tru/cos tacho v1.0

Security Target

Document Attributes

Author:	Martin Becker
File name:	Security Target trucos tacho v1.0.pdf
Status:	Release
Save date:	19. April 2012
Version:	1.4

Further attributes:	**Sensitivity:**	Public	**Category:**	Specification
	Approved by:			

Remark: The electronic copy always supersedes the print-out!

Document History

Author	Version	Date	Description
Jürgen Scheffer	0.1	06.12.2010	Internal Draft
Jürgen Scheffer	0.9	18.02.2011	Draft for Certification Request
Martin Becker	0.91	21.03.2011	Sec. 1 to 6 completely revised
Martin Becker	0.92	28.03.2011	Sec. 7 (TOE Summary Specification) completed
Martin Becker	0.93	13.04.2011	• Boundary of TOE defined more precisely • SFP, SFR and TSF added for personalisation phase • Comments of evaluator included
Martin Becker	0.94	22.06.2011	• Comments of evaluator included
Martin Becker	0.95	09.08.2011	Change of TOE name
Martin Becker	0.96	24.08.2011	Version of the Security Target of the Infineon IC changed to final version
Martin Becker	0.97	31.08.2011	Sec. 8 (Statement of compatibility) added
Martin Becker	0.98	29.09.2011	New versions V1.0 and V1.01 of /PP0070/ included
Martin Becker	0.99	24.10.2011	Patch loading no longer possible in personalisation phase
Martin Becker	1.0	31.01.2012	• Tachograph Protection Profile /PP0070/ V1.02, 15.11.2011 included • Lists of guidance documents and delivered keys added
Jürgen Scheffer	1.1	02.04.2012	• Changes according BSI Review
Jürgen Scheffer	1.2	12.04.2012	• Changes according BSI Review
Jürgen Scheffer	1.3	16.04.2012	• Changes according BSI Review
Jürgen Scheffer	1.4	19.04.2012	• Changes according BSI Review

Document Approval

	Date	Name / Signature
Technical Release		
Document Release		

Table of Contents

1 ST Introduction (ASE_INT)

This section provides TOE overview information required to enable a potential user of the Security Target (ST) to determine, whether the ST is of interest.

1.1 ST Reference and TOE reference

Title:	Security Target tru/cos tacho v1.0
Version:	1.4
Date:	19. April 2012
Publisher:	Trüb AG
CC Version	Common Criteria Version 3.1
Assurance Level:	EAL4 augmented
Evaluation Body:	TÜV Informationstechnik GmbH (TÜViT)
Certification Body:	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany)

This Security Target refers to the Tachograph Smart Card Product “tru/cos tacho v1.0” provided by the Trüb AG for the Common Criteria Evaluation.

It claims the Common Criteria Protection Profile “Digital Tachograph – Smart Card (Tachograph Card)” /PP0070/, registered by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0070.

The evaluation of the TOE is carried out as a composite evaluation. Therefore the evaluation of the TOE uses the results of the evaluation of the underlying semiconductor Infineon SLE78CX360P /ST_IC/ with cryptographic libraries and with specific IC dedicated software which is certified according common criteria EAL5 under the reference BSI-DSZ-CC-0727-2011 /CR_IC/.

1.2 TOE Overview

1.2.1 TOE Definition and Operational use

The Target of Evaluation (TOE) addressed by this Security Target is the Tachograph Smart Card product “tru/cos tacho v1.0” developed by the Trüb AG in the sense of Annex I(-B) /AIB/, /CorrReg/ intended to be used in the Digital Tachograph Systems which contains additionally Motion Sensors and Vehicle Units as recording equipment.

This Tachograph Smart Card is a smart card which comprises:

- the security controller including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (operating system),

- the Tachograph application depending on the Tachograph Card type (driver card, workshop card, control card or company card) and
- the associated guidance documentation.

The basic functions of the Tachograph Card are:

- to store card identification and cardholder identification data. This data is used by the Vehicle Unit to identify the card holder, provide functions and data access rights accordingly, and ensure card holder accountability for his activities;
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

This Tachograph Card is therefore intended to be used by a card interface device of a Vehicle Unit. It may also be used by any card reader (e.g. of a personal computer) if it has the appropriate access right.

Concerning the write access, during the end-usage phase of the Tachograph Card life-cycle (life-cycle phase 7), only Vehicle Units may write user data to the card.

The functional requirements for this Tachograph Card are specified in Annex I(-B) body text /AIB/, /CorrReg/ and Appendix 2 /AIB-A2/, the common security mechanisms are specified in Appendix 11 /AIB-A11

1.2.2 TOE major Security Features for Operational use

The main security features of the TOE are as specified in /AIB-A10/:

- 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 to protect

- 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 /AIB-A10/, sec. 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 /AIB-A11/, sec. 4.9.

All cryptographic mechanisms including algorithms and the length of corresponding keys have to be implemented exactly as required and defined in EU documents /AIB-A10/ and /AIB-A11/.

1.2.3 TOE Type

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 /AIB/, /CorrReg/, Appendix 2 /AIB-A2/, Appendix 10 /AIB-A10/ and Appendix 11 /AIB-A11/. In particular, this implies the conformance with the following standards:

- ISO/IEC 7810 Identification cards – Physical characteristics
- ISO/IEC 7816 Identification cards - Integrated circuits with contacts:
  - Part 1: Physical characteristics
  - Part 2: Dimensions and location of the contacts
  - Part 3: Electronic signals and transmission protocols
  - Part 4: Inter-industry commands for interchange
  - Part 8: Security related inter-industry commands
- ISO/IEC 10373 Identification cards – Test methods

Following the Tachograph Card Protection Profile /PP0070/, the typical smart card product life-cycle is decomposed in 7 phases as follows:

- Phase 1: Smart Card Embedded Software Development
- Phase 2: IC Design and IC Dedicated Software Development
- Phase 3: IC Manufacturing and testing
- Phase 4: IC Packaging and Testing
- Phase 5: Smart Card Product Finishing Process
- Phase 6: Smart Card Personalisation
- Phase 7: Smart Card Product End-usage

The CC does not prescribe any specific life-cycle model. However, in order to define the application of the assurance classes, the CC assumes the following implicit life-cycle model consisting of three phases:

- TOE development (including the development as well as the production of the TOE)
- TOE delivery
- TOE operational use (including Smart Card Personalisation and Smart Card Product End-usage)

1.2.4 Boundary of the TOE

The module initialisation as part of Phase 5 belongs to the TOE development. The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the Tachograph Card specification /AIB-A2/, but isn't embedded in a plastic card and isn't personalised yet.

Thus, the Phases 1 up to 4 are part of the TOE development in the sense of the CC. The Phases 6 and 7 – Smart Card Personalisation and Smart Card Product End-Usage of the TOE – are part of the operational use in the sense of the CC.

The Phase 5 is part of both, TOE development and operational use: the module initialisation is part of the TOE development, but the embedding of the modules into the plastic card body is part of the operational use in the sense of the CC.

1.2.5 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 the security of the TOE.

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).

1.2.6 Guidance Documentation

Component	Version / Date	Description
AGD_PRE	1.07 / 19.04.2012	tru/cos tacho v1.0 Initialization Manual, Trüb AG
AGD_OPE.Perso	1.06 / 19.04.2012	tru/cos tacho v1.0 Personalization Manual, Trüb AG
AGD_OPE.Enduser	1.0. / 19.04.2012	tru/cos tacho v1.0 Enduser Manual, Trüb AG

1.2.7 Delivered Cryptographic Keys

Key	Descrption
MEK	Master Embedding Key: 3DES key which is unique for each tru/cos tacho v1.0 personalization bureau

1.3 TOE Description

1.3.1 TOE Logical Scope

The main security features of the TOE are as specified in /AIB-A10/:

- 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 to protect

- 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 /AIB-A10/, sec. 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 /AIB-A11/, sec. 4.9.

All cryptographic mechanisms including algorithms and the length of corresponding keys have to be implemented exactly as required and defined in EU documents /AIB-A10/ and /AIB-A11/.

1.3.2 TOE Architecture

The Tachograph Smart Card Product “tru/cos tacho v1.0” is realised as a native operating system written in “C” on the semiconductor Infineon SLE78CX360P with cryptographic libraries and with specific IC dedicated software.

The following figure shows the global architecture of the TOE:

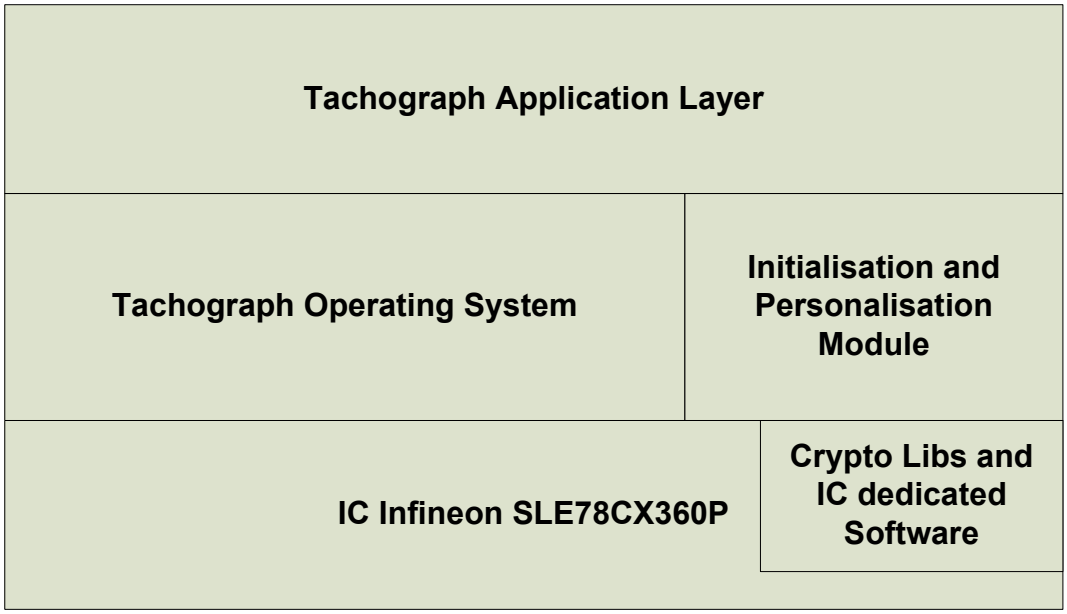


Figure 1: TOE Architecture

Tachograph Application Layer:

The Tachograph Application Layer consists of the card type specific file structure and cryptographic data, accessible in Life-Cycle Phase 7, as specified in /AIB/, /AIB-A2/ and /AIB-A10/.

