which the evidence applies.
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to **[recipient]** given **[validity of the certificate].**

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

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 **[Triple DES key generation]** and specified cryptographic key sizes **[112 bits]** that meet the following **[A1B Session keys, cf. [EEC/A1B]]**
FCS_CKM.1.1 / Card private 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 / 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.3 Cryptographic key access

Hierarchical to: No other component

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

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	The TSF shall destroy cryptographic keys in accordance with a specified

A1B cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.

Note:

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

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/SIGN The TSF shall perform **[Digital signature generation and verification]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[1024 bits]** that meet the following**: [RSA SHA PKCS#1]**.

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/MAC The TSF shall perform **[MAC computation]** in accordance with a specified cryptographic algorithm **[TDES-CBC]** and cryptographic key sizes **[112 bits]** that meet the following**: [SP800-67] and [SP800-38 A]**.

FCS_COP.1.1/ENC The TSF shall perform **[Encryption and decryption]** in accordance with a specified cryptographic algorithm **[TDES-ECB]** and cryptographic key sizes **[112 bits]** that meet the following**: [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 SFP]** on **[**

Read User data by Owner,

Write Identification data by Issuer,

Write Activity data by Owner

Create File Structure by Issuer]

and all operations among subjects and objects covered by the SFP.

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 SFP]** to objects based on the following:

1. **Subjects: Issuer, Owner**
2. **Objects: Files structure and data, Software**
3. **User_Group security attribute**

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

User data may be read from the TOE by any user, except cardholder identification data, which may be read from control cards or company cards by VEHICLE_UNIT only.

Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle.

Activity data may be written to the TOE by VEHICLE_UNIT only.

No User may upgrade TOE's software

Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.

FDP_ACF.1.3/ AC_SFP SFP The TSF shall explicitly 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 [**any user]** 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 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 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 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"

1. Identification data
2. Activity data
3. Card private key
4. Euro public key

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **[integrity error]** on all objects, based on the following attributes: **[integrity checked stored data]**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **[warn the entity connected].**

Dependencies: No dependency

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 / Card interface A1B The TSF shall detect when **[*1*]** unsuccessful authentication attempts occur related to **[authentication of a card interface device in usage phase]**.

FIA_AFL.1.2 / Card interface A1B When the defined number of unsuccessful authentication attempts has been **met** , the TSF shall **[**

- **warn the entity connected**
- **assume the user as NON_VEHICLE_UNIT]**

FIA_AFL.1.1 / PIN check The TSF shall detect when **[*5*]** unsuccessful authentication attempts occur related to **[PIN check (workshop card)]**.

FIA_AFL.1.2 / PIN check When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[**

- **warn the entity connected**
- **block the PIN**
- **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_ID, USER_GROUP]**

Refinement:

USER_GROUP is either VEHICLE_UNIT or NON_VEHICLE_UNIT

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

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 / Driver & Workshop Cards The TSF shall allow **[Export user data with security attributes (card data download function)]** on behalf of the user to be performed before the user is authenticated.

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

Control & Company Cards

FIA_UAU.1.1/ Control & company Cards	The TSF shall allow **[Export user data without security attributes except cardholder identification data]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 / Control & company Cards	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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 **[any 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_ID, USER_GROUP.**
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 FMT: Security management

6.1.7.1 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other component

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

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

6.1.7.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

Hierarchical to: No other component

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

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.2 Secure security attributes

Hierarchical to: No other component

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

Dependencies:

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other component

FMT_MSA.3.1/ The TSF shall enforce the **[AC_SFP SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ The TSF shall allow the **[none]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

6.1.7.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

Hierarchical to: No other component

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

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

6.1.7.4 FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other component

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

Dependencies: No Dependency

6.1.7.5 FMT_SMR Security management roles

FMT_SMR.1 Security roles

Hierarchical to: No other component

FMT_SMR.1.1 The TSF shall maintain the roles **[Issuer]** and **[Owner]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.1.8 FPR:Privacy

6.1.8.1 FPR_UNO Unobservability

FPR_UNO.1 Unobservability

Hierarchical to: No other component

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

Dependencies: no dependency

6.1.9 FPT: Protection of the TSF

6.1.9.1 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: **[power cut-off or variations, unexpected reset].**

Dependencies: ADV_SPM.1 Informal TOE security policy model

6.1.9.2 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 **[clock frequency, voltage tampering and penetration of protection layer]** to the **[integrated circuit]** by responding automatically such that the SFRs are always enforced.

