T · · Telesec ·

Specification Version 1.0

of the Security Target

TCOS Tachograph Card

Dokumentenkennung:	CD:TCOS:EVAL.ASE
Dateiname:	ASE-Tachograph.doc
Stand:	07.05.2004
Version:	1.0
Autor:	Ernst-G. Giessmann
Geltungsbereich:	Telesec Entwicklungsgruppe CD
Vertraulichkeitsstufe:	
erstellt:	Ernst-G. Giessmann
geprüft:	Hartmut Findeklee
freigegeben:	Burkhard Fuchs

History

Version	Date	Remark
1.0	2004-05-07	First Edition

Inhaltsverzeichnis

Abbreviations

ACD	Activity data
CA	Certification Authority
CC	Common Criteria Version
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
EQT.SK	Equipment Secret Key (SCD)
EQT.PK	Equipment Public Key (SVD)
KMWC	Master Key Workshop Card (cf. [TACHO] Km_{WC})
IDD	Identification data
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
RAD	Reference authentication data
SCA	Signature-Creation Application
SCD	Signature-Creation Data (EQT.SK)
SMK	Secret Messaging Keys
SOF	Strength of Function
SVD	Signature-Verification Data (EQT.PK)
TSC	TSF Scope of Control
TOE	Target of Evaluation
VAD	Verification Authentication Data
VU	Vehicle Unit
non-VU	Subject not identified as VU

1 ST Introduction

1.1 ST Identification

ST Identification: Security Target refers to the Smartcard Product “TCOS Tachograph Card Version 1.0” (TOE) of T-Systems TeleSec for CC evaluation.

Title: Specification Version 1.0 of the Security Target TCOS Tachograph Card

Date: 07.05.2004

Author: T-Systems TeleSec, Ernst-G. Giessmann

Certification ID: BSI-DSZ-CC-0242

TOE: TCOS-Tachograph Card, the version of the TOE is 1.0

1.2 ST Overview

The security target is the description of a TOE as a smartcard based on an Infineon chip SLE66CX322P, the chip being certified according to CC EAL5+ [BSI2003], and the TCOS 3.0 operating system. The TOE is supplied with a dedicated filesystem, that defines the type of the Tachograph Card (driver card, company card, workshop card, or control card).

The evaluated configuration of the TOE is the smartcard with the security application (embedded software). The IC platform is based on ISO-7816, and a dedicated ISO-filesystem is associated with the application.

The TOE follows the composite evaluation aspects (see also [AIS36]).

The TOE complies with the Tachograph Card Specification Annex 10 and Annex 11 of EC regulation 1360/2002 [TACHO]. This implies the compliance with PP9911 and PP0002. All issues related with the Infineon chip SLE66CX322P security controller have already been covered by a hardware evaluation [BSI2003].

1.3 CC Conformance

The ST claims the conformance of the TOE to Common Criteria for IT Security Evaluation 2.1 with current final interpretations (2003-10-31)

- Part 1,
- Part 2 (extended) and
- Part 3.

The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations and the JIL (Joint Interpretation Library) document “Security Evaluation and Certification of Digital Tachographs”, Version 1.12, dated June 2003.

The part 2 is extended because of the requirement FCS_RND.1, which is included in the hardware evaluation.

This ST claims conformance to PP9911 [PP9911] and to PP0002 [PP0002].

The evaluation assurance level of the TOE is EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 and AVA_VLA.4 ([PP9911] and [JILTACHO]).

The minimum strength for the TSF is “high”.

The evaluation of the TOE uses the result of the CC evaluation of the Infineon chip SLE66CX322P/m1484; especially the hardware part of the composite evaluation is covered by the certification report [BSI2003].

The security functionality (TSF) of this chip conforms to [PP0002]. Since both the chip and the TOE conform to this protection profile the requirements of [AIS36] for consistency of the relevant ST are fulfilled.

Since the hardware has already been evaluated, this ST will focus on the embedded software and the relevant composite aspects. The conformance to the [PP0002] is covered by the IC certification; its objectives and requirements are not replicated here.

2 TOE Description

2.1 TOE Definition

The TOE is a Smart Card with an operating system (TCOS 3.0) and a dedicated file-system according to the intended type of the tachograph card.

The components of the TOE are therefore the underlying hardware (IC), the operating system TCOS 3.0 (ES) and the dedicated filesystem (FS). A detailed description of the parts of TOE will be given in other documents.