Tachograph Operating System:

The Tachograph Operating System consists of the executable code necessary for the required Tachograph Card commands and the related security features in Life-Cycle Phase 7 as specified in /AIB/, /AIB-A2/, /AIB-A10/ and /AIB-A11/.

Initialisation and Personalisation Module:

For the initialisation phase of the TOE (Life-Cycle Phase 5) the Smartcard Embedded Software contains a set of initialisation commands which are only accessible during this phase. After completion of initialisation these commands are no longer available.

Initialised cards contain the file structure and cryptographic data of all card types (Driver Card, Workshop Card, Company Card and Control Card). However, the cards are not specialised, i.e. the card type is not set.

For the personalisation phase of the TOE (Life-Cycle Phase 6) the Smartcard Embedded Software contains a set of personalisation commands which are only accessible during this phase. After completion of personalisation these commands are no longer available.

During personalisation phase a special command has to be sent to the TOE as first personalisation command to specialise the TOE to a Driver Card, Workshop Card, Company Card or Control Card.

Furthermore, the Initialisation and Personalisation Module manages the specific states of the TOE's operating system according to specified and unalterable rules.

IC Infineon SLE78CX360P with cryptographic libraries and with specific IC dedicated software:

The IC including cryptographic libraries and IC dedicated software are described in the documentation of IC Designer Infineon Technologies AG, /IC_PRM/, /IC_HRM/, /IC_SEC/ and /IC_ACL/. It is certified according to Common Criteria EAL5, see /ST_IC/ for more details.

1.3.3 TOE Life-Cycle

The following table describes the seven life-cycle phases of the TOE in detail:

Phase	Description
Phase 1: **"Smart Card Embedded Software Development"**	The embedded software of TOE is developed to protect and control the TOE during the Phases 4 to 7. The **Smart Card Embedded Software Developer (Trüb AG)** is responsible for • the Smart Card Embedded Software Development (operating system and Tachograph application) and • the creation of the guidance documentation for the TOE. Therefore the **Smart Card Embedded Software Developer** uses the guidance and security documentation for the IC /IC_PRM/, /IC_HRM/, /IC_SEC/ and /IC_ACL/ and the IC dedicated Software provided and securely delivered by the IC Manufacturer to support the developing of the Smart Card Embedded Software and creating the guidance documentation. The delivery of the Crypto Library from Infineon to Trüb AG has to follow a dedicated secure delivery process covered by ALC_DVS. This Phase 1 is part of the TOE development in the sense of the CC.
Phase 2: **"IC Design and IC Dedicated Software Development"**	The IC Designer (Infineon Technologies AG) • designs the IC, • develops the IC dedicated Software, • provides software and information to the smart card embedded software developer and • receives the smart card embedded software from the developer. The delivery of the embedded software from the developer to the IC Designer has to follow a trusted and verified process. This process is done by using the dedicated secure delivery procedure defined in /CC_SecureX/. From the delivered embedded software, the designed IC and the IC dedicated Software a database is created by the IC Designer. This database is used in the next life-cycle phase to produce the IC. This Phase 2 is part of the TOE development in the

	sense of the CC.
Phase 3: **"IC Manufacturing and Testing"**	The **IC Manufacturer (Infineon Technologies AG)** is responsible for producing the IC following the main steps • IC manufacturing • IC testing Then **IC Manufacturer** generates the mask for the IC manufacturing based on the database created in Life-Cycle Phase 2. The **IC Manufacturer** delivers the produced IC in form of wafers. This Phase 3 is part of the TOE development in the sense of the CC.
Phase 4: **"IC Packaging and Testing"**	The **IC Packing Manufacturer (Infineon Technologies AG)** is responsible for • the IC packing (Production of the Modules) and • testing of the produced modules The **IC Packing Manufacturer** delivers the produced IC in form of modules on reels to the Initialiser and in form of sample cards to the Smart Card Embedded Software Developer. This Phase 4 is part of the TOE development in the sense of the CC.
Phase 5: **"Smart Card Product Finishing Process"**	The **Initialiser (Trüb AG)** is responsible for • module initialisation The **Smart Card Product Manufacturer (Trüb AG or external manufacturer)** is responsible for • embedding of the modules into the card body and • testing of the produced cards This Phase 5 is part of the TOE development (module initialisation) and part of the operational use (embedding of modules and testing of produced cards).
Phase 6: **"Smart Card Personalisation"**	The **Personaliser (Trüb AG or external personaliser)** is responsible for • smart card personalisation and • testing of the produced Tachograph Cards. All test specific functions that are used during the former phases are no longer accessible after personalisation process is completed. This Phase 6 is part of the operational use in the sense of the CC.

Phase 7: **"Smart Card Operational Use"**	The **Smart Card Issuer** is responsible for • the smart card delivery to the end user of the Tachograph Card After the cards have been delivered to the end users they can be used without any restrictions. All test specific functions that are used during the former phases are not accessible because they have been deactivated in his phase. This Phase 7 is part of the operational use in the sense of the CC.

Table 1 TOE Life-Cycle

2 Conformance Claim (ASE_CCL)

2.1 CC Conformance Claim

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

as follows:

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

has to be taken into account.

2.2 PP Claim

This Security Target claims strict conformance with the Common Criteria Protection Profile “Digital Tachograph – Smart Card (Tachograph Card)” /PP0070/, registered by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0070.

As this evaluation is a composite evaluation, the underlying integrated circuit of the TOE (Infineon SLE78CX360P) is certified in accordance with the Security IC Platform Protection Profile /PP0035/, registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.

2.3 Package Claim

This Security Target is conformant to EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see /PP0070/ sec. 6.2 and sec. 6.2 below).

2.4 Conformance Rationale

TOE Type: The TOE in this Security Target as described in sec. 1.2.1 and sec. 1.2.3 above is the very same as the TOE type described in the corresponding sections of /PP0070/.

Security Problem Definition: in this Security Target all assets, assumptions, threats, and organisational security policies from /PP0070/ are reproduced, additionaly T.Unauthorized_Personalisation is defined in this Security Target.

Security Objectives: in this Security Target all security objectives for the TOE and all security objectives for the operational environment from /PP0070/ are reproduced, additionaly the Security Objective OT.Personalisation_Access is defined in this Security Target.

Security requirements: The security assurance requirements from /PP0070/ are fully included in this SecurityTarget, and no further security assurance requirements.
The security functional requirements of /PP0070/ are fully included in this Security Target. Some have been renamed with a suffix “/end_usage” due to an iteration performed in this Security Target. Some additional functional requirements (about additional access control functionality in the personalisation phase) have been added by using iteration operations to this Security Target, these are marked with a suffix “/personalisation”).
Furthermore, the newly introduced SFP named AC_PERSO_SFP was added to the requirement FDP_ITC.1, the newly introduced subject **Non-**Personalisation Unit was added to requirement FIA_AFL.1/C, and the newly introduced attributes PERSO_UNIT and NON_PERSO_UNIT were added to the requirements FIA_USB.1 and FIA_ATD.1 instead of iterating these requirement components, which would be equivalent but would have unnecessarily expanded the statement of SFRs in this Security Target).

3 Security Problem Definition (ASE_SPD)

Application note 1: Although each of the Tachograph Card types (driver card, workshop card, control card or company card) is used in different environment the aspects of the Security Problem Definitions are described in general for the Tachograph Card considering the whole Digital Tachograph Systems and the corresponding usage of Tachograph Cards

3.1 Introduction

3.1.1 Assets

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

Object No	Asset	Definition	Generic security property to be maintained by the TOE
1	Identification data (IDD)	Primary asset: card identification data, cardholder identification data (see Glossary for more details)	Integrity
2	Activity data (ACD)	Primary asset: cardholder activities data, events and faults data and control activity data (see Glossary for more details)	Integrity, Authenticity, for parts of the activity data also Confidentiality
3	Signature creation data (SCD)	Secondary asset: private key used to perform an electronic signature operation	Confidentiality, Integrity
4	Secret messaging keys (SMK)	Secondary asset: session keys (TDES) used to protect the Tachograph Card communication by means of secure messaging	Confidentiality, Integrity
5	Signature verification data (SVD)	Secondary asset: public keys certified by Certification Authorities, used to verify electronic signatures	Integrity, Authenticity
6	Verification authentication data (VAD)	Secondary asset: authentication data provided as input for authentication attempt as authorised user (PIN)	Confidentiality (This security property is not maintained by the TOE but by the TOE environment)
7	Reference authentication data (RAD)	Secondary asset: data persistently stored by the TOE for verification of the authentication attempt as authorised user	Confidentiality, Integrity
8	Data to be signed (DTBS)	Secondary asset: the complete electronic data to be signed (including both user message and signature attributes)	Integrity, Authenticity
9	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	Integrity

Table 2: Assets to be protected by the TOE and its environment

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 /AIB-A10/ defines “sensitive data” which include security data and user data as data stored by the Tachograph Card that need to be protected for integrity, unauthorised modification and confidentiality. User data include identification data and activity data and match User Data in the sense of the CC. Security data are defined as specific data needed to support security enforcing and match the TSF data in the sense of the CC.

3.1.2 Subjects and external entities

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

External Entity No.	Subject No.	Role	Definition
1	1	Administrator	S.Administrator: the subject is usually active only during Initialisation/Personalisation (Phase 6) – listed here for the sake of completeness.
2	2	Vehicle Unit	S.VU: Vehicle Unit (with a UserID) which the Tachograph Card is connected to.
3	3	Non Vehicle Unit	S.Non-VU: Other device (without UserID) which the Tachograph Card is connected to.
4	-	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 assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential.