Dependencies: No dependency

6.1.9.3 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 **[Card private key]** when shared between the TSF and another trusted IT product.

FPT_ TDC.1.2 The TSF shall use **[Extract from message and decipher]** when interpreting the TSF data from another trusted IT product.

Dependencies: No dependency

6.1.9.4 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 stored TSF executable code.

Dependencies: No dependency

6.1.10 FTP: Trusted Path / Channel

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

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

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
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 5. 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.1	Testing : Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA	**Vulnerability assessment**
AVA_VAN.5	Methodical vulnerability analysis,

Table 6. 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.

6.3.1.1 Security Functional Requirements [PP/9911] vs. Objectives on the TOE [PP/9911]

The rationale of [PP/9911] section 8.3 demonstrates that the set of security functional requirements that it specifies is suitable to satisfy the related TOE security objectives. This rationale is not repeated here.

6.3.1.2 Security Functional Requirements [EEC/A1B] vs. Objectives on the TOE [EEC/A1B]

Objectives of [EEC/A1B] Vs. SFR of [EEC/A1B]	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
FAU_SAA.1				
FCO_NRO.1				X
FCS_CKM.1				X
FCS_CKM.2				X
FCS_CKM.3				
FCS_CKM.4				
FCS_COP.1				X
FDP_ACC.2	X	X	X	
FDP_ACF.1	X	X	X	
FDP_DAU.1				
FDP_ETC.2				X
FDP_SDI.2	X	X	X	
FIA_AFL.1			X	
FIA_ATD.1				
FIA_UAU.1				
FIA_UAU.3			X	
FIA_UAU.4			X	
FIA_UID.1				
FPT_FLS.1				
FPT_TST.1				
FTP_ITC.1				X

O.Card_Identification_Data

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions, FDP_SDI.2: Stored data integrity monitoring and action contribute to the security of identification data stored during card personalization process.

O.Card_Activity_Storage

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions,FDP_SDI.2: Stored data integrity monitoring and action contribute to the security of user data stored by the vehicle unit.

O.Data_Access

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions,FDP_SDI.2: Stored data integrity monitoring and action, FIA_AFL.1: Authentication Failure Handling, FIA_UAU.3: Unforgeable authentication, FIA_UAU.4: Single-use authentication mechanisms contribute to limit user data write Access Rights to authenticated vehicle units.

O.Secure_Communication

FCO_NRO.1: Selective proof of origin, FCS_CKM.1: Cryptographic key generation, FCS_CKM.2: Cryptographic key distribution, FCS_COP.1: Cryptographic operations, FDP_ETC.2: Export of user data with security attributes, FTP_ITC.1: Inter-TSF trusted channel contribute to the security of communications.

6.3.1.3 Security Functional Requirements [PP/BSI-0035] vs.TOE Objectives [PP/BSI-0035]

The rationale for [PP/BSI-0035] is done in [ST-IC].

6.3.1.4 Security Functional Requirements [PP/9911] vs. TOE Objectives [EEC/A1B]

Objectives of [EEC/A1B] Vs. SFR of [PP/9911]	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
FAU_SAA.1				
FCS_CKM.3				
FCS_CKM.4				
FCS_COP.1				X
FDP_ACC.2	X	X	X	
FDP_ACF.1	X	X	X	
FDP_DAU.1				
FDP_ETC.1				X
FDP_ITC.1				
FDP_RIP.1				
FDP_SDI.2	X	X		
FIA_AFL.1				
FIA_ATD.1				
FIA_UAU.1				
FIA_UAU.3				
FIA_UAU.4				
FIA_UID.1				
FIA_USB.1				
FMT_MOF.1				
FMT_MSA.1				
FMT_MSA.2				
FMT_MSA.3				
FMT_MTD.1				
FMT_SMR.1				
FPR_UNO.1				
FPT_FLS.1	X	X		
FPT_PHP.3				

Objectives of [EEC/A1B] Vs. SFR of [PP/9911]	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
FPT_TDC.1				
FPT_TST.1				

O.Card_Identification_Data

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions, FDP_SDI.2: Stored data integrity monitoring and action, FPT_FLS.1: Failure with preservation of secure state contribute to the security of identification data stored during card personalization process.

O.Card_Activity_Storage

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions, FDP_SDI.2: Stored data integrity monitoring and action, FPT_FLS.1: Failure with preservation of secure state contribute to the security of user data stored by the vehicle unit.

O.Data_Access

FDP_ACC.2: Complete access control, FDP_ACF.1: Security based access control functions contribute to limit user data write Access Rights to authenticated vehicle units.

