oberthur TECHNOLOGIES
THE M COMPANY

ID One Tachograph

Public security target

Table of contents

LIST OF FIGURES 4

LIST OF TABLES 5

1 INTRODUCTION 6

1.1 SECURITY TARGET REFERENCE 6
1.2 REFERENCES 6
1.3 DEFINITIONS 8

2 TARGET OF EVALUATION DESCRIPTION 9

2.1 TARGET OF EVALUATION OVERVIEW 9
2.1.1 TOE type 9
2.1.2 Logical scope 10
2.1.3 Physical scope 11
2.1.4 Required non-TOE hardware/software/firmware 12
2.1.5 Usage and major security features of the TOE 12
2.1.6 Scope of evaluation 13
2.2 TARGET OF EVALUATION REFERENCE 14
2.3 LIFE CYCLE 14
2.3.1 Development environment 15
2.3.2 Production environment 17
2.3.3 Operational environment 18
2.3.4 Coverage of the different Life Cycle state by the assurance components AGD & ALC 18
2.3.5 TOE State depending on the phase 19
2.3.6 Mapping with the life cycle described in [16] 20
2.3.7 Link with PP life cycle 21
2.4 CONFORMANCE CLAIM 22
2.5 PROTECTION PROFILE REFERENCE 22

3 SECURITY PROBLEM DEFINITION 24

3.1 ASSETS 24
3.2 USERS / SUBJECTS 25
3.3 THREATS 26
3.3.1 Phase 6 26
3.3.2 Phase 7 26
3.4 ORGANISATIONAL SECURITY POLICIES 27
3.5 ASSUMPTIONS 27

4 SECURITY OBJECTIVES 29

4.1 SECURITY OBJECTIVES FOR THE TOE 29
4.1.1 Phase 6 29
4.1.2 Phase 7 29
4.1.3 Phase 6 and 7 30

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 30
4.2.1 Phase 6 30
4.2.2 Phase 7 31
4.3 SECURITY OBJECTIVES RATIONALE 31
4.3.1 Threats 31
4.3.2 Organisational Security Policies 32
4.3.3 Assumptions 32
4.3.4 SPD and Security Objectives 32
5 EXTENDED REQUIREMENTS 35
5.1 EXTENDED FAMILIES 35
5.1.1 Extended Family FPT_EMS - TOE Emanation 35
5.1.2 Extended Family FCS_RNG - FCS_RNG: Random Number Generation 36
6 SECURITY REQUIREMENTS 37
6.1 SECURITY FUNCTIONAL REQUIREMENTS 37
6.1.1 SFR from the Tachograph Protection Profile 39
6.1.2 Additional SFR 51
6.2 SECURITY ASSURANCE REQUIREMENTS 56
6.2.1 Rationale for composition with Security Assurance Package E3hCC31_AP 56
6.2.2 Rationale for composition with ALC_DVS.2 57
7 TOE SUMMARY SPECIFICATION 58
7.1 TOE SUMMARY SPECIFICATION 58
INDEX 62

List of figures

Figure 1: Tachograph Cards 10
Figure 2: CALLIOPE Architecture 11
Figure 3: CALLIOPE life cycle 15

List of tables

Table 1: Life cycle phase coverage 19
Table 2: TOE state following the life cycle phase 19
Table 3: TOE state following the PP life cycle 20
Table 4: Interaction of subjects with the TOE 20
Table 5: Specific case of PP life cycle phase 6 21

1 Introduction

1.1 Security Target Reference

The Security Target is identified as follows:

Title	CALLIOPE – ASE - Public Security Target
Reference	110 6350
Edition	5
Date	25/03/2015
Editor	Oberthur Technologies
CC version	3.1 revision 3
EAL	EAL4, augmented with: - ATE_DPT.2 - AVA_VAN.5 - ALC_DVS.2
ITSEF	UL
Certification Body	CESG
Evaluation scheme	UK

1.2 References

	References
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009
[4]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2009-07-004, Version 3.1, Revision 3, July 2009
[5]	Annex I(B) of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)
[6]	Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No.3821/85 on recording equipment in road transport, Official Journal of the European Communities L 71-86, 13.03.2004
[7]	Appendix 2 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] – Tachograph Cards Specification

	References
[8]	Appendix 10 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] - Generic Security Targets
[9]	Appendix 11 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] -Common Security Mechanisms
[10]	Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1(B), Version 1.12, June 2003
[11]	RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003
[12]	Security IC Platform Protection Profile, BSI-CC-PP-0035, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0035-2007
[13]	Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806
[14]	Smartcard Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 1999. Registered at French certification body under the number PP/9911
[15]	Common Criteria ProtectionProfile Machine Readable Travel Document with „ICAO Application", Extended Access Control, Version 1.10, 25th March 2009; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0056
[16]	Digital Tachograph – Smart card (Tachograph Card) – BSI-CC-PP-0070
[17]	JIL - Composite product evaluation for Smart Cards and similar devices v1.2
[18]	FQR 110 5592 – Tachograph Javacard Applet – circulation List
[19]	Security IC Platform Protection Profile - BSI-PP-0035
[20]	Rapport de certification ID-One Cosmo v7.0.1-n Standard ANSSI-CC-2012/30
[21]	AGD PRE document for CALLIOPE FQR 110 6199 Ed 1 – CALLIOPE – AGD_PRE
[22]	AGD OPE document for CALLIOPE FQR 110 6217 Ed 2 – CALLIOPE – AGD_OPE
[23]	AGD PRE document for Cosmo v.7.0.1 Standard FQR 110 4910 Ed 7 – TERPSICHORE – AGD_PRE
[24]	AGD OPE document for Cosmo v.7.0.1 Standard FQR 110 4911 Ed 4 – TERPSICHORE – AGD_OPE
[25]	AGD OPE Security recommandations for Cosmo v.7.0.1 Standard FQR 110 4912 Ed 4 – TERPSICHORE – AGD_OPE – Security recommandations
[26]	Application Note 10 from ANSSI
[27]	Application of Attack Potential to smartcards v2.8 – JIL document – January 2012
[28]	AGD OPE document for Cosmo v.7.0.1 Standard FQR 110 6249 Ed 2 – Guidance for compatibility Application Note 10
[29]	AGD OPE document for Cosmo v.7.0.1 Standard FQR 110 6303 Ed 1 - Security guidance for compatibility Application Note 10
[30]	AGD OPE document for Cosmo v.7.0.1 Standard FQR 110 6325 Ed 1 - Applications on ID-One Cosmo V7.0.1

1.3 Definitions

Elements	Definition
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 as defined by requirements 190, 191, 192, 194, 215, 231 and 235
Cardholder activities data	User data related to the activities carried by the cardholder as defined by requirements 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 and 237
Cardholder identification data	User data related to cardholder identification as defined by requirements 195, 196, 216, 232 and 236
Control activity data	User data related to law enforcement controls as defined by requirements 210 and 225
DFA	Differential Fault Analysis, side-channel attack type
Digital Tachograph	Recording equipment
Events and faults data	User data related to events or faults as defined by requirements 204, 205, 207, 208 and 223
Identification data	Identification data include card identification data and cardholder identification data
JOP	Java Card Open Platform, certified in accordance with a Java Card protection profile and conformant to ANSSI-note 10 [26]
Security data	The specific data needed to support security enforcing functions (eg. crypto keys)
Sensitive data	Data stored by the tachograph card that need to be protected for integrity, unauthorized modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data
System	Equipment, people or organizations involved in any way with the recording equipment

2 Target Of Evaluation description

2.1 Target Of Evaluation Overview

2.1.1 TOE type

The TOE is compliant with the Tachograph Protection Profile. The Personalisation has been added in the scope of the evaluation.

The TOE is a smart card, the Tachograph Card, which is configured and implemented as a driver card, workshop card, control card or company card in accordance with the specification documents Annex I(B) body text [5], [6], Appendix 2 [7], Appendix 10 [8] and Appendix 11 [9]. In particular, this implies the conformance with the standards:

- ISO/IEC 7816 Identification cards – Integrated circuits with contacts (Part 1, Part 2, Part 3, Part 4 and Part 8)

CALLIOPE is a single product that is personalized after its delivery point as one of those four Tachograph Card Types:

- driver card
- workshop card
- control card
- company card

The Tachograph card is a composite product, composed of the Tachograph applet that is embedded on a Java Card Open Platform.
The Java Card Open Platform has been evaluated under the French Scheme [20].