Table 3: Subjects and external entities

Application note 2: This table defines the subjects in the sense of /CC1/ 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 /CC1/). From this point of view, the TOE itself does not differ between ‘subjects’ and ‘external entities’.

3.2 Threats

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

The Threats for the Tachograph Card are taken form the Protection Profile /PP0070/.

Threat name	Description

T.Unauthorised_Personalisation	**Personalisation without being authorised** A successful personalisation of initialised copies of the TOE while not being authorised would be a threat to the security of the TOE. The threat agent for **T.Unauthorised_Personalisation** is Attacker.
T.Identification_Data	**Modification of Identification Data** A successful modification of identification data held by the TOE (IDD, see sec., 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, see sec. 3.1, deletion, addition or modification) during import or export would be a threat to the security of the TOE. The threat agent for T.Data_Exchange is Attacker.
T.Personalisation_Data	**Disclosure or Modification of Personalisation 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.

Table 4: Threats

3.3 Organisational Security Policy

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.

Security Policy	Description
P.EU_Specifications	**EU Specifications Conformance**

	All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/. 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.

Table 5: Organisational Security Policies (OSP)

3.4 Assumptions

Security always concerns the whole system the weakest element of the chain determines the total system security. Assumptions described hereafter have to be considered for a secure system using Smart Card products.

Assumption	Description
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 /AIB-A2/ 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.

Table 6: Assumptions

4 Security Objectives (ASE_OBJ)

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

The security objectives for the TOE (OT) and the security objectives for the TOE environment (OE) will be defined in the following form

- **OT/OE.Name Description**

4.1 Security Objectives for the TOE

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

Security Objective	Description
OT.Personalisation_Access	**Personalisation Access Limitation** The TOE must limit write access to initialised copies of the TOE to authenticated personalisers.
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 /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/.
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 /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/.
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 /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/.
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 /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/.

Table 7: Security Objectives for the TOE

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:

Security Objective	Description
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 /AIB-A2/ 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.
OE.Tachograph_Components	**Implementation of Tachograph Components** All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents /AIB/, /CorrReg/, /AIB-A2/, /AIB-A10/ and /AIB-A11/. 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.

Table 8: Security Objectives for the Operational Environment

4.3 Security Objective Rationale

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

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

Table 9: Security Objective Rationale

A detailed justification required for suitability of the security objectives to cope with the security problem definition is given below.

T.Unauthorised_Personalisation is addressed by OT.Personalisation_Access. Limitation of personalisation of initialised copies of the TOE to personalisers only directly counters the threat T.Unauthorized_Personalisation.

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

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

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

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

data as well as the disclosure of cryptographic material during the execution of the personalisation process.

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

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

5 Extended Component Definitions (ASE_ECD)

The Protection Profile /PP0070/ uses one component defined as extension to CC part 2. It is defined in the same way as in most smart card PPs, for example in /ICAO-PP/, registered and certified by BSI under the reference BSI-CC-PP-0056.

5.1 Definition of the Family FPT_EMS

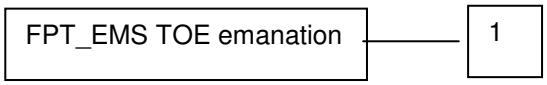
The family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based 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 /CC2/.

The family "TOE Emanation (FPT_EMS)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 Security Requirements (ASE_REQ)

This chapter defines the detailed security requirements of the TOE. This statement defines the functional and assurance security requirements that the TOE satisfies in order to meet the security objectives for the TOE.

The CC allows several operations to be performed on security requirements (on the component level); *refinement, selection, assignment* and *iteration* are defined in paragraph 8.1 of Part 1 of the CC /CC-1/. All these operations are used in this ST.

The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the ST author are denoted by showing as ***underlined bold text in italics***.

The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the ST author are denoted by showing as **underlined bold text**.

The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. In order to trace elements belonging to a component, the same slash "/" with iteration indicator is used behind the elements of a component.

The operations already performed in the underlying PP are not highlighted, but the operations additionally done in the ST (in comparison to the PP) are identified by editorial means.

6.1 Security Functional Requirements (SFRs)

This chapter defines the detailed security functional requirements for the TOE using functional requirements components as specified in /PP0070/. Furthermore, the ST contains additional requirements needed for the personalisation phase. These extensions are denoted by showing as *text in italics*. The Requirements for the IC are not covered by this chapter because they are defined in the security target /ST_IC/ for the IC including the crypto library.

6.1.1 Security Function Policy

6.1.1.1 Security Function Policy Personalisation Access Control (AC_PERSO_SFP)

*The **Security Function Policy Personalisation Access Control (AC_PERSO_SFP)** for Tachograph Cards in personalisation phase is defined as follows:*

*The **SFP AC_PERSO_SFP** is only relevant for the Personalisation phase of the Tachograph Card.*

Subjects:

- *Personalisation Unit*
- *Non- Personalisation Unit (other card interface devices)*

Security attributes for subjects:

- *USER_GROUP (PERSO_UNIT, NON_PERSO_UNIT)*

Objects:

- *data fields for user data:*
  - *identification data (card identification data, cardholder identification data)*

- *data fields for security data:*
  - *card'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)*
  - *PIN (for workshop card only)*
  - *SYSTEM key as personalisation key*

- *security data:*
  - *SYSTEM key as personalisation key*

- *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*

- *life-cycle state of the TOE*

Security attributes for objects:

- *Access Rules based on implicitly defined Access Conditions (see below) for:*
  - *data fields for user data*
  - *data fields for security data*
  - *life-cycle state of the TOE*

Operations:

- *data fields for user data:*
  - *identification data: selecting (command Select), writing (commands Update Binary, Put Data),*

- *data fields for security data:*
  - *card's private signature key: writing (command Put Data),*
  - *public keys: writing (command Put Data)*
  - *PIN (for workshop card only): writing (command Put Data)*
  - *SYSTEM key: writing (command Change Reference Data)*

- *security data:*
  - *SYSTEM key: external authentication (command External Authenticate)*
  - *SYSTEM Key: change (command Change Reference Data)*

- *TOE file system (incl. file structure, additional internal structures, access conditions):*
  - *administrate/change access conditions (command Put Data)*

- *identification data of the TOE: read (command Get Data)*

- *personalisation identification data of the TOE: update (command Update Binary)*

- *life-cycle state of the TOE*
  - *Switch of the life-cycle state (command Card Ready)*

Access Rules:

*The **SFP AC_PERSO_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 the object. The following conditions are defined:*

- *Implicit ALW (Always) - The commands Get Data, Select File and External Authenticate with the SYSTEM key can be executed without restrictions.*

- *AUT (Key based authentication) - The commands Card Ready, Change Reference Data, Put Data and Update Binary can be executed only if the preceding external authentication (done by the command External Authenticate with the SYSTEM key) has been conducted successfully.*

- *NEV (Never) – Writing of data fields with AC NEV by using the commands Put Data and Update Binary is never allowed.*

6.1.1.2 Security Function Policy Access Control (AC_SFP)

The **Security Function Policy Access Control (AC_SFP)** for Tachograph Cards in the end-usage phase based on the Tachograph Cards Specification /AIB-A2/, sec. 3 and 4, GST /AIB-A10/, sec. 4.3.1 and 4.3.2 as well as /JIL/, 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 the card has been completed.

Subjects:

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

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

Security attributes for subjects:

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

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

Objects:

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

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

Security attributes for objects:

- Access Rules based on defined Access Conditions (see below) for:
  - user data

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

Operations:

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

- security data:
    - card's private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication (command External Authenticate)
    - public keys (in particular card's public signature key): referencing over a MSE command (for further usage within cryptographic operations as authentication, verification of a digital signature etc.)
    - session keys: securing of commands with Secure Messaging
    - PIN (only relevant for Workshop Card): verification (command Verify PIN)
- TOE software code: No Operations
- TOE file system (incl. file structure, additional internal structures, access conditions): No Operations
- identification data of the TOE: selecting and reading
- identification data of the TOE's personalisation (date and time of personalisation): selecting and reading

Access Rules:

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access the object. The possible commands are described in the Tachograph Card specification /AIB-A2/, sec 3.6. Following Access Conditions are defined in the Tachograph Card specification /AIB-A2/, 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 /AIB-A2/, sec 3.6 and Tachograph Common Security Mechanisms /AIB-A11/, sec. 5.
- AUT and PRO SM (combined, see description above)

For each type of Tachograph Card the Access Rules (which make use of the Access Condition described above) for the different objects are implemented according to the requirements in the Tachograph Card Specification /AIB-A2/, sec. 4 and GST /AIB-A10/, 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.

6.1.2 CLASS FAU SECURITY AUDIT

FAU_SAA Security audit analysis

FAU_SAA.1 Potential violation analysis {chapter 4.5 of /AIB-A10/} Hierarchical to: No other components Dependencies: FAU_GEN.1 Audit data generation	
FAU_SAA.1.1	The TSF shall be able to detect failure events as cardholder authentication failures, self test errors, stored data integrity errors and activity data input integrity errors, to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events : 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) **no other rules**

Application Note 3: 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.

6.1.3 CLASS FCO COMMUNICATION

FCO_NRO Non-Repudiation of Origin

FCO_NRO.1 Selective proof of origin {chapter 4.8.2 of /AIB-A10/, DEX_304, DEX_305, DEX_306} Hierarchical to: No other components Dependencies: FIA_UID.1 Timing of identification	
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 Mechanism /AIB-A11/, sec. 6, CSM_035.

6.1.4 CLASS FCS CRYPTOGRAPHIC SUPPORT

FCS_CKM Cryptographic key management

FCS_CKM.1 Cryptographic Key generation {chapter 4.9 of /AIB-A10/, CSP_301} Hierarchical to: No other components. Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	
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 /AIB-A11/, sec. 3, CSM_012, CSM_013 **(refinement: session key validity shall expire at the end of the session (withdrawal of the card or reset of the card) or after 240 uses (one use of the key = one command using secure messaging sent to the card and associated response), whichever event occurs first)**, CSM_015, CSM_020.