O.Secure_Communication

FCS_COP.1: Cryptographic operations, FDP_ETC.1: Export of user data without security attributes contribute to the security of communications.

6.3.1.5 *Security Functional Requirements [EEC/A1B] vs. TOE Objectives [PP/9911]*

Objectives of [PP/9911] vs. SFR of [EEC/A1B]	O.TAMPER_ES	O.CLON	O.OPERATE	O.FLAW	O.DIS_MECHANISM2	O.DIS_MEMORY	O.MOD_MEMORY
FAU_SAA.1			**X**				
FCO_NRO.1							
FCS_CKM.1	**X**						
FCS_CKM.2	**X**						
FCS_CKM.3							
FCS_CKM.4							
FCS_COP.1							
FDP_ACC.2							
FDP_ACF.1							
FDP_DAU.1							
FDP_ETC.2							
FDP_SDI.2	**X**						**X**
FIA_AFL.1							
FIA_ATD.1							
FIA_UAU.1							
FIA_UAU.3							
FIA_UAU.4							
FIA_UID.1							
FPT_FLS.1	**X**		**X**				
FPT_TST.1	**X**		**X**				
FTP_ITC.1							

O.TAMPER_ES:
FCS_CKM.1 Cryptographic key generation, FCS_CKM.2 Cryptographic key distribution,

FDP_SDI.2: Stored Data Integrity Monitoring and Action, FPT_FLS.1 Failure with preservation of secure state,

O.OPERATE:

FAU_SAA.1: Potential violation analysis, FPT_FLS.1 Failure with preservation of secure state,

O.MOD_MEMORY:

FDP_SDI.2: Stored Data Integrity Monitoring and Action contributes to prevent unauthorised modifications

6.3.1.6 Security Functional Requirements [PP/9911] vs. TOE Objectives [PP/BSI-0035]

Objectives of [PP/BSI-0035] Vs. SFR of [PP/9911]	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification	O.RND
FAU_SAA.1								
FCS_CKM.3								
FCS_CKM.4								
FCS_COP.1		X						
FDP_ACC.2						X	X	
FDP_ACF.1						X	X	
FDP_DAU.1								
FDP_ETC.1								
FDP_ITC.1								
FDP_RIP.1		X			X			
FDP_SDI.2			X	X				
FIA_AFL.1								
FIA_ATD.1								
FIA_UAU.1								
FIA_UAU.3								
FIA_UAU.4								
FIA_UID.1								
FIA_USB.1								
FMT_MOF.1								
FMT_MSA.1								
FMT_MSA.2								
FMT_MSA.3								
FMT_MTD.1								
FMT_SMR.1								
FPR_UNO.1	X							
FPT_FLS.1								

Objectives of [PP/BSI-0035] Vs. SFR of [PP/9911]	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification	O.RND
FPT_PHP.3		X		X	X			
FPT_TDC.1								
FPT_TST.1			X	X				

O.Leak_Inherent (Protection against Inherent Information Leakage) provides protection against disclosure of critical data by measurement and analysis of signals. This objective is met by FPR_UNO.1, which requires the prevention of secret data.

O.Phys-Probing (Protection against Physical Probing) provides protection against disclosure of critical data by mere measurement. This objective is met by the encryption of FCS_COP, by the unavailability of FDP_RIP.1 & by the physical protection of FPT_PHP.3.

O.Malfunction (Protection against Malfunctions) provides protection against disclosure of critical data or dysfunction through changes of environmental conditions. This objective is met by FDP_SDI.2, which watches the integrity of data. This objective is also met by FPT_TST.1, which tests the TOE.

O.Phys-Manipulation (Protection against Physical Manipulation) provides protection against disclosure of critical data or dysfunction du to manipulation of the TOE. This objective is met by the same SFR as those that meet O.Malfunction. This objective is also met by FPT_PHP.3, which deals with the physical protection of the TOE.

O.Leak-Forced (Protection against Forced Information Leakage) provides protection against disclosure of critical data caused by an attacker. This objective is met by FDP_RIP.1, which protects sensitive data. This objective is also met by FPT_PHP.3, which deals with the physical protection of the TOE.

O.Abuse-Func (Protection against Abuse of Functionality) provides protection against unauthorized use of functions. FDP_ACC.2 & FDP_ACF.1 meet this objective by checking that functions are executed in the right phase.