The tachograph cards can be one of the following types defined in the Annex 2 of the Tachograph Card Specification:

- driver card,
- workshop card,
- control card and
- company card.

All of them are used for displaying, storing and downloading of data stored by recording equipment of a vehicle and allow for identification of the identity (or a identity group) of the cardholder.

The usual smart card product life-cycle is decomposed in 7 phases [PP9911, Fig. 2.2 p. 13] as follows:

- Phase 1: Smart card Embedded Software Development
- Phase 2: IC Design and IC dedicated software development
- Phase 3: IC Manufacturing
- Phase 4: IC Packaging and testing
- Phase 5: Smart card product Finishing process
- Phase 6: Smart card Personalization

- Phase 7: Smart Card product end-usage

The phase 6 described in [PP9911] as personalization can be separated in two steps, the initialization of the embedded software and personalization of the end-user data, for short referred in the following as initialization and personalization. The product is finished after initialization, after testing the OS and creation of the dedicated filesystem with security attributes. The TOE exists only in the end-usage phase. The security policy (cf. [TACHO, Appendix 10] formulated in the current ST is valid only for phase 7. The correct delivery and the correct personalization is covered by the Administrator guidance. Nevertheless all elements, objectives, assumptions from phases 1 to 5 and phase 6 before the personalization are referenced here. The phase 6 after the initialization and phase 7 of the card life-cycle is considered in detail.

The delivery of the TOE is to the personalization body.

2.2 TOE Boundaries

2.2.1 TOE Physical Boundaries

Smart card as used in this ST means an integrated circuit containing a microprocessor, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory which include RAM, ROM, and EEPROM.

The carrier is typically made of plastic and conforms to ISO 7810 and 7813 – Identification Cards, but may have also the smaller size of a subscriber identification module (SIM).

The chip is embedded in a module which provides the capability for standardized connection to systems separate from the chip through contacts in accordance with ISO 7816.

The contacts are the physical boundaries of the TOE.

2.2.2 TOE Logical Boundaries

All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical

boundaries of the TOE are given by the I/O interface of the TCOS 3.0 operating system.

The input to the TOE is transmitted over the physical interface as an octet string that has the structure of Command Application Protocol Data Unit (CAPDU).

The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

These Application Protocol Data Units are described in more detail in an other document.

3 TOE Security Environment

3.1 Assets

Assets are security relevant elements of the TOE. The primary and secondary assets defined in [SLE66CX322P, p.11], which contain all assets defined in [PP9911] are the following:

- the Smart Card Embedded Software including specifications, implementation and related documentation,
- the application data of the TOE (such as IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data, see section above), this corresponds to the User Data in [SLE66CX322P].
- The TOE itself and its correct operation, including the additional asset from [SLE66CX322P], the random number generator, are assets.

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

3.1.1 Application data

1. IDD (Identification data): Integrity of cardholder identification and card identification data must be maintained.

2. ACD (Activity data): Integrity and authenticity of activity data (cardholder activities data, events and faults data and control activity data) must be maintained.

3. SCD (Signature Creation Data): private key used to perform an electronic signature operation(confidentiality of the SCD must be maintained).

4. SMK (Secret Messaging Keys): Confidentiality and Integrity of 3DES keys used to protect secure messaging must be maintained during generation, transport (if any) and storage. Despite of that the KMWC (Master key workshop card) is only a part of the motion sensor master key, used for pairing of motion sensor with VU, it is considered here as a secret key too, because the other part of the motion sensor master key is known to the VU.

5. SVD (Signature Verification Data): public keys certified by Certification Authorities, to verified electronic signatures (i.e. of certificates).

6. VAD (Verification authentication data) means authentication data provided as input by knowledge (PIN).

7. RAD (Reference authentication data) means data persistently stored by the TOE for verification of the authentication attempt as authorized user.

8. DTBS (Data to be signed) means the complete electronic data to be signed (including both user message and signature attributes).

3.2 Subjects

The subjects are the users of the TOE.

S.Administrator	Installing the security data and identification data
S.VU	Vehicle unit (activity data recording device) with a UserID
S.Non-VU	Non vehicle unit (without a UserID)

3.3 Threat agents

S.OFFCARD

Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a high level attack potential and knows no secret.