The Tachograph card is conformant to:

COMMISSION REGULATION (EC) No 1360/2002

of 13 June 2002

adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport

(Text with EEA relevance)

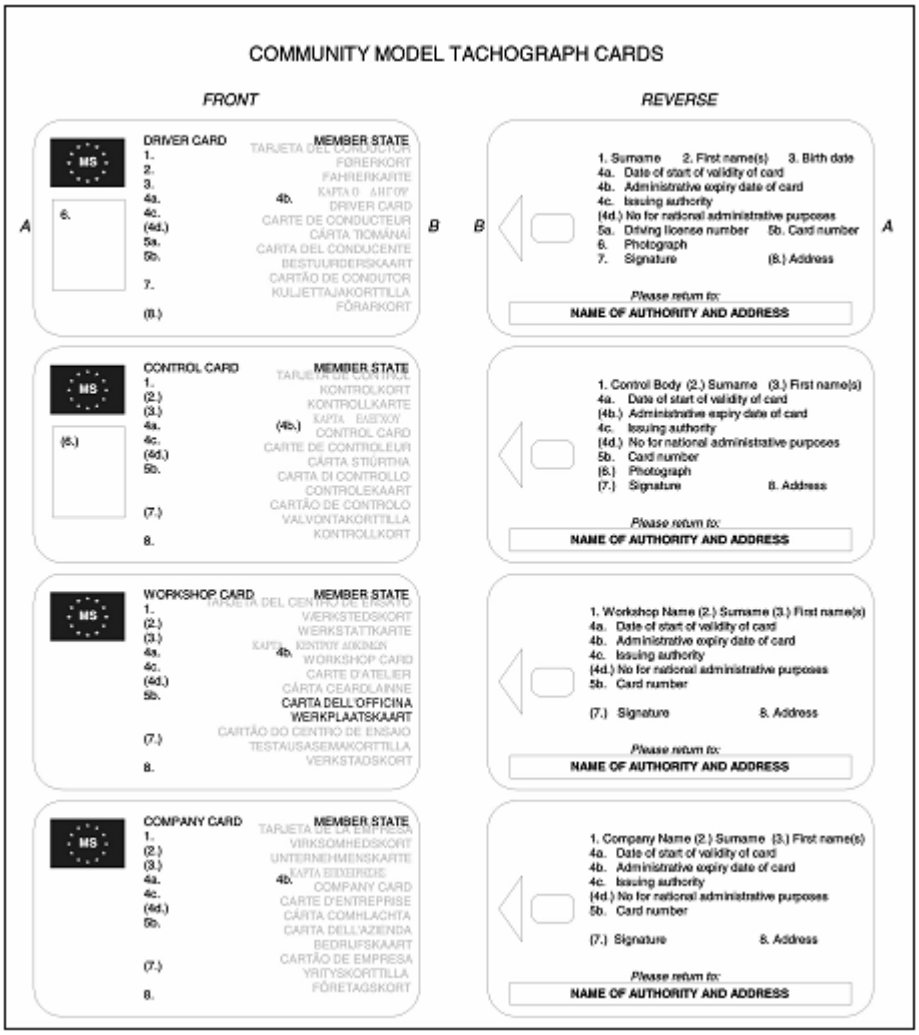

Figure 1: Tachograph Cards

2.1.2 Logical scope

As the underlying Javacard Open Platform is certified as a Javacard Open Platform, known applets of the underlying Javacard Open Platform may be used with the chronotachygraph applet (the list is indicated in [30]).

The tachograph applet fulfils the recommendations indicated in the guidance documentation of the Javacard Open Platform ([23], [24] and [25]).

The logical scope of the TOE may be depicted as follows:

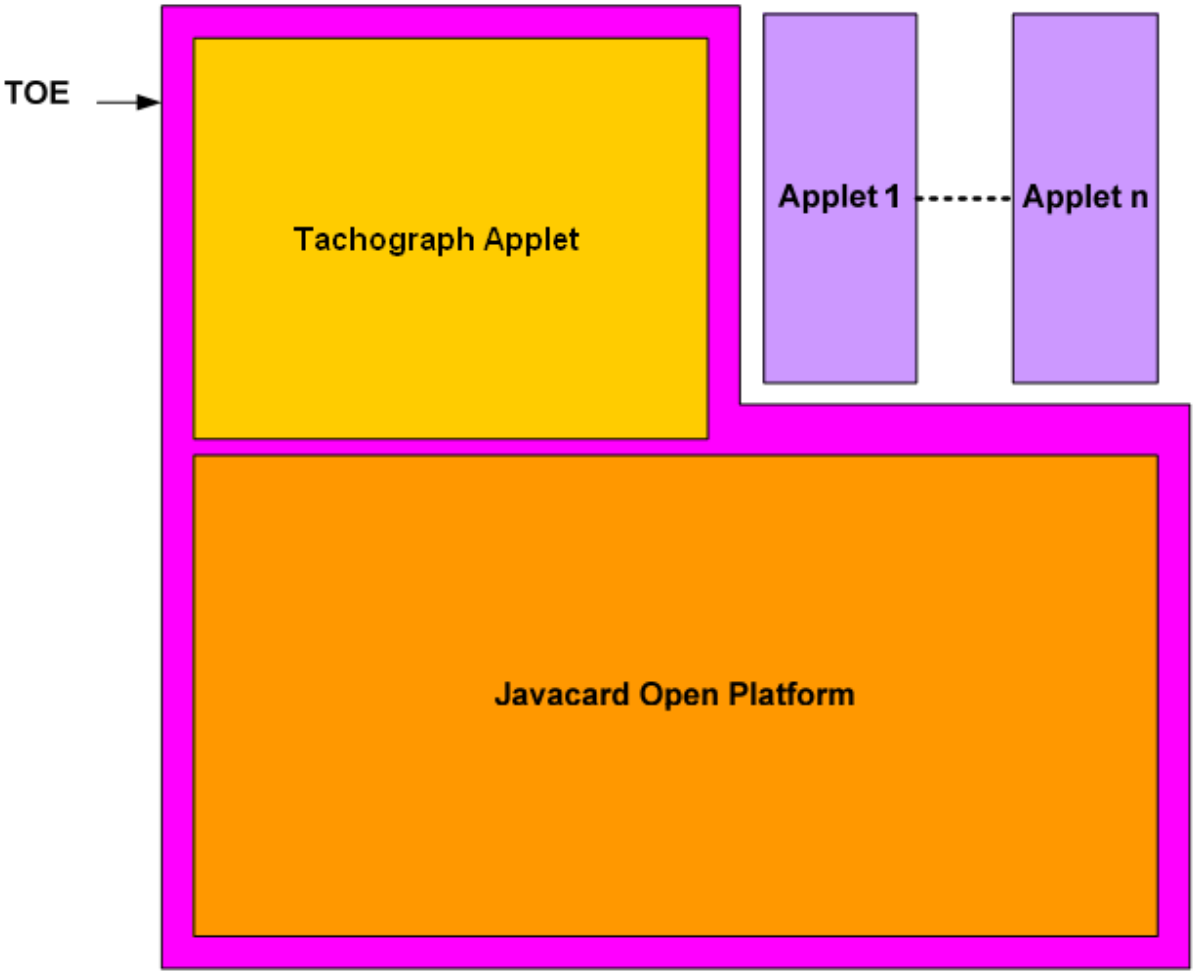

Figure 2: CALLIOPE Architecture

2.1.3 Physical scope

The TOE is made of the following part:

- The javacard open platform, identified in the following as [JOP], whose references are indicated in [20]
- The javacard package that is loaded in EEPROM and instanciated, identified in the following as 'Applet'

The javacard open platform [JOP] is self protected as it requires the authentication of its user prior to any action.

2.1.3.1 Physical overview

Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.

2.1.4 Required non-TOE hardware/software/firmware

The TOE is the Tachograph Card (contact based smart card). It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate the TOE needs a card reader (integrated in the Vehicle Unit or connected to another device, e.g. a personal computer).

2.1.5 Usage and major security features of the TOE

Described in chapter § 1.2.2 of [16], the main security features of the TOE are:

- The TOE must preserve card identification data and cardholder identification data stored during card personalisation process
- The TOE must preserve user data stored in the card by Vehicle Units

Specifically the Tachograph Card aims at protecting:

- the data stored in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,
- the integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

The main security features stated above are provided by the following major security services (please refer to [8], chap. 4):

- User and Vehicle Unit identification and authentication,
- Access control to functions and stored data,
- Accountability of stored data,
- Audit of events and faults,
- Accuracy of stored data,
- Reliability of services,
- Data exchange with a Vehicle Unit and export of data to a non-Vehicle Unit,
- Cryptographic support for ‘identification and authentication’ and ‘data exchange’ as well as for key generation and distribution in corresponding case according to [9], sec. 4.9.