FCS_CKM.2 Cryptographic key distribution {chapter 4.9 of /AIB-A10/, CSP_302} Hierarchical to: No other components. Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_CKM.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 /AIB-A11/ , sec. 3, CSM_012, CSM_013 CSM_015, CSM_020 and Tachograph Card Specification /AIB-A2/, sec. 3.6.

FCS_CKM.4 Cryptographic key destruction {chapter 4.9 of /AIB-A10/, CSP_301} Hierarchical to: No other components Dependencies: [FCS_ITC.1 Import of user data without security attributes, or FCS_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **erasing of the stored key value** that meets the following: Tachograph Common Security Mechanism /AIB-A11/, sec. 3, CSM_013 **(session key validity shall expire at the end of the session (withdrawal of the card or reset of the card) or after 240 uses (one use of the key = one command using secure messaging sent to the card and associated response), whichever event occurs first)**, and Tachograph Card Specification /AIB-A2/, sec. 3.6.

FCS_COP Cryptographic operation

FCS_COP.1/RSA Cryptographic operation {CSM_003 and further chapters of /AIB-A11/} Hierarchical to: No other components Dependencies: [FCS_ITC.1 Import of user data without security attributes, or FCS_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1.1/RSA	The TSF shall perform the cryptographic operations (encryption, decryption, signature creation and signature verification as well as certificate verification for the authentication between the Tachograph Card and the Vehicle Unit and signing for downloading to external media) in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes of 1024 bits that meet the following: [Tachograph Common Security Mechanisms /AIB-A11/, 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 /AIB-A2/, sec. 3.

FCS_COP.1/TDES Cryptographic operation {CSM_002 and further chapters of /AIB-A11/} Hierarchical to: No other components Dependencies: [FCS_ITC.1 Import of user data without security attributes, or FCS_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
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 /AIB-A11/, sec. 2, CSM_005, sec. 3, CSM_015, sec. 5, CSM_021- CSM_031 and Tachograph Card Specification /AIB-A2/, sec. 3.

6.1.5 CLASS FDP USER DATA PROTECTION

FDP_ACC Access control policy

FDP_ACC.2/personalisation Complete access control {chapter 4.3.1, ACT_301, ACT_302, chapter 4.4 of /AIB-A11/ as well as /JIL/, sec. 2.6} Hierarchical to: FDP_ACC.1 Subset access control Dependencies: FCS_ACF.1 Security attribute based access control	
FDP_ACC.2.1/ personalisation	The TSF shall enforce the **AC_PERSO_SFP** on **subjects:** • **Personalisation Unit** • **Non-Personalisation Unit (other card interface devices)** **objects:** • **data fields for user data:** ○ **identification data (card identification data, cardholder identification data)** • **data fields for security data:** ○ **card'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)** ○ **PIN (for workshop card only)** ○ **SYSTEM key as personalisation key** • **security data:** ○ **SYSTEM key as personalisation key** • **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** • **life-cycle state of the TOE** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/personalisation	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_ACC.2/end_usage Complete access control {chapter 4.3.1, ACT_301, ACT_302, chapter 4.4 of /AIB-A11/ as well as /JIL/, sec. 2.6} Hierarchical to: FDP_ACC.1 Subset access control Dependencies: FCS_ACF.1 Security attribute based access control	

FDP_ACC.2.1/end usage	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/end_usage	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 Access control functions

FDP_ACF.1/personalisation Security attribute based access control {chapters 3.3 and 4 of /AIB-A2/, chapter 4.3.2, ACT_301, ACT_302, chapter 4.4 of /AIB-A10/ as well as /JIL/, sec. 2.6} Hierarchical to: No other components Dependencies: FCS_ACC.1 Subset access control FCS_MSA.3 Static attribute initialisation	
FDP_ACF.1.1/ personalisation	The TSF shall enforce the **AC_PERSO_SFP** on **subjects:** • **Personalisation Unit** • **Non- Personalisation Unit (other card interface devices)** **objects:** • **data fields for user data:**

	○ **identification data (card identification data, cardholder identification data)** • **data fields for security data:** ○ **card'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)** ○ **PIN (for workshop card only)** ○ **SYSTEM key as personalisation key** • **security data:** ○ **SYSTEM key as personalisation key** • **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** • **life-cycle state of the TOE** • **security attributes for subjects:** ○ **USER_GROUP** • **security attributes for objects:** ○ **Access Rules**
FDP_ACF.1.2/ personalisation	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/ personalisation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ personalisation	The TSF shall explicitly deny access of subjects to object based on the following additional rules: **none**.

FDP_ACF.1/end_usage Security attribute based access control {chapters 3.3 and 4 of /AIB-A2/, chapter 4.3.2, ACT_301, ACT_302, chapter 4.4 of /AIB-A10/ as well as /JIL/, sec. 2.6} Hierarchical to: No other components Dependencies: FCS_ACC.1 Subset access control FCS_MSA.3 Static attribute initialisation	

FDP_ACF.1.1/ end usage	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:
	  ○ 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
	• security attributes for subjects:
	  ○ USER_GROUP
	  ○ USER_ID
	• security attributes for objects:
	  ○ Access rules

FDP_ACF.1.2/ end usage	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/ end usage	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ end usage	The TSF shall explicitly deny access of subjects to object based on the following additional rules: none.

FDP_DAU Data authentication

FDP_DAU.1 Basic Data Authentication {chapter 4.6.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies.	
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.

FDP_ETC Export from the TOE

FDP_ETC.1 Export of user data without security attributes {chapter 4.3.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]	
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.

FDP_ETC.2 Export of user data with security attributes {DEX_304, DEX_305, DEX_306, chapter 4.8 of /AIB-A10/} Hierarchical to: No other components Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	
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.

FDP_ITC Import from outside of the TOE

FDP_ITC.1 Import of user data without security attributes {chapters 4.3.1 and 4.3.2, RLB_305, chapter 4.7.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: [FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FCS_MSA.3 Static attribute initialisation	
FDP_ITC.1.1	The TSF shall enforce the AC_SFP **and AC_PERSO_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.

FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {RLB_306, RLB_307, chapter 4.7 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource from*** the following objects: **cryptographic keys, PINs**.

FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action {chapter 4.6.1 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors before accessing** on all objects, based on the following attributes: **integrity checked stored data**.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall warn the entity connected.

6.1.6 CLASS FIA IDENTIFICATION AND AUTHENTICATION

FIA_AFL Authentication failures

FIA_AFL.1/C Authentication failure handling {UIA_301, chapter 4.2.2 of /AIB-A10/, chapter 4.2.3 of /AIB-A10/} Hierarchical to: No other components Dependencies: FIA_UAU.1 Timing of authentication	
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 (**in end-usage phase) and as Non-Personalisation unit (in personalisation phase)**.

FIA_AFL.1/WSC Authentication failure handling {UIA_302, chapter 4.2.2 of /AIB-A10/, chapter 4.2.3 of /AIB-A10/} Hierarchical to: No other components Dependencies: FIA_UAU.1 Timing of authentication

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.

FIA_ATD User attribute definition

FIA_ATD.1 User attribute definition {chapter 4.2.1 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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, **PERSO_UNIT, NON_PERSO_UNIT**) • USER ID (VRN and Registering MSC for subject S.VU).

Note: FIA_ATD.1 is not iterated, see sec.2.4 for more information

FIA_UAU User Authentication

FIA_UAU.1 Timing of authentication {UIA_301, chapter 4.2.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: FIA_UID.1 Timing of identification	
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.

FIA_UAU.3 Unforgeable authentication {UIA_301, chapter 4.2.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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.

FIA_UAU.4 Single-use authentication mechanisms {UIA_301, chapter 4.2.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to key based authentication mechanism.

FIA_UID User identification

FIA_UID.1 Timing of Identification {chapter 4.2.1 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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 4: 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 User-subject binding

FIA_USB.1 User-subject binding {chapters 4.3.1, 4.7.2 (RLB_304, RLB_305) of /AIB-A10/} Hierarchical to: No other components Dependencies: FIA_ATD.1 User attribute definition	
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, **PERSO_UNIT, NON_PERSO_UNIT**) • 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: **usage of TOE's access rule mechanism**
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: **no changes of user security attributes possible**.

Note: FIA_USB.1 is not iterated, see sec.2.4 for more information

6.1.7 CLASS FPR PRIVACY

FPR_UNO Unobservability

FPR_UNO.1 Unobservability {RLB_304, chapter 4.7.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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.

6.1.8 CLASS FPT Protection of the TSF

FPT_EMS TOE Emanation

FPT_EMS.1 TOE Emanation {RLB_304, chapter 4.7.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FPT_EMS.1.1	The TOE shall not emit **power variations, timing variations during command execution** in excess of **non-useful information** enabling access to private key(s) and session keys and **PIN (workshop card only) and activity data**.
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 **PIN (workshop card only) and activity data**.

FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state {RLB_306, chapter 4.7.3, RLB_307, chapter 4.7.4 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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)

FPT_PHP TSF physical protection

FPT_PHP.3 Resistance to physical attack {RLB_304, chapter 4.7.2 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to all TOE components implementing the TSF by responding automatically such that the SFRs are always enforced.

Application note 5: 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.

FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1 Inter-TSF basic TSF data consistency {DEX_301, DEX_302, DEX_303, chapter 4.8.1 of /AIB-A10/, chapter 5.3 of /AIB-A11/} Hierarchical to: No other components Dependencies: No dependencies	
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 Mechanism /AIB-A11/, and Tachograph Card Specification /AIB-A2/, sec. 3.6 when interpreting the TSF data from another trusted IT product.

FPT_TST TSF self test

FPT_TST.1 TSF testing {RLB_301, RLB_302, RLB_303, chapter 4.7.1 of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

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

6.1.9 CLASS FTP TRUSTED PATH/CHANNELS

FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel {DEX_301, DEX_302, DEX_303, chapter 4.8.1of /AIB-A10/} Hierarchical to: No other components Dependencies: No dependencies	
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.