3.4 Assumptions

The assumptions A.Process-Card, A.Plat-Appl, A.Resp-Appl and A.Key-Function are defined in [SLE66CX322P chap. 3.2, p. 12]. The assumptions A.DEV_ORG*, A.DLV_PROTECT*, A.DLV_AUDIT*, A.DLV_RESP*, A.USE_TEST*, A.USE_PROD* and A.USE_DIAG* are specified in [PP9911, 3.2. p. 18]. All assumptions must be considered. Nevertheless the assumption which are indicated by a “*” are common with

the IC PP [PP0002] and therefore they are only referenced because they are covered by the hardware evaluation.

Relevant for phase 6 and 7 are only A.USE_TEST*, A.USE_PROD* (phase 4 to 6) and A.USE_DIAG* (phase 7). The assumptions A.Process-Card, A.Plat-Appl, A.Resp-Appl and A.Key-Function also apply to this composite ST.

- Concerning the assumption A.Process-Card ("Protection during Packaging, Finishing and Personalization"), the Composite TOE does not differ from the IC hardware, and thus this assumption has to be maintained. See also assumption A.Personalization below, which specifies even more details for the personalization phase.

- Concerning the assumptions A.Plat-Appl ("Usage of Hardware Platform"), A.Resp-Appl ("Treatment of User Data"), and A.Key-Function ("Usage of Key-dependent Functions") the embedded software already fulfills these assumptions:

  - A.Plat-Appl assumes that the Smartcard Embedded Software is designed properly, paying attention to the guidance documentation of the HW evaluation. This will be checked during the evaluation, most likely during examination of the assurance class ADV.

  - A.Resp-Appl assumes that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context. Again, this will be the subject of the composite evaluation.

  - A.Key-Function assumes that key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks. An analysis of the cryptographic mechanisms' resistance against side channel attacks is part of the composite evaluation (vulnerability analysis).

Assumptions that are fulfilled by the underlying hardware no longer have to be maintained for the composite TOE. Therefore the assumptions to be considered in this composite ST are **A.Process-Card** and **A.Personalization** (see below) but they are relevant only for phase6.

In addition, the following specific assumption from [TACHO] applies:

A.Personalization During the personalization the identification data, certificates and secret keys will be written to the filesystem of the TOE. The communication of the personalization device will be under the control of the Administrator and is done in a

secure manner. This assumptions contains also the three assumptions A.DLV_PROTECT*, A.DLV_AUDIT* and A.DLV_RESP* during phase 6.

The confidentiality of private keys shall be maintained during generation, transport (if any) and storage. The key length for the RSA algorithm must be as follows: Modulus 1024 bits, public exponent 64 bits maximum, private exponent 1024 bits [TACHO, CSM_014].

Application notes:

After personalization each tachograph card contains a valid CA-key for authentication and digital signature. Each tachograph card is associated with unique identification data, the Certificate Holder Reference (CHR) that has the purpose of identifying uniquely the legitimate cardholder (i.e. certificate holder).

The key length of the RSA-Modulus *n* is exact 1024 bits, i.e. $2^{1023} < x < 2^{1024}$.

3.5 Threats

The following threats are described in [SLE66CX322P, p. 12]:

- T.Phys-Manipulation
- T.Phys-Probing
- T.Malfunction
- T.Leak-Inherent
- T.Leak-Forced
- T.Abuse-Func
- T.RND

From the threats listed in [PP9911, pp. 13-23] the following are not covered by the evaluation [BSI2003]:

T.DIS_ES1, T.DIS_ES2, T.DIS_TEST_ES, T.DIS_DEL1, T.DIS_DEL2, T.T_TOOLS, T.T_SAMPLE2, T.T_ES, T.T_CMD, T.MOD, T.MOD_DEL1, T.MOD_DEL2, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE.

Application note: Relevant for the TOE in phase 7 are only the following threats:

T.DIS_ES2, T.T_ES, T.T_CMD, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE.

Only these threats have to be considered for this composite evaluation. The other threats are only defined for life cycle phases which are not under consideration as a

part of the security policy for this composite TOE (see [PP9911, table 3.1]) and/or are modeled by assumptions in this composite ST, i.e. they are covered by the assurance classes ADO and ALC.

Additionally the following threats are identified, which are specific for tachograph cards:

T.Ident_Data

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

T.Activity_Data

A successful modification of activity data stored in the TOE would be a threat to the security of the TOE.