All cryptographic mechanisms including algorithms and the length of corresponding keys are implemented exactly as required and defined in EU documents [8] and [9].
The Security Functions provided by the TOE are the following ones:

- Access control in reading
- Access control in writing
- Authentication during phase 7
- Clearing of sensitive information

- Data recording
- Errors messages and exceptions
- Key management
- Signature
- Administrator Authentication (phase 6)
- Physical protection
- Safe state management
- Secure messaging
- Self tests

Depending on the use case and on the ability of the underlying javacard open platform, this embedded software may be used

- in contact mode (T=0 and/or T=1 protocol)
- in contactless protocol (T=CL)
- in USB protocol

2.1.6Scope of evaluation

The scope of evaluation encompasses all the features of the TOE:

- the File System management is part of the scope of the evaluation;
- the access control management is covered.
- Key management and generation are included in the scope;
- Personalization has been added in the scope of the TOE (regarding [16]);

2.2 Target Of Evaluation Reference

The TOE is identified as follows:

TOE name (commercial name)	**ID-One Tachograph**
Name of [JOP]	Cosmo V7.0.1-n
PTF certificates	ANSSI-CC-2012/30
Guidance document for preparation	FQR 110 6199 Ed 1 – CALLIOPE – AGD_PRE
Guidance document for use	FQR 110 6217 Ed 2 – CALLIOPE – AGD_OPE
Guidance document for preparation of [JOP]	FQR 110 4910 Ed 7 – TERPSICHORE – AGD_PRE
Guidance document for operational user of [JOP]	FQR 110 4911 Ed 4 – TERPSICHORE – AGD_OPE
	FQR 110 4912 Ed 4 – TERPSICHORE – AGD_OPE – Security recommandations
	FQR 110 6249 Ed 2 – TERPSICHORE – AGD_OPE – Guidance for compatibility Application Note 10
	FQR 110 6303 Ed 1 – TERPSICHORE – AGD_OPE - Security guidance for compatibility Application Note 10
	FQR 110 6325 Ed 1 – TERPSICHORE – AGD_OPE - Applications on ID-One Cosmo V7.0.1
TOE identification (answer to GET DATA DF 67)	“00 00 00 25”

Name of [Applet]	Tachograph Javacard Applet
Internal identification	P11-08 – Tachograph Card\07670x – Tachograph Javacard Applet
Configuration management (PVCS) label	“076702”

2.3 Life cycle

With respect to the smartcard life-cycle, divided in 7 phases and according to the IC protection profile [19], the TOE life cycle is divided in seven different phases.
The TOE is an applet embedded on a Java Card Open Platform. The underlying platform is conformant to the [19] smartcard life cycle, and the TOE is also conformant to the [19] smartcard lifecycle.

As described in paragraph 52-55 of the Tachograph PP [16], the TOE environment is separated into the following parts:

- **Development environment:**
  TOE parts are designed, tested and manufactured
- **Production environment:**
  TOE is under contruction. The security requirements of the javacard open platform (JOP) are fulfilled and assurance levels are met
- **Operational environment:**
  TOE is self protected and can be used as stated (personalized and used). Once personalized according to [AGD_PRE], the TOE is constructed: the security requirements of the TOE are fulfilled and the assurance levels are met

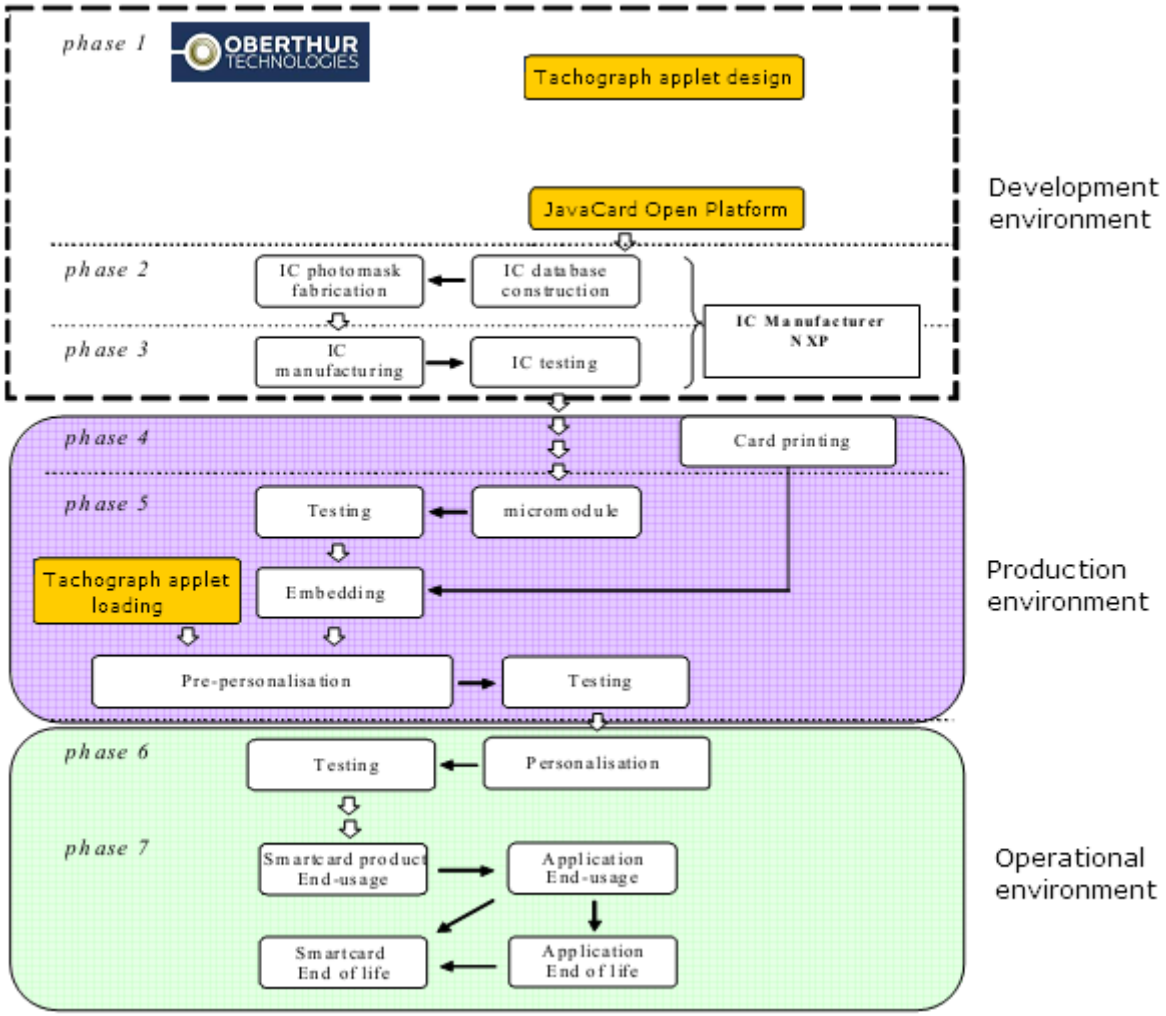

Figure 3: CALLIOPE life cycle

Nota bene:

The yellow boxes correspond to Oberthur Technologies software

2.3.1 Development environment

The development environment encompasses the environment in which the TOE is developed:

- JavaCard Open Platform components
- JavaCard applet package

2.3.1.1 Phase 1: Software development

Javacard Applet and javacard open platform (JOP) development environment is enforced by **OBERTHUR TECHNOLOGIES**.

JavaCard open platform and CAP files confidentiality and integrity are covered by the evaluation of the development premises of **OBERTHUR TECHNOLOGIES**.

To ensure security, access to development tools and products elements (PC, card reader, documentation, source code...) is protected. The protection is based on measures for prevention and detection of unauthorized access.

Two levels of protection are applied:

- Access control to **OBERTHUR TECHNOLOGIES** offices and sensitive areas
- Access to development data through the use of a secure computer system to design, implement and test software

The software development phase of the javacard open platform is covered by the certificate **[JOP].**

At the end of this phase:

- The Javacard Open Platform code is transferred to the chip manufacturer in order to be masked on silicium. The integrity and confidentiality of the data transfer between the premises of **OBERTHUR TECHNOLOGIES** and the chip manufacturer is covered by the certificate of **[JOP].**

At the end of phase 1, the JavaCard package is protected in integrity by the environment

2.3.1.2 Phase 2: Hardware development

In this phase, the Javacard Open Platform (JOP) is being built.

This phase takes place at the manufacturing site of the silicium provider.

JavaCard Open Platform code is protected in confidentiality and integrity, covered by the evaluation of the development premises of the silicium manufacturer (see **[JOP]**).

2.3.1.3 Phase 3: JavaCard Open platform manufacturing

In this phase, the javacard open platform (JOP) is self protected.

This phase takes place at the manufacturing site of the silicium provider.

At the end of phase 3, JOP is self protected: all its security functions are activated

2.3.2 Production environment

The production environment encompasses the environments in which the parts of TOE are gathered (javacard open platform and CAP files). It corresponds to the production of the javacard open platform (JOP).

It corresponds to the following steps:

- Software is engraved in the silicium to get the javacard open platform (JOP).
- The chip is mounted on a physical layout (card, USB token...)
- The javacard open platform is prepersonalized
- The javacard open platform is personalized
- Loading of the applet Javacard package
- The application is instantiated

2.3.2.1 Phase 4: JavaCard Open Platform packaging

The JOP is under the control of the Manufacturing Agent. This subject is in charge of the JOP packaging.
This phase spans the phase 4 of the JOP life cycle.

2.3.2.2 Phase 5: TOE initialization

The Javacard open platform (JOP) is under the control of the Manufacturing Agent. This subject shall be authenticated prior to any action on the javacard open platform.

This phase is done in the manufacturing site of Vitré (France – 35) or Shenzhen (China). The procedures and the IT infrastructure ensure the integrity and authenticity of the keys.

During this phase, at the prepersonalization step, the Tachograph Applet is loaded.

In any case, at the end of phase 5, the composite TOE is constructed and self-protected

This phase spans the following phases of the javacard open platform (JOP) life cycle:

- Phase 5
- Phase 6
- Phase 7

Depending on the case, the following process can be applied:

- the javacard open platform (JOP) is switched in phase 5 and the applet may be instantiated in this phase;
- the javacard open platform (JOP) is switched in phase 6 and the applet may be instantiated in this phase;
- the javacard open platform (JOP) is switched in phase 7 and the applet may be instantiated in this phase;

During all these phases, the javacard open platform (JOP) is self-protected as it requires the authentication of the Manufacturing Agent prior to any operation.