6.2 Security Assurance Requirements (SARs)

The security assurance requirements are based on the assurance package E3hCC31_AP as defined in /PP0070/.

Assurance Classes	Assurance Family	E3hCC31_AP (based on EAL4)
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_INT	-
	ADV_TDS	3
	ADV_SPM	-
Guidance Documents	AGD_OPE	1
	AGD_PRE	1
Life-Cycle Support	ALC_CMC	4
	ALC_CMS	4
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	ATE_FUN	1
	ATE_IND	2
Vulnerability Assessment	AVA_VAN	5

Table 10: Assurance package E3hCC31_AP

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 6: The requirement {RLB_304} is partially covered by ADV_ARC (self-protection).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.Personalisation_Access	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communications
FAU_SAA.1		X	X		X
FCO_NRO.1					X
FCS_CKM.1					X
FCS_CKM.2					X
FCS_CKM.4					X
FCS_COP.1/RSA					X
FCS_COP.1/TDES					X
FDP_ACC.2/personalisation	X				
FDP_ACC.2/end_usage		X	X	X	X
FDP_ACF.1/personalisation	X				
FDP_ACF.1/end_usage		X	X	X	X
FDP_DAU.1					X
FDP_ETC.1					X
FDP_ETC.2					X
FDP_ITC.1					X
FDP_RIP.1					X
FDP_SDI.2		X	X		
FIA_AFL.1/C	X			X	
FIA_AFL.1/WSC				X	
FIA_ATD.1	X			X	
FIA_UAU.1	X			X	
FIA_UAU.3	X			X	X
FIA_UAU.4					X
FIA_UID.1	X			X	
FIA_USB.1	X			X	
FPR_UNO.1					X
FPT_EMS.1	X	X	X	X	X
FPT_FLS.1	X	X	X	X	X
FPT_PHP.3	X	X	X	X	X
FPT_TDC.1					X
FPT_TST.1	X	X	X	X	X
FTP_ITC.1					X

Table 11: Coverage of Security Objectives for the TOE by SFRs

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

According to the security objective **OT.Personalsation_Access**, the TOE limits the write access to initialised copies of the TOE in the TOE's personalisation phase to authenticated personalisers only. The access to the TOE file system in this phase is regulated by the security function policy AC_PERSO_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2/personalisation and

FDP_ACF.1/personalisation, restricts explicitly the write access to authenticated personalisers, i.e. personalisation units. The components FIA_USB.1 and FIA_ATD.1 with their definition of the user security attributes supply a distinction between personalisation units and non-personalisation units. The components FIA_UID.1 and FIA_UAU.1 ensure that especially write access during personalisation is not possible without a preceding successful authentication process. If the authentication fails, the component FIA_AFL.1/C reacts with a warning to the connected entity, and the user will be assumed as different from a personaliser. The component FIA_UAU.3 prevents the use of forged authentication data. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to personalisation write access.

According to the security objective **OT.Card_Identification_Data**, the TOE preserves card identification data and cardholder identification data stored during card personalisation process as specified by the EU documents. The access to the TOE's data, especially to the identification data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2/end_usage and FDP_ACF.1/end_usage, denies explicitly the write access to personalised identification data. The integrity of the stored data within the TOE, especially the integrity of the identification data is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1 (as single failure event or in combination with other failure events), the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the stored identification data and their modification.

According to the security objective **OT.Card_Activity_Storage**, the TOE preserves user data stored in the card by Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2/end_usage and FDP_ACF.1/end_usage, restricts explicitly the write access to user data to authenticated Vehicle Units. The integrity of the stored data within the TOE, especially the integrity of the user data written by Vehicle Units is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1, the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the user data written by Vehicle Units and their modification.

According to the security objective **OT.Data_Access**, the TOE limits the user data write access in the TOE's end-usage phase to authenticated Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2/end_usage and FDP_ACF.1/end_usage, restricts explicitly the write access to user data to authenticated Vehicle Units. The components FIA_USB.1 and FIA_ATD.1 with its definition of the user security attributes supply a distinction between Vehicle Units and other card interface devices. The components FIA_UID.1 and FIA_UAU.1 ensure that especially write access to user data is not possible without a preceding successful authentication process. If the authentication fails, the component FIA_AFL.1/C resp. FIA_AFL.1/WSC reacts with a warning to the connected entity, and the user will be assumed as different from a Vehicle Unit. The component FIA_UAU.3 prevents the use of forged authentication data. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to user data write access.

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

The component FTP_ITC.1 together with FDP_ETC.1 and FDP_ITC.1 offers the possibility to secure the data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel assuring identification of its end points and protection of the data transfer from modification and disclosure. Hereby, both parties are capable of verifying the received data with regard to their integrity and authenticity. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys which is covered by the components FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1/RSA for cryptographic support. The cryptographic component FCS_COP.1/TDES realise the securing of the data exchange itself. The components FPR_UNO.1 guarantees for the unobservability of the install process of

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

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

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

6.3.2 SFR Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The table below shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAA.1	FAU_GEN.1 Audit data generation	justification 1 for non-satisfied dependencies
FCO_NRO.1	FIA_UID.1 Timing of identification	FIA_UID.1
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2, FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FCS_COP.1/RSA	[FDP_ITC.1 Import of user data without	justification 2 for non-satisfied

	security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	dependencies
FCS_COP.1/TDES	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FDP_ACC.2/personalisation	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/personalisation
FDP_ACC.2/end_usage	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/end_usage
FDP_ACF.1/personalisation	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation	FDP_ACC.2/personalisation, justification 3 for non-satisfied dependencies
FDP_ACF.1/end_usage	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation	FDP_ACC.2/end_usage, justification 3 for non-satisfied dependencies
FDP_DAU.1	No dependencies	-
FDP_ETC.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	FDP_ACC.2/end_usage
FDP_ETC.2	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	FDP_ACC.2/end_usage
FDP_ITC.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.2/end_usage, FDP_ACC.2/personalisation, justification 3 for non-satisfied dependencies
FDP_RIP.1	No dependencies	-
FDP_SDI.2	No dependencies	-
FIA_AFL.1/C	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_AFL.1/WSC	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.3	No dependencies	-
FIA_UAU.4	No dependencies	-
FIA_UID.1	No dependencies	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FPR_UNO.1	No dependencies	-
FPT_EMS.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FPT_TDC.1	No dependencies	-
FPT_TST.1	No dependencies	-
FTP_ITC.1	No dependencies	-

Table 12: Dependency rationale overview

Justifications for non-satisfied dependencies:

Justification 1: The dependency FAU_GEN.1 (Audit Data Generation) is not applicable to the TOE. Tachograph Cards do not generate an audit record but react with an error response resp. reset. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.

Justification 2: The SFR FCS_COP.1/RSA uses keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFRs is needed to be defined for this specific instantiations of FCS_COP.1/RSA.

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

6.3.3 Security Assurance Requirements Rationale

The current ST is claimed to be conformant with the assurance package E3hCC31_AP (cf. sec. 2.3 above). As already noticed there in sec. 6.2, the assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

The main reason for the choice of the package E3hCC31_AP is the legislative framework /JIL/, where the assurance level required is defined in form of the assurance package E3hAP (for CCv2.1). The author of /PP0070/ only translated this assurance package E3hAP into the assurance package E3hCC31_AP in accordance with the current version 3.1 of the CC (/CC3/). These packages are commensurate with each other.

The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects and external entities, entry ‘Attacker’). This decision represents a part of the conscious security policy for the Tachograph Cards required by the legislative /AIB/, /CorrReg/ and reflected by the current PP.

The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependencies fulfilled by
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1

	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 13: SAR Dependencies

The refinement added to the chosen SAR package (refer to sec. 6.2) addresses the flexibility of the ST related to the TOE's delivery. In dependency on the chosen time point of the TOE's delivery, the developer documentation and evidence has to be set-up appropriately and the evaluation body is in charge of examining the provided developer evidence for suitability in relationship to the TOE's delivery model.

6.3.4 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

a) SFRs

The dependency analysis in section 6.3.2 SFR Dependency Rationale for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. Furthermore, the current ST accurately and completely reflects the Generic Security Target /AIB-A10/. Since the GST /AIB-A10/ is part of the related legislation, it is assumed to be internally consistent. Therefore, due to conformity between the current ST and /AIB-A10/, also subjects and objects being used in the current ST are used in a consistent way.

b) SARs

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 6.3.2 SFR Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification (ASE_TSS)

7.1 TOE Security Functions

This section provides a description of the TOE's Security Functions, which show how the TOE covers the SFRs of section 6.1.

The Security Functions are grouped into the following categories:

- **Card Personalisation**
- **Cryptographic Operations**: authentication, PIN verification, secure messaging, certificate verification/unwrapping, creation and verification of digital signature and hash calculation
- **Access Control**
- **Protection Mechanisms**: integrity, self tests, data erasure, hardware and further software protection mechanisms

7.1.1 Card Personalisation

SF.PERSO **Card Personalisation**

In the personalisation phase only a limited set of personalisation commands is available.

As an implicitly defined Access Rule an external authentication (command EXTERNAL AUTHENTICATE) is necessary. The Tachograph Card uses the triple DES SYSTEM key for this authentication.

The EXTERNAL AUTHENTICATE command decrypts a cryptogram given by the IFD to recover an eight byte random number and verifies this random number with the random number stored in the card. The external authenticate procedure needs a preceding GET CHALLENGE command to create and store the used random number by using the TRNG of the IC.

A successful performed EXTERNAL AUTHENTICATE command sets a security state.

An unsuccessful external authentication does not set the security state and warns the entity connected in the response to the EXTERNAL AUTHENTICATE command.

If the security state for a successfully performed EXTERNAL AUTHENTICATE command is set then the personalisation data can be written to the card as defined by the SFP Personalisation Access Control (AC_PERSO_SFP) in sec. 6.1.1. The commands UPDATE BINARY, PUT DATA and CHANGE REFERENCE DATA are used to write user and security data, the command CARD READY finishes the personalisation phase and changes the life-cycle state to end usage phase.