O.Identification (TOE Identification) provides a means to store identification data. FDP_ACC.2 & FDP_ACF.1 meet this objective with the Identity Init SFP.

6.3.1.7 Security Functional Requirements [PP/BSI-0035] vs. TOE Objectives [PP/9911]

TOE Security objectives of [PP/9911] Vs. SFR of [PP/BSI-0035]	O.TAMPER_ES	O.OPERATE	O.DIS MECHANISM2	O.DIS MEMORY	O.MOD MEMORY	O.FLAW	O.CLON
FAU_SAS.1							
FCS_RND.1							
FDP_ITT.1							
FDP_IFC.1				X	X		
FMT_LIM.1		X					
FMT_LIM.2		X					
FPT_FLS.1		X					
FPT_ITT.1							
FPT_PHP.3	X			X	X		
FRU_FLT.2		X					

O.TAMPER_ES provides protection against modification of security attributes. This objective is met by the physical protection of FPT_PHP.3.

O.OPERATE ensures continued correct operations. This objective is met by FMT_LIM.1, FMT_LIM.2, FPT_FLS.1 & FRU_FLT, which ensures that that the TOE works correctly inside its normal conditions & that the TOE behaves safely when the normal conditions are not met.

O.DIS_MEMORY & O.MOD_MEMORY provide protection against disclosure & modification in memory. These objectives are met by the physical protection of FPT_PHP.3 and by the flow control policy FDP_IFC.1.

6.3.1.8 Security Functional Requirements [EEC/A1B] vs. TOE Objectives [PP/BSI-0035]

TOE Security objectives of [PP/BSI-0035] Vs. SFR of [EEC/A1B]	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification	O.RND
FAU_SAA.1								
FCO_NRO.1								
FCS_CKM.1								
FCS_CKM.2								
FCS_CKM.3								
FCS_CKM.4								
FCS_COP.1		X						
FDP_ACC.2						X	X	
FDP_ACF.1						X	X	
FDP_DAU.1								
FDP_ETC.2								
FDP_SDI.2			X	X				
FIA_AFL.1								
FIA_ATD.1								
FIA_UAU.1								
FIA_UAU.3								
FIA_UAU.4								
FIA_UID.1								
FPT_FLS.1								
FPT_TST.1			X	X				
FTP_ITC.1								

O.Phys-Probing (Protection against Physical Probing) provides protection against disclosure of critical data by mere measurement. This objective is met by the encryption of FCS_COP.

O.Malfunction (Protection against Malfunctions) provides protection against disclosure of critical data or dysfunction through changes of environmental conditions. This objective is met by FDP_SDI.2, which watches the integrity of data. This objective is also met by FPT_TST.1, which tests the TOE.

O.Phys-Manipulation (Protection against Physical Manipulation) provides protection against disclosure of critical data or dysfunction du to manipulation of the TOE. This objective is met by the same SFR as those that meet O.Malfunction.

O.Abuse-Func (Protection against Abuse of Functionality) provides protection against unauthorized use of functions. FDP_ACC.2 & FDP_ACF.1 meet this objective by checking that functions are executed in the right phase.

O.Identification (TOE Identification) provides a means to store identification data. FDP_ACC.2 & FDP_ACF.1 meet this objective with the Identity Init SFP.

6.3.1.9 Security Functional Requirements [PP/BSI-0035] vs. TOE Objectives [EEC/A1B]

TOE Security Functional Requirement / TOE Security objectives	O.Card_Identification_Data	O.Card_Activity_Storage	O.Data_Access	O.Secure_Communication
FAU_SAS.1				
FCS_RND.1				
FDP_ITT.1				
FDP_IFC.1	**X**	**X**	**X**	**X**
FMT_LIM.1				
FMT_LIM.2				
FPT_FLS.1				
FPT_ITT.1				
FPT_PHP.3	**X**	**X**		
FRU_FLT.2				

O.Card_Identification_Data protects against the modification of stored data. This objective is met by the physical protection of PFT_PHP.3 and by the flow control policy FDP_IFC.1.

O.Card_Activity_Storage protects against the modification of stored data. This objective is met by the physical protection of PFT_PHP.3 and by the flow control policy FDP_IFC.1.

O.Data_Access protects against the modification of stored data. This objective is met by the flow control policy FDP_IFC.1.

O.Secure_Communication provides secure communications. This objective is met by FDP_IFC.1.

These rationales are sufficient for the ST rationale, as there is no additional TOE security objective and no additional functional requirement to these PP in this ST.