At the point of delivery, the TOE does not allow any other applet to be loaded.

2.3.3 Operational environment

The operational environment encompasses the environments in which the TOE is personalized and used.

It corresponds to the following steps:

- Personalization of the Tachograph Application
- Use of the Tachograph Application

2.3.3.1 Phase 6: TOE personalization

The TOE is under the control of the Administrator in charge of personalizing the Applet. This subject shall be authenticated prior to any action on the Javacard open platform and the TOE.

This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Administrator is responsible for ensuring a sufficient level of security during this phase.

During this phase, the applet is personalized according to [AGD_PRE]: creation of applicative data (SCD, SVD, RAD, File,…).

At the end of phase 6, the TOE is personalized

2.3.3.2 Phase 7: TOE usage

The TOE behaviour is conformant with EU Regulation 1360-2002 / appendix 2 p.97.

2.3.4 Coverage of the different Life Cycle state by the assurance components AGD & ALC

The following steps of the life cycle are covered as follows:

Life Cycle Phase	Environment	Covered by
Phase 1	**Development**	**ALC [JOP]** **ALC [CALLIOPE]**
Phase 2	**Development**	**ALC [JOP]**
Phase 3	**Development**	**ALC [JOP]**
Javacard Open Platform is self protected **Javacard package is protected by the environment**		
Phase 4	**TOE Production**	**ALC [AUDIT-PLANT]**
Phase 5	**TOE Production**	**ALC [CALLIOPE]** **ALC [AUDIT-PLANT]**
TOE is self protected **TOE is constructed**		
TOE delivery point		
Phase 6	**Operational**	**AGD_PRE [JOP]** **AGD_OPE [JOP]** **AGD_PRE [CALLIOPE]**
TOE is personalized		
Phase 7	**Operational**	**AGD_OPE [JOP]** **AGD_OPE [CALLIOPE]**

Table 1: Life cycle phase coverage

The point of delivery of the TOE is the end of phase 5. Therefore, phases 6 to 7 are fully covered by [AGD] as well as the personalization key management in the environment.

2.3.5 TOE State depending on the phase

The following table describes the TOE self protection.

Life cycle phase	Javacard package State at the end of the phase	JOP State at the end of the phase	TOE state at the end of the phase
Phase 1	Constructed but not self protected	In construction	In construction
Phase 2	Constructed but not self protected	In construction	In construction
Phase 3	Constructed but not self protected	Constructed and self protected	In construction
Phase 4	N/A	Self protected	In construction
Phase 5	Application is instantiated and self protected	Self protected	Constructed and self protected
Phase 6	Self protected	Self protected	Constructed and self protected
Phase 7	Self protected	Self protected	Constructed and self protected

Table 2: TOE state following the life cycle phase

2.3.6 Mapping with the life cycle described in [16]

The following table describes the TOE state, regarding the [16].

TOE life cycle phase	Life cycle phase with respect to [16]
Phase 1	Design
Phase 2	N/A
Phase 3	N/A
Phase 4	N/A
Phase 5	Loading of the Tachograph Applet
Phase 6	Personalization
Phase 7	Usage, destruction

Table 3: TOE state following the PP life cycle

For each of these phases, the following subjects may interact with the TOE.

TOE life cycle phase	Subject interacting with the TOE
Phase 1	OBERTHUR TECHNOLOGIES
Phase 2	IC MANUFACTURER
Phase 3	IC MANUFACTURER
Phase 4	MANUFACTURING AGENT
Phase 5	MANUFACTURING AGENT
Phase 6	ADMINISTRATOR
Phase 7	USER

Table 4: Interaction of subjects with the TOE

2.3.7 Link with PP life cycle

The TOE lifecycle is conformant with the life cycle described in **[16]** (§ 59).

However, the phase 6 as described in **[16]** is split between phase 5 and 6 of the TOE life cycle as follows:

PP life cycle	PP life cycle details	TOE life cycle
Phase 6	Initialisation (1) Initialisation of the embedded software	End of phase 5, covered by ALC This step corresponds to the applet instantiation
	TOE delivery point	
	Intialisation (2) creation of the application structure	Phase 6 of the TOE life cycle, covered by AGD. This step corresponds to the creation of the file structure and the specialization of the TOE (driver, control, company, workshop)
	Personalisation of the end-user data	Phase 6 of the TOE life cycle, covered by AGD

Table 5: Specific case of PP life cycle phase 6

2.4 Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 3.

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict Conformance
Part 2	Conformance to the extended part. ▪ FCS.RNG.1: "Random number generation" ▪ FPT_EMS.1: "TOE Emanation"
Part 3	Conformance to EAL 4, augmented with ▪ AVA_VAN.5: *"Advanced methodical vulnerability analysis"* ▪ ATE_DPT.2: *"Testing: security enforcing modules"* ▪ ALC_DVS.2: *"Sufficiency of security measures"*

2.5 Protection Profile Reference

This security target claims a **strict conformance** to the Tachograph Protection Profile:

Common Criteria Protection Profile

Digital Tachograph – Smart Card (Tachograph Card)

Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10

Common Criteria

BSI-CC-PP-0070

The European Regulation [5], [6] requires for Tachograph Cards the assurance level ITSEC E3 high as specified in [8], chap. 6 and 7.

JIL [10], Annex A defines a CC assurance package called E3hAP. This assurance package is intended to reach an equivalent assurance level in the framework of a CC certification as reached with an ITSEC E3 high certification (as required in [8]) and maps adequately (i.e. in particular in conjunction with the Digital Tachograph System) all assurance requirements from ITSEC E3 high into comparable CC (version 2.1) requirements.

The current official CCMB version of Common Criteria is Version 3.1, Revision 3. This version defines in its part 3 assurance requirements components partially differing from the respective requirements of CC v2.x. The CC community acts on the presumption that the EAL-Assurance Packages defined in CCv3.1 and CCv2.x are equivalent and can therefore be used for certification activities without restrictions.

Based on these statements, an appropriate assurance package E3hCC31_AP as shown in table 6 (section 2.6.4.2) below was compiled and defined. The validity of this proposal is confined to the Digital Tachograph System. The assurance package E3hCC31_AP does not define a new security level, but only directly switches the requirements in E3hAP which are related to the older CC version 2.1 to the current version 3.1 of the CC ([3]).

3 Security Problem Definition

3.1 Assets

The assets to be protected by the TOE and its environment within phase 6 and 7 of the TOE's life-cycle are the application data defined as follows:

Identification data (IDD)

Primary asset: card identification data, cardholder identification data (see Glossary for more details)

Property: Integrity

Activity data (ACD)

Primary asset: cardholder activities data, events and faults data and control activity data (see Glossary for more details)

Properties: Integrity, Authenticity, for parts of the activity data also Confidentiality

Signature creation data (SCD)

Secondary asset: private key used to perform an electronic signature operation

Properties: Confidentiality, Integrity

Secret messaging keys (SMK)

Secondary asset: session keys (TDES) used to protect the Tachograph Card communication by means of secure messaging

Properties: Confidentiality, Integrity

Signature verification data (SVD)

Secondary asset: public keys certified by Certification Authorities, used to verify electronic signatures

Properties: Integrity, Authenticity

Verfication authentication data (VAD)

Secondary asset: authentication data provided as input for authentication attempt as authorised user (PIN)

Properties: Confidentiality (This security property is not maintained by the TOE but by the TOE environment)

Reference authentication data (RAD)

Secondary asset: data persistently stored by the TOE for verification of the authentication attempt as authorised user

Properties: Confidentiality, Integrity

Data to be signed (DTBS)

Secondary asset: the complete electronic data to be signed (including both user message and signature attributes)

Properties: Integrity, Authenticity

TOE File system incl. specific identification data

Secondary asset: file structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation

Property: Integrity

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

3.2 Users / Subjects

This Protection Profile considers the following subjects, who can interact with the TOE:

Administrator

S.Administrator: the subject is usually active only during Initialisation/Personalisation (Phase 6)

Vehicle Unit

S.VU: Vehicle Unit (with a UserID), which the Tachograph Card is connected to.

Other devices

S.Non-VU: Other device (without UserID) which the Tachograph Card is connected to.

Attacker

It is a human or process acting on his behalf being located outside the TOE. For example, a driver could be an attacker if he misuses the driver card. An attacker is a threat agent (a person with the aim to manipulate the user data or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the maintained assets. The attacker is assumed to possess an at most *high* attack potential.

During phases 4 and 5, a manufacturing agent interferes with the Javacard Open Platform. This subject is not mentionned as part of a subject for the composite TOE, because it is relevant to site audit.

Application note: This table defines the subjects in the sense of [1] which can be recognised by the TOE independently of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates - for each of the respective external entities except the Attacker, who is listed for completeness - an 'image' inside and 'works' then with

this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not distinguish between 'subjects' and 'external entities'.

Nota bene:

In this security target the personalisation process has been included in the TOE scope.

3.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats are defined in reference to the according assets protected by the TOE and result from the method of TOE's use in the operational environment.

The following threat has been added in the security target:

- T.Authentication_Masquerade

The following threats described also in GST [8], sec. 3.3.1 are defined in the current Security Target.