7.1.2 Cryptographic Operations

SF.MUT_AUTH **Mutual Authentication**

The TOE provides the functionality of mutual authentication, i.e. the IFD can authenticate itself against the Tachograph Card (external authentication, EXTERNAL AUTHENTICATE command) and vice versa (internal authentication, INTERNAL AUTHENTICATE command).

Each party shall demonstrate to the other that it owns a valid RSA key pair, the public key of which has been certified by a Member State certification authority, itself being certified by the European certification authority.

The Tachograph Card obtains the public key of the IFD by a VERIFY CERTIFICATE command. VERIFY CERTIFICATE is covered by the TSF SF.CERT.

The Tachograph Card uses its own card specific RSA private key.

The INTERNAL AUTHENTICATE command computes an encrypted digital signature of a concatenation of IFD and Tachograph Card known data which contain random numbers and a hash value. The Tachograph Card creates the random numbers by using the True Random Number Generator (TRNG) of the IC. The used hash algorithm is SHA-1.

The EXTERNAL AUTHENTICATE command decrypts and verifies a digital signature given by the IFD to recover a concatenation of IFD and Tachograph known data containing a hash and random values. The Tachograph Card verifies the data and the hash value. The used hash algorithm is SHA-1. The external authenticate procedure needs a preceding GET CHALLENGE command to create a random number by using the TRNG of the IC.

A successful performed EXTERNAL AUTHENTICATE command sets a security state used by the TSF SF.ACC.

An unsuccessful external authentication resets all security states and warns the entity connected in the response to the EXTERNAL AUTHENTICATE command.

Furthermore, EXTERNAL AUTHENTICATE creates a TDES Session Key according to SF.KEY_GEN.

The key size of the modulus of the RSA key pair is 1024 bit.

SF.VERIFY **PIN Verification**

The TOE authenticates the user by a card holder verification (VERIFY command). The VERIFY command initiates the comparison of the PIN sent within the command data with the reference PIN stored in the card.

A successful performed card holder verification command sets a security state used by the TSF SF.ACC.

The number of unsuccessful card holder verification is limited, i.e. after 5 unsuccessful authentication attempts the TSF warns the entity connected, blocks the PIN check procedure and indicates to subsequent users the reason of the blocking by returning an adequate error code.

The runtime of the card holder verification is independent of the comparison data and of the verification result. Thus, the card holder verification is resistant against timing attacks (TSF SF.SW_PROTECTION).

SF.SM **Secure Messaging**

The TOE provides a trusted channel / secure messaging mechanism by using a Session Key created by a previous mutual authentication (TSF SF.MUT_AUTH). Commands and responses can be protected by a cryptographic checksum to ensure integrity and by encryption of data to ensure confidentiality.

Secure messaging is used by the Tachograph application to read or update file data using READ BINARY and UPDATE BINARY commands.

The cryptographic algorithm is TDES in CBC mode with ICV=0 and cryptographic key sizes of 128 bits with 112 effective bits.

SF.CERT **Certificate verification and unwrapping**

The Tachograph Card obtains the public key by a VERIFY CERTIFICATE command which also checks the validity of the public key.

When a VERIFY CERTIFICATE command is successful, the public key is stored in the security environment of the Tachograph Card for future use. This key can be set for the use in security related commands by the MANAGE SECURITY ENVIRONMENT command. Security related commands are INTERNAL / EXTERNAL AUTHENTICATE (TSF SF.MUT_AUTH), PSO: VERIFY DIGITAL SIGNATURE (TSF SF.SIG) or another VERIFY CERTIFICATE.

The public key is presented to the Tachograph Card in a non self-descriptive Card Verifiable certificate signed by a certification authority by using RSA.

The key size of the modulus used to create and verify the certificate is 1024 bit.

SF.SIG **Digital Signature Creation and Verification**

The TOE can create a digital signature of a hash value previously computed and stored in the card by the command PERFORM HASH OF FILE (TSF SF.HASH). The command which performs the signature creation is PSO: COMPUTE DIGITAL SIGNATURE. It uses the Tachograph Card specific RSA private key.

The TOE can verify a digital signature sent to the Tachograph Card with a PSO: VERIFY DIGITAL SIGNATURE command. PSO: VERIFY DIGITAL SIGNATURE uses the public key stored into the card by PSO: VERIFY CERTIFICATE (TSF SF.CERT) and selected by the command MANAGE SECURITY ENVIRONMENT. PSO: VERIFY DIGITAL SIGNATURE also uses a hash value previously stored into the card by a PSO: HASH command.

The TOE uses the signature scheme with appendix RSASSA-PKCS1-v1_5 according to /RSA-PKCS#1/. The key size of the modulus is 1024 bit.

SF.HASH **Hash Calculation**

The TOE can calculate a hash value of the contents of the currently selected file. The command which performs this hash calculation is PERFORM HASH OF FILE. The hash value is stored in the card and can be used by the command PSO: COMPUTE DIGITAL SIGNATURE.

The hash algorithm is SHA-1 according to /FIPS180-3/.

SF.SES_KEY **Session Key Generation and Limit of Use**

During a mutual authentication (TSF SF.MUT_AUTH) a TDES Session Key according to /AIB-A11/, sec. 3.3.3 is created.

This key can be used by TSF SF.SM for all subsequent cryptographic operations using secure messaging. Its validity expires at the end of the session (withdrawal of the card or reset of the card) or after 240 commands using secure messaging sent to the card plus associated responses, whichever event occurs first.

The cryptographic key size of the Session Key is 128 bits with 112 effective bits.

7.1.3 Access Control

SF.ACC **Access Control Mechanism**

The TOE supports an Access Control mechanism as defined by the SFP Access Control (AC_SFP) in sec. 6.1.1.

7.1.4 Protection Mechanisms

SF.INTEGRITY **Data Integrity Checks**

The TOE checks the integrity of data elements during start-up (TSF SF.SELFTEST) and before usage.

In case of integrity error detection the TOE informs the IFD about the error and prohibits the usage of the corresponding data.

The following data elements stored in the card are involved:

- All dedicated and elementary files of the Tachograph Card file system
- The PIN
- All cryptographic keys
- Internal state and structure data
- Software code stored in the NVM

The integrity check is performed with the following methods:

- Error Detection Code (EDC) functionality of Memory Encryption/Decryption Unit (MED) of the IC as described in /IC_HRM/, section 12.4: detection of permanent memory integrity errors.
- Post Failure Detection mechanism (PFD) of the IC as described in /IC_SEC/, section 4.1 and /IC_HRM/, section 12.5: detection of cache integrity errors.
- XOR: detection of integrity errors of internal state and structure data

SF.SELFTEST **Self Test**

The TOE performs a self test during initial start-up after reset or power-on and periodically during command execution.

This self test includes
- integrity check of data elements as defined in TSF SF.INTEGRITY and
- integrity check of any software code not stored in ROM.

In case of integrity error detection the access to the TOE data is not possible any more, and the TOE informs the IFD about the error detection.

SF.DATA_ERASURE **Erasure of Data after Usage**

The TOE erases all security relevant data upon the deallocation of the data.

This erasure includes the following data:

- Volatile data after each command, e.g. the stack.
- The complete RAM during initial start-up
- Session Keys after the maximum number of possible use or after performing a new mutual authentication (TSF SF.MUT_AUTH) or after selecting an application (SELECT Command)

SF.HW_PROTECTION **Hardware Protection Mechanisms**

The TOE uses all hardware protection mechanism of the IC as required according to /IC_SEC/.

The hardware mechanisms include:

- Hiding of sensitive data transfers and operations
- Protection against SPA, DPA, DFA and timing attacks
- Shield protection
- Physical integrity of the IC

In case of failure detection the TOE changes to a secure state. Depending on the type of the failure the TOE will be irreversible locked or can be reactivated by a reset.

SF.SW_PROTECTION Software Protection Mechanisms

In addition to the already defined software measures the TOE uses further software protection mechanisms as follows:

- Software measures against SPA, DPA, DFA and timing attacks
- Confidentiality of the secrets (PIN and cryptographic keys) by storing them TDES encrypted in the NVM
- Rollback / Rollforward mechanism to ensure data consistency after an unexpected reset or power-down
- Protection mechanisms against program flow manipulation

In case of failure detection the TOE changes to a secure state. Depending on the type of the failure the TOE will be irreversible locked or can be reactivated by a reset.

7.2 Security Functions Rationale

7.2.1 Overview

The following table provides an overview for SFR coverage. It shows which TSF supports which SFR. It shows that each SFR is supported by at least one TSF and that each TSF supports at least one SFR.

SFR \ TSF	SF.PERSO	SF.MUT_AUTH	SF.VERIFY	SF.SM	SF.CERT	SF.SIG	SF.HASH	SF.SES_KEY	SF.ACC	SF.INTEGRITY	SF.SELFTEST	SF.DATA_ERASURE	SF.HW_PROTECTION	SF.SW_PROTECTION
FAU_SAA.1			X	X						X	X			
FCO_NRO.1					X	X	X							
FCS_CKM.1		X						X						
FCS_CKM.2		X						X						
FCS_CKM.4												X		
FCS_COP.1/RSA		X			X	X								

FCS_COP.1/TDES				X										
FDP_ACC.2/ personalisation	X													
FDP_ACF.1/ personalisation	X													
FDP_ACC.2/ end_usage									X					
FDP_ACF.1/ end_usage									X					
FDP_DAU.1					X	X	X							
FDP_ETC.1									X					
FDP_ETC.2						X	X		X					
FDP_ITC.1	X								X					
FDP_RIP.1												X		
FDP_SDI.2										X				
FIA_AFL.1/C		X												
FIA_AFL.1/WSC			X											
FIA_ATD.1	X								X					
FIA_UAU.1	X								X					
FIA_UAU.3		X	X											
FIA_UAU.4		X												
FIA_UID.1	X								X					
FIA_USB.1	X								X					
FPR_UNO.1		X		X										
FPT_EMS.1													X	X
FPT_FLS.1													X	X
FPT_PHP.3													X	X
FPT_TDC.1		X		X	X	X		X						
FPT_TST.1											X			
FTP_ITC.1		X		X				X						

Table 14: Coverage of SFRs by TSFs

7.2.2 Rationale

This section contains the rationale why and how the TSFs cover the list of SFRs.