T.Data_Exchange

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

3.6 Organization Security Policies

There are no organizational security policies (cf. [TACHO, Appendix 10]).

Relevant for the TOE may be P.Process-TOE and P.Add-Functions in [SLE66CX322P, p. 13]; however, these policies are not needed in this composite ST (see section 8.1.3).

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the IC are referenced in the ST evaluation of the IC [BSI-DSZ-CC-0223-2003], the security objectives for the embedded software (OS) are referenced in the PP9911.

The following objectives are taken over from the [SLE66CX322P] are based on the [PP0002]:

- O.Phys-Manipulation
- O.Phys-Probing
- O.Malfunction
- O.Leak-Inherent
- O.Leak-Forced
- O.Abuse-Func
- O.Identification
- O.RND
- O.Add-Functions

The following objectives are taken over from the Protection Profile [PP9911]:

- O.TAMPER_ES
- O.CLON*
- O.OPERATE*
- O.FLAW*
- O.DIS_MECHANISM2
- O.DIS_MEMORY*
- O.MOD_MEMORY*

All objectives taken from the [SLE66CX322P] also apply to the composite target. Objectives marked with (*) are covered by the hardware, the objectives in [PP9911] being relevant for the TOE are the following:

OT.TAMPER_ES

The TOE must prevent tampering with its security critical parts. Security mechanisms have especially to prevent the unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys.

The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.

OT.DIS_MECHANISM2

The TOE shall ensure that the ES security mechanisms are protected against unauthorized disclosure.

Application note: The objectives are renamed from O.AnyExample to OT.AnyExample for consistency reasons.

Additionally the Appendix 10 of tachograph card specification lists the following objectives

OT.Card_Identification_Data

The TOE must preserve of card identification data and cardholder identification data stored during card personalization process.

OT.Card_Activity_Storage

The TOE must preserve of user data stored in the card by vehicle units.

Application note:

The user data consists of identification data and activity data, cf. [TACHO, Appendix 10, sec. 2.2]. The TOE must preserve the integrity of this data objects.

OT.Data_Access

The TOE must limit user data write access rights to authenticated vehicle units.

OT.Secure_Communication

The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the tachograph application.

OT.Personalization

The TOE provides the functionality to download the identification data, certificates and secret keys to the filesystem of the TOE in secure manner.

4.2 Security Objectives for the Environment

The security objectives for the environment of the TOE are referenced in the evaluation documentation [SLE66CX322P]:

- OE.Plat-Appl
- OE.Resp-Appl
- OE.Process-TOE
- OE.Process-Card

and in [PP9911]:

- O.DEV_TOOLS*, O.DEV_DIS_ES, O.SOFT_DLV*, O.INIT_ACS O.SAMPLE_ACS (phase 1)
- O.DLV_PROTECT*, O.DLV_AUDIT*, O.DLV_RESP* (delivery process phase 4 to 7)
- O.DLV_DATA (delivery from phase 1 to 4,5 and 6)
- O.TEST_OPERATE* (phase 4 to 6)
- O.USE_DIAG* (phase 7)

Note, that there are no security objectives for the environment defined in [PP9911] that apply to phase 7 of the smart card life cycle, which are not already covered by appropriate assurance components selected for this composite ST. The Objectives O.DLV_PROTECT, O.DLV_AUDIT and O.DLV_RESP are guaranteed by ADO_DEL.2. Objective O.USE_DIAG is already implied by OE.Personalization, and the objective O.TEST_OPERATE by OE.Plat-Appl.

These objectives are supplemented with the tachograph specific objectives for the Non-IT-environment.

OE.Secure_Communication

The environment shall support secure communication protocols and procedures.

OE.Personalization During the personalization the identification data, certificates and secret keys shall be written to the filesystem of the TOE. The communication of the personalization device must be under the control of the Administrator and shall be done in a secure manner. The confidentiality of private keys shall be maintained during generation, transport (if any) and storage. The key length for the RSA algorithm must be as follows: Modulus 1024 bits, public exponent 64 bits maximum, private exponent 1024 bits [TACHO, CSM_014].