3.3.1 Phase 6

T.Personalisation_Data

Disclosure or Modification of Personalization Data

A successful modification of personalisation data (such as TOE file system, cryptographic keys, RAD) to be stored in the TOE or disclosure of cryptographic material during the personalisation would be a threat to the security of the TOE. The threat addresses the execution of the TOE's personalisation process and its security.

The threat agent for T.Personalisation_Data is Attacker

Nota bene:

This threat, drawn from [16], only applies in phase 6; when the personalisation takes place.

T.Authentication_Masquerade

Masquerade of Administrator authentication

A successful replay of the Administrator authentication, a masquerade of the Administrator, or bypassing of access control during phase 6 would allow setting or changing the following assets: Identification data, Activity data, SCD, SVD, RAD and TOE file system. As such, it is a major threat to the global security objectives of the TOE.

The threat agent for T.Authenticaton_Masquerade is Attacker

3.3.2 Phase 7

All the other threats drawn from [16] only apply once the TOE is personalized and ready to be used by the final user.

T.Identification_Data

Modification of Identification Data

A successful modification of identification data held by the TOE (IDD, see sec. 3.1, e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.

The threat agent for T.Identification_Data is Attacker

T.Activity_Data

Modification of Activity Data

A successful modification of activity data stored in the TOE (ACD, see sec. 3.1, e.g. cardholder activities data, events and faults data and control activity data) would be a threat to the security of the TOE.

The threat agent for T.Activity_Data is Attacker

T.Data_Exchange

Modification of Activity Data during Data Transfer

A successful modification of activity data (ACD deletion, addition or modification, see sec. 3.1) during import or export would be a threat to the security of the TOE.

The threat agent for T.Data_Exchange is Attacker

3.4 Organisational Security Policies

The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operation.

P.EU_Specifications

EU Specifications Conformance

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

3.5 Assumptions

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

A.Personalisation_Phase

Personalisation Phase Security

All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation are correct according to the Tachograph Card Specification [7] and are handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and

information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

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

The following Security Objectives have been added in the Security Target:

- OT.Personalisation_AC
- OT_Personalisation_Confidentiality
- OT.Lifecycle_Security

4.1.1 Phase 6

OT.Personalisation_AC

Access control during personalisation

The TOE must ensure that the Tachograph user data (stored in filesystem) and TSF data (European Key, RAD, Card Authentication Key Pair, Card Issuance Date) can be written by authorized Administrator only. The user data and the TSF data may be written only during personalisation and cannot be changed after personalisation of the Tachograph card.

OT.Personalisation_Confidentiality

SCD and RAD are protected during Phase 6

The TOE must ensure confidentiality SCD and RAD during their exchange between the TOE and the personalization equipment after the Administrator Authentication.

4.1.2 Phase 7

All the the following security objectives drawn from [16] only apply once the TOE is personalized and ready to be used by the final user.

OT.Card_Identification_Data

Integrity of Identification Data

The TOE must preserve card identification data and cardholder identification data stored during card personalisation process as specified by the EU documents [5] to [9].

OT.Card_Activity_Storage

Integrity of Activity Data

The TOE must preserve user data stored in the card by Vehicle Units as specified by the EU documents [5] to [9].

OT.Data_Access

User Data Write Access Limitation

The TOE must limit user data write access rights to authenticated Vehicle Units as specified by the EU documents [5] to [9].

OT.Secure_Communications

Secure Communications

The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application as specified by the EU documents [5] to [9].

4.1.3 Phase 6 and 7

OT.Lifecycle_Security

The TOE shall manage its own life cycle states as well as reversible and irreversible transitions between them. The TOE shall reject operations unexpected in its current life cycle.

4.2 Security objectives for the Operational Environment

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

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

4.2.1 Phase 6

OE.Personalisation_Phase

Secure Handling of Data in Personalisation Phase

All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation must be correct according to the Tachograph Card Specification [7] and must be handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider must control all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality.

For the definition of the terms 'Personalisation Phase', 'initialisation' and 'personalisation' refer to sec. 1.2.3 [16].

For further information on the Tachograph Card lifecycle, refer to section 2.3.

4.2.2 Phase 7

OE.Tachograph_Components

Implementation of Tachograph Components

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

Application Note:

In particular, the Vehicle Unit shall fulfill the requirement UIA_212 stated in [5] : "In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long"

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Phase 6

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

- OT.Personalisation_AC for the authenticity of the data during their transfer in phase 6, with the guarantee that the sent data are issued by the Administrator
- OT.Personalisation_Confidentiality for the confidentiality of the data during their transfer in phase 6

T.Authentication_Masquerade T.Authentication_Masquerade is addressed by OT.Personalisation_AC for the access control of the sent data in phase 6 that requires the Administrator authentication prior any sensitive actions. This objective avoids any attackers to impersonate the Administator.

4.3.1.2 Phase 7

T.Identification_Data T.Identification_Data is addressed by OT.Card_Identification_Data. The unalterable storage of personalised identification data of the TOE (cardholder identification data, card identification data) as defined in the security objective OT.Card_Identification_Data counters directly the threat T.Identification_Data. OT.Lifecycle_Security prevents from inverting life cycle phases, such as the TOE in phase 7 can not be reverted to phase 6. The Administrator can no longer be identified and so the Identication Data are unalterable.

T.Activity_Data T.Activity_Data is addressed by OT.Card_Activity_Storage and OT.Data_Access. The unalterable storage of Activity data as defined in the security objective OT.Card_Activity_Storage counters directly the threat T.Activity_Data. In addition, the security objective OT.Data_Access limits the user data write access to authenticated Vehicle Units so that the modification of activity data by regular card commands can be conducted only by authenticated card interface devices. OT.Lifecycle_Security prevents from inverting life cycle phases, such as the TOE in phase 7 can not be reverted to phase 6. The Administrator can no longer be identified and so the Activity Data are unalterable.

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

4.3.2 Organisational Security Policies

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

4.3.3 Assumptions

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

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale

T.Personalisation_Data	OT.Personalisation_AC, OT.Personalisation_Confidentiality, OE.Personalisation_Phase	Section 4.3.1
T.Authentication_Masquerade	OT.Personalisation_AC	Section 4.3.1
T.Identification_Data	OT.Card_Identification_Data, OT.Lifecycle_Security	Section 4.3.1
T.Activity_Data	OT.Card_Activity_Storage, OT.Data_Access, OT.Lifecycle_Security	Section 4.3.1
T.Data_Exchange	OT.Secure_Communications	Section 4.3.1

Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.Personalisation_AC	T.Personalisation_Data, T.Authentication_Masquerade	
OT.Personalisation_Confidentiality	T.Personalisation_Data	
OT.Card_Identification_Data	T.Identification_Data	
OT.Card_Activity_Storage	T.Activity_Data	
OT.Data_Access	T.Activity_Data	
OT.Secure_Communications	T.Data_Exchange	
OT.Lifecycle_Security	T.Identification_Data, T.Activity_Data	
OE.Personalisation_Phase	T.Personalisation_Data	
OE.Tachograph_Components		

Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.EU_Specifications	OT.Card_Identification_Data, OT.Card_Activity_Storage, OT.Data_Access, OT.Secure_Communications, OE.Tachograph_Components	Section 4.3.2

OSPs and Security Objectives - Coverage

Security Objectives	**Organisational Security Policies**	**Rationale**
OT.Personalisation_AC	tok26	
OT.Personalisation_Confidentiality	tok26	
OT.Card_Identification_Data	P.EU_Specifications	
OT.Card_Activity_Storage	P.EU_Specifications	
OT.Data_Access	P.EU_Specifications	
OT.Secure_Communications	P.EU_Specifications	
OT.Lifecycle_Security		

OE.Personalisation_Phase		
OE.Tachograph_Components	P.EU_Specifications	

Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Personalisation_Phase	OE.Personalisation_Phase	Section 4.3.3

Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions	Rationale
OE.Personalisation_Phase	A.Personalisation_Phase	
OE.Tachograph_Components		

Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FPT_EMS - TOE Emanation

5.1.1.1 Description

The family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

5.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

The family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

Definition

FPT_EMS.1 TOE Emanation

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

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

Dependencies: No dependencies.

5.1.2 Extended Family FCS_RNG - FCS_RNG: Random Number Generation

5.1.2.1 Description

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

5.1.2.2 Extended Components

Extended Component FCS_RNG.1

Description

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

Definition

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

6 Security Requirements

6.1 Security Functional Requirements

The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in chap. 4 of the ITSEC based Tachograph Card GST in [8].