FAU_SAA.1

The TSF SF.VERIFY realizes the monitoring of cardholder authentication failure required by FAU_SAA.1. The TSF SF.INTEGRITY realizes the monitoring of stored data integrity error, and the TSF SF.SM the monitoring of activity data input integrity error required by FAU_SAA.1. The TSF SF.SELFTEST realizes the monitoring of self test error required by FAU_SAA.1.

FCO_NRO.1

The TSF SF.SIG covers the functionality of creating a digital signature of a hash value which is previously computed and stored by the TSF SF.HASH. Both are needed to cover the generation of evidence of origin required by FCO_NRO.1. The TSF SF.SIG also covers the functionality of verifying the evidence of origin of information required by FCO_NRO.1 by verifying a digital signature. The used public key is obtained by a certificate verification covered by the TSF SF.CERT.

FCS_CKM.1

The TSF SF.SES_KEY used by the TSF SF.MUT_AUTH supplies functionality of session key generation required by FCS_CKM.1.

FCS_CKM.2

The TSF SF.SES_KEY used by the TSF SF.MUT_AUTH supplies functionality of session key distribution required by FCS_CKM.2.

FCS_CKM.4

The TSF SF.DATA_ERASURE erases the session key after the maximum number of possible use by the TSF SF.SM, after performing a new mutual authentication (TSF SF.MUT_AUTH) or after selecting an application (SELECT Command). This behavior is required by FCS_CKM.4.

FCS_COP.1/RSA

The TSF SF.MUT_AUTH performs encryption, decryption, signature creation and verification for the authentication between Tachograph Card and Vehicle Unit using RSA as required by FCS_COP.1/RSA, Tachograph Common Security Mechanisms /AIB-A11/, sec. 2-6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_020 and Tachograph Card Specification /AIB-A2/, sec. 3.

The TSF SF.CERT performs certificate verification using RSA as required by FCS_COP.1/RSA, Tachograph Common Security Mechanisms /AIB-A11/, sec. 2-6, CSM_003, CSM_004, CSM_014, CSM_016, CSM_017, CSM_018, CSM_019, CSM_020 and Tachograph Card Specification /AIB-A2/, sec. 3.

The TSF SF.SIG performs signing of data using and signature verification using RSA as required by FCS_COP.1/RSA, Tachograph Common Security Mechanisms /AIB-A11/, sec. 2-6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_033, CSM_034, CSM_035 and Tachograph Card Specification /AIB-A2/, sec. 3.

FCS_COP.1/TDES

The TSF SF.SM performs encryption, decryption, Retail-MAC generation and verification using TDES as required by FCS_COP.1/TDES.

FDP_ACC.2/personalisation, FDP_ACF.1/personalisation

The TSF SF.PERSO meets directly the SFRs FDP_ACC.2/personalisation and FDP_ACF.1/personalisation for the personalisation phase because it enforces completely the Security Function Policy AC_PERSO_SFP and it enforces the rules to determine if an operation among controlled subjects and controlled objects is allowed as defined in FDP_ACF.1.2.

FDP_ACC.2/end_usage, FDP_ACF.1/end_usage

The TSF SF.ACC meets directly the SFRs FDP_ACC.2/end_usage and FDP_ACF.1/end_usage for the end usage phase because it enforces completely the Security Function Policy AC_SFP and it enforces the rules to determine if an operation among controlled subjects and controlled objects is allowed as defined in FDP_ACF.1.2.

FDP_DAU.1

The TSF SF.SIG covers the functionality of creating a digital signature of a hash value which is previously computed and stored by the TSF SF.HASH. Both are needed to cover the generation of evidence of activity data required by FDP_DAU.1. The TSF SF.SIG also covers the functionality of verifying the evidence of origin of information from S.VU and S.Non-VU required by FDP_DAU.1 by verifying a digital signature. The used public key is obtained by a certificate verification covered by the TSF SF.CERT.

FDP_ETC.1

The TSF SF.ACC meets the SFR FDP_ETC.1 as it controls the export of user data by enforcing AC_SFP..

FDP_ETC.2

The TSFs SF.SIG and SF.HASH perform the SFR FDP_ETC.2 because they export user data with the user data's associated security attributes by hashing the content of an elementary file and computing the digital signature of this hash code. The digital signature is unambiguously associated with the exported user data from that EF. The TSF SF.ACC also meets the SFR FDP_ETC.2 as it controls the export of user data by enforcing AC_SFP.

FDP_ITC.1

The TSFs SF.ACC and SF.PERSO meet the SFR FDP_ITC.1 as they control the import of user data by enforcing AC_SFP resp. AC_PERSO_SFP.

FDP_RIP.1

The TSF SF.DATA_ERASURE meets directly the SFR FDP_RIP.1 as it deletes all previous information content of a resource upon the deallocation of the resource. The erasure implies all security relevant data, i.e. cryptographic keys and PINs.

FDP_SDI.2

The TSF SF.INTEGRITY performs the SFR FDP_SDI.2 because it realizes the monitoring of integrity error of user data stored in containers and informs the entity connected in case of detecting an integrity error.

FIA_AFL.1/C

The TSF SF.MUT_AUTH covers the SFR FIA_AFL.1/C as it implements the authentication of a card interface device and warns the entity connected when an unsuccessful authentication attempt has been met or surpassed.

FIA_AFL.1/WSC

The TSF SF.VERIFY covers the SFR FIA_AFL.1/WSC as it implements the PIN based user authentication and considers the failure handling as required by FIA_AFL.1/WSC: warn the entity connected and block the PIN check procedure when 5 authentication attempts has been met or surpassed.

FIA_ATD.1

The TSFs SF.PERSO and SF.ACC maintain the security attributes as required by the SFR FIA_ATD.1 because they enforce AC_PERSO_SFP and AC_SFP which apply the required security attributes:

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT, PERSO_UNIT, NON_PERSO_UNIT)
- USER ID (VRN and Registering MSC for subject S.VU)

FIA_UAU.1

The TSFs SF.PERSO and SF.ACC perform the SFR FIA_UAU.1 as their enforced Security Function Policies AC_PERSO_SFP and AC_SFP define which TSF-mediated actions are allowed before or after the user is authenticated in personalisation phase and in end-usage phase, respectively.

FIA_UAU.3

The TSFs SF.MUT_AUTH and SF.VERIFY cover the unforgeable authentication mechanisms as required by SFR FIA_UAU.3.

FIA_UAU.4

The TSF SF.MUT_AUTH handles the prevention of reuse of authentication data related to key based authentication mechanisms as required by SFR FIA_UAU.4..

FIA_UID.1

The TSFs SF.PERSO and SF.ACC cover the SFR FIA.UID.1 as they handle the access rule mechanism used for the timing of user identification in personalisation phase and in end-usage phase, respectively.

FIA_USB.1

The TSFs SF.PERSO and SF.ACC cover the SFR FIA_USB.1 as it handles user-subject binding as required by FIA_USB.1 in personalisation phase and in end-usage phase, respectively.

FPR_UNO.1

The TSFs SF.MUT_AUTH and SF.SM cover the SFR FPR_UNO.1 as they ensure that Attackers are unable to observe the operation on security and activity data by any user. SF_MUT_AUTH meets FPR_UNO.1 by exchanging RSA-encrypted authentication tokens, whereas SF.SM meets FPR_UNO.1 by exchanging TDES-encrypted data.

FPT_EMS.1

The TSFs SF.HW_PROTECTION and SF.SW_PROTECTION meet the SFR FPT_EMS.1 as they contain all needed hardware and software based mechanisms against side channel analysis to prevent emission of secrets from the smart card circuit contacts.

FPT_FLS.1

The TSFs SF.HW_PROTECTION and SF.SW_PROTECTION meet the SFR FPT_FLS.1 as they contain all needed hardware and software based mechanisms to preserve a secure state as required by FPT_FLS.1.

FPT_PHP.3

The TSFs SF.HW_PROTECTION and SF.SW_PROTECTION meet the SFR FPT_PHP.3 as they contain all needed hardware and software based mechanisms to ensure resistance of the TOE to physical attacks.

FPT_TDC.1

All key based cryptographic operations cover the Inter-TSF basic TSF data consistency, i.e. they interpret key material (session keys and certificates) consistently according to the rules as required by FPT_TDC.1.

The key based cryptographic operations are: SF.MUT_AUTH, SF.SM, SF.CERT, SF.SIG and SF.SES_KEY.

FPT_TST.1

The TSF SF.SELFTEST covers the SFR FPT_TST.1 as it implements the self tests during initial start-up and periodically during normal operation to verify the integrity of the TSF and TSF data.

FTP_ITC.1

The inter-TSF trusted channel as required by SFR FTP_ITC.1 is covered by TSF SF.SM. The establishment of the trusted channel is performed by TSF SF.MUT_AUTH and SF.SES_KEY by creating a Session Key.

8 Statement of compatibility with platform ST

This ST describes a composite TOE, which is based on the platform smart card security controller M7801 A12 (Infineon SLE78CX360P) including optional Software Libraries for RSA, EC and SHA-2.

M7801 A12 was evaluated and certified according to CC 3.1, EAL5+, as expressed by /ST_IC/ and /CR_IC/ (certification ID BSI-DSZ-CC-0727-2011).

8.1 Compatibility with platform assumptions

The assumptions about the operational environment of the platform TOE are:

- A.Process-Sec-IC Protection during Packaging, Finishing and Personalization,
- A.Plat-Appl Usage of Hardware Platform,
- A.Resp-Appl Treatment of User Data,
- A.Key-Function Usage of Key-dependent Functions.

The assumptions A.Plat-Appl, A.Resp-Appl and A.Key-Function address different aspects of the development of the embedded software and will therefore be automatically regarded in the evaluation of the composite TOE.

The assumption A.Process-Sec-IC has got one aspect that is also significant for the operational environment of the composite TOE, this is protection during personalisation. This is covered in this composite ST by the corresponding assumption A.Personalisation_Phase (Personalisation Phase Security).