6.3.2 DEPENDENCIES

6.3.2.1 SFRs dependencies

Requirements	CC dependencies	Satisfied dependencies
FAU_SAA.1	FAU_GEN.1	unsupported
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.3	(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	(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	FDP_ACC.1. FMT_MSA.3	FDP_ACC.2/AC_SFP SFP, FMT_MSA.3
FDP_DAU.1	none	
FDP_ETC.1	(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, FMT_MSA.3
FDP_RIP.1	none	
FDP_SDI.2	none	
FIA_AFL.1/ interface GP	FIA_UAU.1	FIA_UAU.1/Drivers & Workshop Cards FIA_UAU.1/Control & Company Cards
FIA_AFL.1/ interface A1B	FIA_UAU.1	FIA_UAU.1/Drivers & Workshop Cards FIA_UAU.1/Control & Company Cards
FIA_AFL.1/ PIN	FIA_UAU.1	FIA_UAU.1/Drivers & Workshop Cards FIA_UAU.1/Control & Company Cards
FIA_ATD.1	none	
FIA_UAU.1/Drivers & Workshop Cards	FIA_UID.1	FIA_UID.1
FIA_UAU.1/ Control & Company Cards	FIA_UID.1	FIA_UID.1
FIA_UAU.3	none	
FIA_UAU.4	none	
FIA_UID.1	none	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1

Requirements	CC dependencies	Satisfied dependencies
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	(FDP_ACC.1 or FDP_IFC.1), FMT_SMF.1, FMT_SMR.1	FDP_ACC.2/AC_SFP SFP , FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1), FMT_MSA.1, FMT_SMR.1	FDP_ACC.2/AC_SFP SFP , FMT_SMA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_SMA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	none	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPR_UNO.1	none	
FPT_FLS.1	none	
FPT_PHP.3	none	
FPT_TDC.1	none	
FPT_TST.1	none	
FTP_ITC.1	none	

6.3.2.2 Rational for the exclusion of dependencies

The dependency FAU_GEN.1 of FAU_SAA.1 is unsupported.
From [PP/9911] “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 Smart Card 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. »

6.3.3 Assurance measures rationale

6.3.3.1.1 ADV Development

ADV_ARC: Security architecture description

ADV_ARC.1 done in [ARC_PHAESTOS3].

ADV_FSP: Complete functional specification

ADV_FSP.4 done in [FSP_PHAESTOS3].

ADV_IMP: Implementation representation of the TSF

ADV_IMP.1 done in [IMP_PHAESTOS3].

ADV_TDS: Basic modular design

ADV_TDS.3 done in [TDS_PHAESTOS3].

6.3.3.1.2 AGD Guidance documents

AGD_OPE: Operational user guidance

AGD_OPE.1 done in [OPE_PHAESTOS3].

AGD_PRE: Preparative procedures

AGD_PRE.1 done in [PRE_PHAESTOS3].

6.3.3.1.3 ALC Life cycle support

ALC_ CMC: Production support, acceptance procedures and automation

ALC_ CMC.4 done in [CMC_PHAESTOS3].

ALC_ CMS: Problem tracking CM coverage

ALC_ CMS.4 done in [CMS_PHAESTOS3].

ALC_ DVS: Identification of security measures

ALC_DVS.2 done in [DVS_PHAESTOS3].

ALC_ DEL: Delivery procedures

ALC_DEL.1 done in [DEL_PHAESTOS3].

ALC_ LCD: Developer defined life-cycle model

ALC_LCD.1 done in [LCD_PHAESTOS3].

ALC_ TAT: Well-defined development tools

ALC_TAT.1 done in [TAT_PHAESTOS3].

6.3.3.1.4 ATE Tests

ATE_COV: Coverage

ATE_COV.2 done in [COV_PHAESTOS3].

ATE_DPT Testing: security enforcing modules

ATE_DPT.1 done in [DPT_PHAESTOS3].

ATE_FUN: Functional tests

ATE_FUN.1 done in [FUN_ PHAESTOS3].

ATE_IND: Independent testing

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

6.3.3.1.5 AVA Vulnerability assessment

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[1]-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.

[1] 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 / ENC FCS_COP.1 / 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. 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.	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 / MEM	The TSF shall enforce the Access Control Policy to restrict the ability to modify the security attributes Special Function Registers to configure the MMU segmentation to code executed in the System Mode.		X		FPT_TST.1
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 modification of the Special Function Registers containing security attributes, and modification of the MMU Segment Table.		**X**		FPT_TST.1
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 [EEC/A1B], 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