Security Function Policy: AC_SFP

The Security Function Policy Access Control (AC_SFP) for Tachograph Cards in the end-usage phase based on the Tachograph Cards Specification [7], sec. 3 and 4, GST [8], sec. 4.3.1 and 4.3.2 as well as JIL [10], sec. 2.6 is defined as follows: The SFP AC_SFP is only relevant for the end-usage phase of the Tachograph Card, i.e. after the personalisation of the card has been completed. Subjects:

- S.VU (in the sense of the Tachograph Card specification)
- S.Non-VU (other cardinterface devices)

Security attributes for subjects:

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)
- USER_ID Vehicle Registration Number (VRN) and Registering Member State Code (MSC), exists onlyfor subject S.VU

Objects:

- user data:
  - identification data (card identification data, cardholder identification data)
  - activity data (cardholder activities data, events and faults data, control activity data)
- security data:
  - cards´s private signature key
  - public keys (in particular card´s public signature key; keys stored permanently on the card or imported into the card using certificates)
  - session keys
  - PIN (for workshop card only)
- TOE software code
- TOE file system (incl. file structure, additional internal structures, access conditions)
- identification data of the TOE concerning the IC and the Smartcard Embedded Software (indicated as identification data of the TOE in the following text)
- identification data of theTOE`s personalisation concerning the date and time of the personalisation (indicated as identification data of the TOE`s personalisation in the following text)

Security attributes for objects:

- Access Rulesbased on defined Access Conditions (see below) for:
- user data
- security data

- identification data of the TOE
- identification data of the TOE's personalisation
- Digital signature for each data to be signed

Operations:

- user data:
  - identification data: selecting (command Select), reading (command Read Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)
  - activity data: selecting (command Select), reading (command Read Binary), writing / modification (commandUpdate Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)
- security data:
  - card´s private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication(command External Authenticate)
  - public keys (in particular card´s public signature key): referencing over a MSE-command (for further usage withincryptographic operations as authentication, verification of a digital signature etc.)
  - session keys: securing of commands with Secure Messaging
  - PIN (only relevant for Workshop Card): verification (command Verify PIN)
- TOE software code: No Operations
- TOE file system(incl. file structure, additionalinternal structures, access conditions): No Operations
- identificationdata of the TOE: selecting and reading
- identification data of the TOE?s personalisation (date and time of personalisation): selecting and reading.

Access Rules:

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

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

- AUT and PRO SM (combined, see description above)

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

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

6.1.1 SFR from the Tachograph Protection Profile

6.1.1.1 Phase 6 and 7

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up and periodically during normal operation** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

Application Note:

Refer to RLB_301, RLB_302, RLB_303, chapter 4.7.1 of [8]

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **Integrity errors** on all objects, based on the following attributes: **IntegrityControlledData**.

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

Application Note:

refer to chapter 4.6.1

The following data persistently stored by TOE have the user data attribute " integrityControlledData ":

- PINs (i.e. objects instance of class OwnerPin orsubclass of interface PIN)
- keys (i.e. objects instance of classes implemented the interface Key)
- packages Java Card

- Activity Data and Identification User Data

If the maximum is reached (15) the Kill card is launched.

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **AC_SFP** on **Subjects:**

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

Objects:

- **User data:**
  - **Identification data**
  - **Activity data**
- **Security data:**
  - **Card's private signature key**
  - **Public keys**
  - **Session keys**
  - **PIN (for workshop card)**
- **TOE software code**
- **TOE file system**
- **Identification data of the TOE**
- **Identification data of the TOE's personalisation**

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

FDP_ACC.2.2 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.

Application Note:

Refer to chapter 4.3.1, ACT_301, ACT_302, chapter 4.4 of [8] as well as JIL [10], sec. 2.6

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **AC_SFP** to objects based on the following:

Subjects:

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

Objects:

- **user data:**
  - **identification data**

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

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

- **GENERAL_READ:**
  - **driver card, workshop card: user data may be read from the TOE by any user**
  - **control card, company card: user data may be read from the TOE by any user, except cardholder identification data which may be read by S.VU only;**
- **IDENTIF_WRITE: all card types: identification data may only be written once and before the end of Personalisation; no user may write or modify identification data during end-usage phase of card's life-cycle;**
- **ACTIVITY_WRITE: all card types: activity data may be written to the TOE by S.VU only;**
- **SOFT_UPGRADE: all card types: no user may upgrade TOE's software;**
- **FILE_STRUCTURE: all card types: files structure and access conditions shall be created before the Personalisation is completed and then locked from any future modification or deletion by any user**
- **IDENTIF_TOE_READ: all card types: identification data of the TOE and identification data of the TOE's personalisation may be read from the TOE by any user;**
- **IDENTIF_TOE_WRITE: all card types: identification data of the TOE may only be written once and before the Personalisation; no user may write or modify these identification data during the Personalisation;**
- **IDENTIF_ TOE_ PERS_WRITE: all card types: identification data of the TOE's personalisation may only be written once and within the Personalisation; no user may write or modify these identification data during end-usage phase of card's life-cycle**.

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Application Note:

Refer to chapters 3.3 and 4 of [7], chapter 4.3.2, ACT_301, ACT_302, chapter 4.4 of [8] as well as JIL [10], sec. 2.6. More information on the access control policies is available in the annex part.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **Side channel emission** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **private key(s) and session keys** and **RAD**.

FPT_EMS.1.2 The TSF shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **private key(s) and session keys** and **RAD**.

Application Note:

Refer to RLB_304, chapter 4.7.2 of [8]

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **Reset**
- **Power supply cut-off**
- **Power supply variations**
- **Unexpected abortion of the TSF execution due to external or internal events (esp. break of a transaction before completion)**.

Application Note:

Refer to RLB_306, chapter 4.7.3, RLB_307, chapter 4.7.4 of [8]

FPT_PHP.3 Resistance to physical attack

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

Application Note:

Refer to RLB_304, chapter 4.7.2 of [8]

The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSF security could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.1.1.2 Phase 7

FAU_SAA.1 Potential violation analysis

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

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

a) Accumulation or combination of

- **cardholder authentication failure**
- **self test error**
- **stored data integrity error**
- **activity data input integrity error**

known to indicate a potential security violation;

b) **none**.

Application Note:

The events cardholder authentication failure, self test error, stored data integrity error and activity data input integrity error may occur in combination or as single failure event.

FCO_NRO.1 Selective proof of origin

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

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

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

Application Note:

Refer to chapter 4.8.2 of [8], DEX_304, DEX_305, DEX_306

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **cryptographic two-keys TDES derivation algorithms** and specified cryptographic key sizes **128 bits with 112 effective bits** that meet the following: **Tachograph Common Security Mechanisms [9], sec. 3, CSM_012, CSM_013, CSM_015, CSM_020**.

Application Note:

refer to chapter 4.9 of [8], CSP_301

As required in sec. 4.9 of [8], session key shall have a limited number of uses. It shall be destroyed after 240 uses (one use of the key = one command using secure messaging sent to the card and associated response).

FCS_CKM.2 Cryptographic key distribution

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

Application Note:

Refer to chapter 4.9 of [8], CSP_302

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Zeroization** that meets the following: **Tachograph Common Security Mechanisms [9], sec. 3, CSM_013 and Tachograph Card Specification [7], sec. 3.6**.

Application Note:

Refer to chapter 4.9 of [8], CSP_301.

As required in sec. 4.9 of [8], session key shall have a limited number of uses. It shall be destroyed after 240 uses (one use of the key = one command using secure messaging sent to the card and associated response). It shall be destroyed as well at the end of the session (withdrawal of the card or reset of the card), or when a secure messaging error occurs.

FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1/RSA The TSF shall perform **the cryptographic operation (encryption, decryption, signature creation and signature verification as well as certificate verification for the authentication between the Tachograph Card and the Vehicle Unit and signing for downloading to external media)** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits** that meet the following: **Tachograph Common Security Mechanisms [9], sec. 2-6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_016, CSM_017, CSM_018, CSM_019, CSM_020, CSM_033, CSM_034, CSM_035 and Tachograph Card Specification [7], sec. 3**.

Application Note:

Refer to CSM_003 and further chapters of [9]

FCS_COP.1/TDES Cryptographic operation

FCS_COP.1.1/TDES The TSF shall perform **the cryptographic operations (encryption and decryption respective Retail-MAC generation and verification) concerning symmetric cryptography** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **of 128 bits with 112 effective bits** that meet the following: **Tachograph Common Security Mechanisms [9], sec. 2, CSM_005, sec. 3, CSM_015, sec. 5, CSM_021-CSM_031 and Tachograph Card Specification [7], sec. 3**.

Application Note:

Refer to CSM_002 and further chapters of [9]

FDP_DAU.1 Basic Data Authentication

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

FDP_DAU.1.2 The TSF shall provide **S.VU and S.Non-VU** with the ability to verify evidence of the validity of the indicated information.

Application Note:

Refer to chpater 4.6.2 of [8]

FDP_ETC.1 Export of user data without security attributes

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

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

Application Note:

Refer to chpater 4.3.2 of [8]

FDP_ETC.2 Export of user data with security attributes

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

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

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

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: **none**.

Application Note:

Refer to DEX_304, DEX_305, DEX_306, chpater 4.8 of [8]

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **AC_SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

Application Note:

Refer to chapters 4.3.1 and 4.3.2, RLB_305, chpater 4.7.2 of [8]

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to and deallocation of the resource from** the following objects: **session key, SCC, authentication status**.

FIA_AFL.1/C Authentication failure handling

FIA_AFL.1.1/C The TSF shall detect when **1** unsuccessful authentication attempts occur related to **authentication of a card interface device**.

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

Application Note:

Refer to UIA_301, chapter 4.2.2 of [8], chapter 4.2.3 of [8]

FIA_AFL.1/WSC Authentication failure handling

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

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

Application Note:

Refer to UIA_302, chapter 4.2.2 of [8], chapter 4.2.3 of [8]

FIA_ATD.1 User attribute definition

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

- **USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)**
- **USER_ID (VRN and Registering MSC for subject S.VU)**.