8.2 Compatibility with platform threats

The threats for the platform TOE,

- T.Phys-Manipulation Physical Manipulation,
- T.Phys-Probing Physical Probing,
- T.Malfunction Malfunction due to Environmental Stress,
- T.Leak-Inherent Inherent Information Leakage,
- T.Leak-Forced Forced Information Leakage,
- T.Abuse-Func Abuse of Functionality,
- T.RND Deficiency of Random Numbers,
- T.Mem-Access Memory Access Violation,

are all related to attacks addressing the IC physically, to make some processing in the IC fail, or to abuse specific functionality of the IC. The threats and OSPs for the composite TOE are defined on a totally different level, i.e. the Tachograph Smart Card Application. All threats for the platform are somehow sub-aspects of the tachograph card threats (e.g. unauthorized access to a tachograph objects can be achieved by physically addressing the IC). Furthermore, the threats for the platform address the fact that security functionality of the composite TOE could be modifies or deactivated by attacking the IC using physical means. Therefore the threats for the platform and the threats and OSPs for the composite TOE are in no contradiction.

8.3 Compatibility with platform OSPs

The OSPs defined for the platform TOE are:

- P.Process-TOE Protection during TOE Development and Production,
- P.Add-Functions Additional Specific Security Functionality.

P.Process-TOE is met by a security objective or the development and production environment for the IC and cannot contradict to any OSP or threat for the composite TOE. The OSP P.Add-Functions requires the platform TOE to implement specific cryptographic functions as service functionality to the embedded software of the composite TOE, which actually uses several of the required cryptographic algorithms in its own Tachograph Card functionality. Therefore the OSPs for the platform are in no contradiction to the threats and OSPs of the composite TOE.

8.4 Compatibility with platform security objectives for the TOE

When looking at the security objectives of the platform TOE,

- O.Phys-Manipulation Protection against Physical Manipulation,
- O.Phys-Probing Protection against Physical Probing,
- O.Malfunction Protection against Malfunction,
- O.Leak-Inherent Protection against Inherent Information Leakage,
- O.Leak-Forced Protection against Forced Information Leakage,
- O.Abuse-Func Protection against Abuse of Functionality,
- O.Identification TOE Identification,
- O.RND Random Numbers,
- O.Add-Functions Additional Specific Security Functionality (cryptographic functions),
- O.Mem-Access Area based Memory Access Control,

these are mainly related to self-protection of the IC, to protection of data stored or processed in the IC, and to supporting functions like random number generation or cryptographic functions. The security objectives for the composite TOE are defined on a totally different level, i.e. the Tachograph Smart Card Application. All the security objectives for the platform do contribute to the Tachograph Card security objectives (e.g. access control on Tachograph objects is only effective as long as the IC will prevent physical attacks) and do harden the Tachograph security functionality in the end. Therefore the security objectives for the platform and the security objectives for the composite TOE are in no contradiction.

8.5 Compatibility with platform security objectives for the operational environment

The security objectives for the operational environment of the platform TOE are:

- OE.Plat-Appl Usage of Hardware Platform,
- OE.Resp-Appl Treatment of User Data,
- OE.Process-Sec-IC Protection during composite product manufacturing.

The security objectives for the operational environment OE.Plat-Appl and OE.Resp-Appl address different aspects of the development of the embedded software and will therefore be automatically regarded in the evaluation of the composite TOE.

The security objective for the operational environment OE.Process-Sec-IC has got one aspect that is also significant for the operational environment of the composite TOE, this is protection during personalisation. This is covered in this composite ST by the corresponding security objective for the operational environment OE.Personalisation_Phase (Secure Handling of Data in Personalisation Phase). (This directly corresponds to the discussion of compatibility with the platform assumptions, where A.Process-Sec-IC, which directly traces to OE.Process-Sec-IC, was found to be the only assumption significant for the operational environment of the composite TOE.)

8.6 Compatibility with platform SFRs

For the composite TOE described in this ST all of the platform SFRs are relevant, except FCS_COP.1/AES, FCS_COP.1/ECDSA, FCS_COP.1/ECDH and FCS_CKM.1/EC, which are irrelevant because the composite TOE does not make use of the Advanced Encryption Standard or any elliptic curve cryptography. All the other platform SFRs are relevant because they require features of self-protection, which directly or indirectly support the functionality of the TOE, e.g. by preventing access to data stored in the TOE using physical means, by detecting integrity errors in the memories of the TOE, or by limiting information leakage when computing TDES or RSA to an amount not exploitable by an attacker.

8.7 Compatibility with platform SARs

The platform TOE was evaluated and certified according to CC3.1 EAL5 augmented with ALC_DVS.2 and AVA_VAN.5. The composite TOE of this ST shall be evaluated and certified according to CC3.1 EAL4 augmented with ATE_DPT.2 and AVA_VAN.5 (as required by /PP0070/). Therefore the security assurance requirements of the composite evaluation are a subset of the security assurance requirements of the platform evaluation because of the following:

- EAL4 is a subset of EAL5 (taking into account hierarchical components)
- ATE_DPT.2 augmented in the composite evaluation is part of EAL5 (due to hierarchical component ATE_DPT.3 included in EAL5)
- AVA_VAN.5 is augmented in both evaluations

8.8 Compatibility with platform TSF

The TSF of the platform TOE are (these are called security features in /ST_IC/):

- SF_DPM Device Phase Management,
- SF_PS Protection against Snooping,
- SF_PMA Protection against Modification Attacks,
- SF_PLA Protection against Logical Attacks,
- SF_CS Cryptographic Support (TDES, AES, RSA, EC, SHA, TRNG).

The first four of these TSF are relevant platform TSF as they are needed to protect the composite TSF and any date stored or processed in the composite TOE against any kind of physical or side-channel attacks or abuse of functionality concerning the IC.

Also the last remaining TSF SF_CS is a relevant platform TSF, as the composite TOE makes use of the platform's TDES, RSA, SHA and true random number generator functions (only a part of SF_CS is not relevant for the TOE, i.e. AES and elliptic curve cryptography functions).

Therefore all TSF of the platform TOE are (at least partly) relevant for the composite TOE. By the nature of the platform TSF (self-protection of the IC, protection of data stored or processed in the IC, and cryptographic support of the embedded software), these cannot be in contradiction with the composite TSF, instead the platform TSF is needed to protect assets and TSF implementation of the composite TOE.

Bibliography

/CC1/	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009
/CC2/	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCIMB-2009-07-002, Version 3.1, Revision 3, July 2009
/CC3/	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCIMB-2009-07-003, Version 3.1, Revision 3, July 2009
/AIB/	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
/CorrReg/	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
/AIB-A2/	Appendix 2 of Annex I B of Commission Regulation (EC) No. 1360/2002 [5] – Tachograph Cards Specification
/AIB-A10/	Appendix 10 of Annex I B of Commission Regulation (EC) No. 1360/2002 [5] - Generic Security Targets
/AIB-A11/	Appendix 11 of Annex I B of Commission Regulation (EC) No. 1360/2002 [5] - Common Security Mechanisms
/JIL/	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 1B, Version 1.12, June 2003
/IC_PRM/	SLE 70 Family Programmer's Reference User's Manual, July 15, 2010, Infineon Technologies AG
/IC_HRM/	SLx 70 Family Hardware Reference Manual, November 2010, Infineon Technologies AG
/IC_SEC/	SLx 78 Controllers Security Guidelines User Manual, Released, February 2011, Infineon Technologies AG
/IC_ACL/	SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, User Interface, November 11, 2010, Infineon Technologies AG
/CC_SecureX/	CC SecureX Extranet Portal User Manual, Infineon Technologies AG
/ST_IC/	Infineon Technologies AG Chipcard and Security, Evaluation Documentation, Security Target M7801 A12 including optional Software Libraries RSA – EC – SHA, Version 0.6, 2011-04-15
/CR_IC/	BSI-DSZ-CC-0727-2011 for Infineon smart card IC (Security Controller) M7801 A12 with optional RSA2048/4096 v1.02.008, EC v1.02.008 SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software from Infineon Technologies AG, 2011-05-17, Bundesamt für Sicherheit in der Informationstechnik
/PP0070/	Digital Tachograph – Smart Card Tachograph Card, Version V1.02, 15.11.2011

/PP0035/	Security IC Platform Protection Profile, BSI-PP-0035, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007
/ICAO-PP/	Common Criteria Protection Profile 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
/AIS36/	AIS 36, Version 3, 19.10.2010
/NIST800-67/	NIST Special Publication 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
/FIPS180-2/	Federal Information Processing Standards Publication 180-2, 2002 August 1, SECURE HASH STANDARD
/RSA-PKCS#1/	PKCS #1: RSA Cryptography Standard
/ISO7816_P3/	Electronic signals and transmission protocol

Glossary and Acronyms

Term	Description
Activity data	Activity data include user activities data, events and faults data and control activity data (date and time of first use of the vehicle, vehicle odometer value at that time, date and time of last use of the vehicle, vehicle odometer value at that time, VRN and registering Member State of the vehicle, date and time the session was opened, a daily presence counter, the total distance travelled by the driver during this day, a driver status at 00.00, information about changed activity, data related to places where daily work periods begin and/or end (the date and time of the entry, the type of entry, the country and region entered, the vehicle odometer value), records of calibrations and/or time adjustments performed as well as counter indicating the number of calibrations performed (workshop card), date and time of the control, type of the control, period downloaded (control card), date and time of the activity, type of the activity, period downloaded (company card)).
CBC	Cipher Block Chaining
CC	Common Criteria
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ES	Embedded Software
GST	Generic Security Target for Tachograph Card as defined in /AIB-A10/
IC	Integrated Circuit
ICV	Initial Chaining Value
IFD	Interface Device
MAC	Message Authentication Code
PIN	Personal Identification Number
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SM	Secure Messaging
SPA	Simple Power Analysis
ST	Security Target
TDES	Triple DES
TOE	Target of Evaluation
TSF	TOE Security Functionality
VU	Vehicle Unit