Application Note:

Refer to chapter 4.2.1 of [8]

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **driver card, workshop card: export of user data with security attributes (card data download function), control card, company card: export of user data without security attributes except export of cardholder identification data** on behalf of the user to be performed before the user is authenticated.

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

Application Note:

Refer to UIA_301, chapter 4.2.2 of [8]

FIA_UAU.3 Unforgeable authentication

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

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

Application Note:

Refer to UIA_301, chapter 4.2.2 of [8]

FIA_UAU.4 Single-use authentication mechanisms

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

Application Note:

Refer to UIA_301, chapter 4.2.2 of [8]

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **none of the TSF-mediated actions** on behalf of the user to be performed before the user is identified.

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

Application Note:

Refer to chapter 4.2.1 of [8]

The identification of the user is reached with the plug-in of the Tachograph Card into a card reader and the following power-up of the card.

FIA_USB.1 User-subject binding

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

- **USER_GROUP (VEHICLE_UNIT for S.VU, NON_VEHICLE_UNIT for S.Non-VU)**
- **USER_ID (VRN and Registering MSC for subject S.VU)**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **refer to AC_SFP**.

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: **refer to AC_SFP**.

Application Note:

refer to chapters 4.3.1, 4.7.2 (RLB_304, RLB_305) of [8]

FPR_UNO.1 Unobservability

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

Application Note:

Refer to RLB_304, chapter 4.7.2 of [8]

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

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

Application Note:

Refer to DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [8], chapter 5.3 of [9]

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **activity data import from a remote trusted product**.

Application Note:

Refer to DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [8]

6.1.2 Additional SFR

6.1.2.1 Phase 6

FCS_CKM.1/Perso Cryptographic key generation

FCS_CKM.1.1/Perso 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: **ANSI X9.31**.

Application Note:

This SFR concerns the TOE key generation for signature and authentication

FCS_CKM.1/Perso_GP Cryptographic key generation

FCS_CKM.1.1/Perso_GP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **TDES 2-Keys** and specified cryptographic key sizes **112 bits effective** that meet the following: **according to SCP01 and SCP02 of Global Platform 2.1.1**.

FCS_CKM.2/Perso Cryptographic key distribution

FCS_CKM.2.1/Perso The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **command GET DATA** that meets the following: **none**.

Application Note:

This SFR concerns the TOE public key distribution for signature and authentication

FCS_COP.1/Perso Cryptographic operation

FCS_COP.1.1/Perso The TSF shall perform **Cryptographic operations** in accordance with a specified cryptographic algorithm **Cryptographic algorithm** and cryptographic key sizes **112 bits effective (3DES 128 bits)** that meet the following **Global Platform 2.1.1**

Cryptographic operations	Cryptographic algorithm
Administrator Authentication	SCP01 or SCP02
GP Secure messaging	SCP01 or SCP02
sensitive data encryption	SCP01 or SCP02

.

Application Note:

This SFR covers the Administrator Authentication and the Secure Messaging during phase 6. This SFR covers also the RAD and SCD ciphering.

FDP_ACC.2/Perso Complete access control

FDP_ACC.2.1/Perso The TSF shall enforce the **Personalization access control** on **all subject and all objects** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/Perso 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.

FDP_ACF.1/Perso Security attribute based access control

FDP_ACF.1.1/Perso The TSF shall enforce the **Personalization access control** to objects based on the following:

- **Subject: Administrator**
- **Objects: all files content, SCD, SVD, RAD, European key and its attributes, KID**
- **Security attribute for subject: role Administrator**
- **Security attribute for objects: Access rules**.

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

- **TOE_PERS_READ: all card types: Only the subject with Administrator role is able to read all the data, including User data, except the RAD and SCD**

- **TOE_PERS_WRITE: all card types: Only the subject with Administrator role is able to write all the data**.

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

FDP_ACF.1.4/Perso The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Application Note:

More information is available on the annex part of the document

FDP_ETC.1/Perso Export of user data without security attributes

FDP_ETC.1.1/Perso The TSF shall enforce the **Personalization Access control** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/Perso The TSF shall export the user data without the user data's associated security attributes

FDP_ITC.1/Perso Import of user data without security attributes

FDP_ITC.1.1/Perso The TSF shall enforce the **Personalization Access Control** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Perso The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Perso The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FDP_UCT.1/Perso Basic data exchange confidentiality

FDP_UCT.1.1/Perso The TSF shall enforce the **Personalization access control** to **receive** user data in a manner protected from unauthorised disclosure.

Application Note:

This SFR concerns the RAD and SCD components

FIA_AFL.1/Perso Authentication failure handling

FIA_AFL.1.1/Perso The TSF shall detect when **1** unsuccessful authentication attempts occur related to **Administrator authentication**.

FIA_AFL.1.2/Perso When the defined number of unsuccessful authentication attempts has been **surpassed and met**, the TSF shall **slow down the next authentication in accordance with the following function: The waiting time is exponential with a maximum number of unsuccessful authentications of 15**.

FIA_ATD.1/Perso User attribute definition

FIA_ATD.1.1/Perso The TSF shall maintain the following list of security attributes belonging to individual users: **role Administrator**.

FIA_UAU.1/Perso Timing of authentication

FIA_UAU.1.1/Perso The TSF shall allow **Initialize Authentication process, Get Data (commercial version and internal version), Select** on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.4/Perso Single-use authentication mechanisms

FIA_UAU.4.1/Perso The TSF shall prevent reuse of authentication data related to **the Administrator authentication mechanism (GP authentication)**.

FIA_UAU.7/Perso Protected authentication feedback

FIA_UAU.7.1/Perso The TSF shall provide only **the result of the authentication (NOK), the key set version, Secure channel identifier and the card random and the card cryptogram** to the user while the authentication is in progress.

Application Note:

NOK is an information stating that Administrator authentication has failed.

FIA_UID.1/Perso Timing of identification

FIA_UID.1.1/Perso The TSF shall allow **Administrator Authentication, Get Data (for commercial version, internal version and File System information), Select Applet and Select DF** on behalf of the user to be performed before the user is identified.

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

FMT_MOF.1/Perso Management of security functions behaviour

FMT_MOF.1.1/Perso The TSF shall restrict the ability to **modify the behaviour of** the functions **Tachograph Card Type (driver card, workshop card, control card and company card) and the GP Secure Messaging level** to **Administrator**.

FMT_MTD.1/Perso Management of TSF data

FMT_MTD.1.1/Perso The TSF shall restrict the ability to **modify** the **TOE life cycle** to **Administrator**.

FMT_SMF.1/Perso Specification of Management Functions

FMT_SMF.1.1/Perso The TSF shall be capable of performing the following management functions: **modify security attributes and data**.

FMT_SMR.2/Perso Restrictions on security roles

FMT_SMR.2.1/Perso The TSF shall maintain the roles: **Administrator**.

FMT_SMR.2.2/Perso The TSF shall be able to associate users with roles.

FMT_SMR.2.3/Perso The TSF shall ensure that the conditions

Roles	Condition for this role
Administrator	Successful authentication of Administrator using a key set of the Card Manager

are satisfied.

FTP_ITC.1/Perso Inter-TSF trusted channel

FTP_ITC.1.1/Perso 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/Perso The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/Perso The TSF shall initiate communication via the trusted channel for **Personalization**.

6.1.2.2 Phase 6 and 7

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a **deterministic hybrid** random number generator that implements: **none**.

FCS_RNG.1.2 The TSF shall provide random numbers that meet **khi 2 test**.

6.2 Security Assurance Requirements

The European Regulation [5], [6] requires for Tachograph Cards the assurance level ITSEC E3 high as specified in [8], chap. 6 and 7.

6.2.1 Rationale for composition with Security Assurance Package E3hCC31_AP

JIL [10], Annex A defines a CC assurance package called E3hAP. This assurance package is intended to reach an equivalent assurance level in the framework of a CC certification as reached with an ITSEC E3 high certification (as required in [8]) and maps adequately (i.e. in particular in conjunction with the Digital Tachograph System) all assurance requirements from ITSEC E3 high into comparable CC (version 2.1) requirements.

The current official CCMB version of Common Criteria is Version 3.1, Revision 3. This version defines in its part 3 assurance requirements components partially differing from the respective requirements of CC v2.x.

The CC community acts on the presumption that the EAL-Assurance Packages defined in CCv3.1 and CCv2.x are equivalent and can therefore be used for certification activities without restrictions.

Based on these statements, an appropriate assurance package E3hCC31_AP as shown specified above in section 2.6.4.2 was compiled and defined. The validity of this proposal is confined to the Digital Tachograph System. The assurance package E3hCC31_AP does not define a new security level, but only directly switches the requirements in E3hAP which are related to the older CC version 2.1 to the current version 3.1 of the CC ([3]).

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

Application note: The requirement (RLB_304) is partially covered by ADV_ARC (self-protection).

6.2.2 Rationale for composition with ALC_DVS.2

The selection of the component ALC_DVS.2 provides a higher level of protection of the TOE during development Phase. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

7 TOE Summary Specification

7.1 TOE Summary Specification

The TOE inherits all the security functions provided by the underlying javacard open platform [JOP] (see the Security targets of the Javacard Open Platform [20]). On top of these, it adds some supplemental security functions that are described hereafter.

Access Control in reading

This function controls read access to files and enforces the security policy for data retrieval. This security function applies both in phase 6 and 7. Prior to any file reading, it ensures the correct access conditions are met:

- The needed subject is authenticated (when needed)
- expected secure messaging level is applied (when needed) In phase 7, it ensures the key stored in the filesystem of the workshop (KWC) can only be returned protected in confidentiality. This function ensures the readilibity of the card by card interface device of a Vehicle Unit or any card reader, in accordance with associated access rights.

Access Control in writing

This function controls write access to files and enforces the security policy for data writing. This security function applies both in phase 6 and 7. Prior to any file writing, it ensures the correct access conditions are met:

- The needed subject is authentified
- expected secure messaging level is applied (when needed)

Authentication during phase 6

This security function is in charge of the mutual authentication, during phase 6 of Tachograph life cycle between the TOE and the Administrator. This security function enables to create a trusted channel by generating shared ephemeral secret keys. This trusted channel enables to fulfill access conditions mandated to personalize the TOE (Read/Update file, load data). The authentication protocol prevents the use of forged data authentication by using randomness. This authentication is based on a symmetric Authentication mechanism based on a Triple DES algorithm. This security function is supported by SF_Cryptographic_Operations.

Authentication during phase 7

This security function is in charge of the mutual authentication, during phase 7 of Tachograph life cycle between the TOE and the IFD (namely a Vehicle Unit). This security function enables to create a trusted channel by generating a shared ephemeral secret key and a secret dynamic non replay counter (SSC). This trusted channel enables to fulfill access conditions mandated to get access rights to files (Read/Update). The authentication protocol prevents the use of forged data authentication by using randomness. This security function is supported by SF_Cryptographic_Operations.

Clearing of sensitive information

This security function ensures the clearing of sensitive information.

- In phase 7
  - Session key, SSC, and authentication state are securely erased when a new authentication is started, or when the TOE is powered off/on
  - Session key and SSC are securely erased in case an error is detected in the incoming command (wrong MAC) or when more than 240 commands under secure messaging have been received
  - Authentication state is securely erased in case an error occurs in the authentication protocols
- In phase 6
  - Session keys and authentication state are securely erased when a new authentication is started, or when the TOE is powered off/on
  - Session keys are securely erased in case an error is detected in the incoming command (wrong MAC)
  - Authentication state is securely erased in case an error occurs in the authentication protocols

Cryptographic operations

This security function ensures the usage of the secure cryptographic functionalities (including random numbers generation) that are resistant against attacks with high potential (AVA_VAN.5). These functionalities are provided by the underlying platform. This security functionality supports the others one by providing them cryptographic operations.

Errors messages and exceptions

This security function is in charge of detecting and recording failures events, such as:

- cardholder authentication failures
- self test errors
- stored data integrity errors
- activity data input integrity errors

Key management

This security function is in charge of the management of key in phase 6 and 7. In particular it is in charge of

- SCD and SVD key generation and enforcing its access control in phase 6
- SCD and SVD key import and enforcing its access control in phase 6
- Confidentiality of SCD during import in phase 6
- Export of SVD and enforcing its access control in phase 6
- Import of public key in phase 7 (VU and MS public keys) through the Card Verifiable certificates (CVC)

Life cycle management

This security functionality ensures the secure life cycle of the TOE. This TSF enures:

- The non-reversibility of phases
- The non-modification of Tachograph card type after personalization
- Only the Administrator can configure the Tahcograph card type in phase 6

Physical protection

This security function protects the TOE against physical attacks. It ensures their detection and provides counteractions.

RAD Management

This security function is in charge of the management of RAD in phase 6 and 7. In particular it is in charge of

- RAD import and enforcing its access control in phase 6
- Confidentiality of RAD during import in phase 6
- Verification of VAD in phase 7

Safe state management

This security function ensures that the TOE gets back to a secure state when

- An error is detected by the SF_Self_test
- A tearing occurs (during a copy of data in EEPROM)

This security function ensures that when such a case occurs, the TOE is either switched in the state "kill card" or becomes mute and gets back in the idle state (all ephemeral states are reset)

Secure Messaging

This security function ensures the authenticity and integrity of the communication between the TOE and the IFD (namely a Vehicle Unit). A trusted channel is established after a successful mutual authentication based on a key transport protocol. This security functions relies on a checksum computed over the incoming command, and the outgoing data using Triple DES algorithm with the secure messaging session key. Moreover, this security function ensures the confidentiality of the content of some file when being read. In such cases, the data are encrypted with the secure messaging session key using triple DES.

In order to protect the TOE against deletion, insertion or replay of protected commands, this security function manages as well a dynamic counter (SSC). This counter is increased each time a protected incoming command/outgoing data is processed. This security function is supported by SF_Cryptographic_Operations.

Self tests

The TOE performs self tests on the TSF data it stores to protect the TOE. In particular, this security function is in charge of:

- Detecting DFA
- Performing self tests of the random generator and cryptographic routines (DES, RSA)
- Monitoring of the integrity of keys, RAD, files, files attributes and TSF data
- Monitoring the integrity of the executable code
- Protecting the cryptographic operation

- Monitoring the correct operation of the executable code

The integrity checking of all the data is checked each time they are accessed. The self tests of the random generator and of the cryptographic routines are made at start up, as well as the integrity checks of the executable code. The protection of the cryptographic operation,of the executable code operation, and against DFA is made during TOE operation. This security function is supported by SF_Cryptographic_Operations.

Signature

This secure function ensures the signature generation of the TOE?s file and its verification. For signature generation, it performs the hash computation of the currently selected, using SHA-1 algorithm and its signature with the TOE?s private key. The signature verification is performed by unwrapping it with the public key imported on the TOE (using SF_Key_Management) and the reference hash provided by the outside. This security function is supported by SF_Cryptographic_Operations.

Index

A

A.Personalisation_Phase 27
Access__Control__in__reading 58
Access__Control__in__writing 58
Activity__data__(ACD) 24
Administrator 25
Attacker 25
Authentication__during__phase__6 58
Authentication__during__phase__7 58

C

Clearing__of__sensitive__information 59
Cryptographic__operations 59

D

Data__to__be__signed__(DTBS) 25

E

Errors__messages__and__exceptions 59

F

FAU_SAA.1 43
FCO_NRO.1 43
FCS_CKM.1 44
FCS_CKM.1/Perso 51
FCS_CKM.1/Perso_GP 51
FCS_CKM.2 44
FCS_CKM.2/Perso 51
FCS_CKM.4 44
FCS_COP.1/Perso 52
FCS_COP.1/RSA 45
FCS_COP.1/TDES 45
FCS_RNG.1 56
FDP_ACC.2 40
FDP_ACC.2/Perso 52
FDP_ACF.1 40
FDP_ACF.1/Perso 52
FDP_DAU.1 45
FDP_ETC.1 46
FDP_ETC.1/Perso 53
FDP_ETC.2 46
FDP_ITC.1 46
FDP_ITC.1/Perso 53
FDP_RIP.1 47
FDP_SDI.2 39
FDP_UCT.1/Perso 53
FIA_AFL.1/C 47
FIA_AFL.1/Perso 53
FIA_AFL.1/WSC 47
FIA_ATD.1 48
FIA_ATD.1/Perso 54
FIA_UAU.1 48
FIA_UAU.1/Perso 54
FIA_UAU.3 48
FIA_UAU.4 49
FIA_UAU.4/Perso 54
FIA_UAU.7/Perso 54
FIA_UID.1 49
FIA_UID.1/Perso 54
FIA_USB.1 49
FMT_MOF.1/Perso 55
FMT_MTD.1/Perso 55
FMT_SMF.1/Perso 55
FMT_SMR.2/Perso 55
FPR_UNO.1 50
FPT_EMS.1 42
FPT_FLS.1 42
FPT_PHP.3 42
FPT_TDC.1 50
FPT_TST.1 39
FTP_ITC.1 50
FTP_ITC.1/Perso 55

I

Identification__data__(IDD) 24

K

Key__management 59

L

Life__cycle__management 59

O

OE.Personalisation_Phase 30
OE.Tachograph_Components 31
OT.Card_Activity_Storage 29
OT.Card_Identification_Data 29
OT.Data_Access 30
OT.Lifecycle_Security 30
OT.Personalisation_AC 29
OT.Personalisation_Confidentiality 29

OT.Secure_Communications 30
Other__devices 25

P

P.EU_Specifications 27
Physical__protection 60

R

RAD__Management 60
Reference__authentication__data__(RAD) ..24

S

Safe__state__management 60
Secret__messaging__keys__(SMK) 24
Secure__Messaging 60
Self__tests 60
Signature 61
Signature__creation__data__(SCD) 24
Signature__verification__data__(SVD) 24

T

T.Activity_Data..... 27
T.Authentication_Masquerade..... 26
T.Data_Exchange 27
T.Identification_Data 26
T.Personalisation_Data..... 26
TOE__File__system__incl.__specific__identification__data 25

V

Vehicle__Unit 25
Verfication__authentication__data__(VAD) 24