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The Security Functional Requirements from [SLE66CX322P]

- FRU_FLT.2 “Limited fault tolerance“
- FPT_FLS.1 “Failure with preservation of secure state”
- FPT_SEP.1 “TSF domain separation”
- FMT_LIM.1 “Limited capabilities”
- FMT_LIM.2 “Limited availability”
- FAU_SAS.1 “Audit storage”
- FPT_PHP.3 “Resistance to physical attack”
- FDP_ITT.1 “Basic internal transfer protection”
- FDP_IFC.1 “Subset information flow control”
- FPT_ITT.1 “Basic internal TSF data transfer protection”
- FCS_RND.1 “Quality metric for random numbers”
- FPT_TST.2 “Subset TOE security testing“
- FDP_ACC.1 “Subset access control”
- FDP_ACF.1 “Security attribute based access control”
- FMT_MSA.3 “Static attribute initialization”
- FMT_MSA.1 “Management of security attributes”
- FCS_COP.1 “Cryptographic support”
- FCS_CKM.1 “Cryptographic key generation”

are listed in [SLE66CX322P, p. 27]. They are either satisfied by the hardware ST or considered in the following chapters.

5.1.1 Security audit analysis (FAU)

5.1.1.1 FAU_SAA.1 Potential violation analysis

If the TOE is configured as a workshop card then the following requirements apply:

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

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events: Accumulation or combination of *[assignment:*

- *cardholder authentication failure,*
- *self test errors,*
- *stored data integrity errors*
- *activity data input integrity errors]*

known to indicate a potential security violation; *[assignment: none*].

5.1.2 Communication (FCO)

5.1.2.1 FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted *[assignment: download data]* at the request of the *[selection: recipient, [assignment:]]*.

FCO_NRO.1.2 The TSF shall be able to relate the *[assignment: digital signature]* of the originator of the information, and the *[assignment: download data]* of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to *[selection: recipient, [assignment:]]* given *[assignment: indefinite]*.

This fulfills the requirement in [TACHO], Appendix 10

DEX_304 The TOE shall be able to generate an evidence of origin for data downloaded to external media.

Application note: The evidence of origin is realized as digital signature for download data.

5.1.3 Cryptographic support (FCS)

5.1.3.1 Cryptographic operation (FCS_COP)

FCS_COP.1.1 The TSF shall perform *[assignment: encryption, message authentication code, digital signature, authentication protocols]* in accordance with a specified cryptographic algorithm *[assignment: RSA, 3DES]* and cryptographic key sizes *[assignment: 1024 bit (RSA), 112 bit (3DES)]* that meet the following: *[assignment: standards listed in [TACHO, Appendix 11]].*

5.1.3.2 Cryptographic Key Management (FCS_CKM)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[assignment: TACHO, Appendix 11, CSM_020]]* and specified cryptographic key sizes *[assignment: 112 bit]* that meet the following: *[assignment: 3DES]*.

This refers to:

CSP_301 If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. Generated cryptographic session keys shall have a limited (TBD by administrator and not more than 240) number of possible use.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[assignment: according to [TACHO, Appendix 11, CSM_020]* that meets the following: *[assignment: according to [TACHO, Appendix 11, CSM_020]*.

This refers to:

CSP_302 If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods.

FCS_CKM.3.1 The TSF shall perform *[assignment: none]* in accordance with a specified cryptographic key access method *[assignment: none]* that meets the following: *[assignment: none]*.

There is no specified access to cryptographic keys like backup, archive, deposition, escrow or recovery.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[assignment: physical deletion by overwriting the memory data with the new key]* that meets the following: *[assignment: [TACHO, Appendix 11, CSM_013, TCS_353]*.

5.1.4 User data protection (FDP)

5.1.4.1 Security attribute based access control policy (FDP_ACC)

FDP_ACC.2.1 The TSF shall enforce the *[assignment*: *AC_SFP]* on *[assignment: S.VU, S.Non-VU],* and all operations among subjects and objects covered by the SFP.

The global security policy becomes apparent from [TACHO], Annex I (B); for a detailed reference see section 6.1.5.

The access control security function policy (AC_SFP) is described in FDP_ACF.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.4.2 Security attribute based access control functions (FDP_ACF)

FDP_ACF.1.1 The TSF shall enforce the *[assignment*: *AC_SFP]* to objects based on *[assignment: USER_GROUP]*.

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

[assignment:

AC_SFP:

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

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

ACTIVITY_WRITE: Activity data may be written to the TOE by S.VU only.

SOFT_UPGRADE: No user may upgrade TOE's software.

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

]

Application note:

The GENERAL_READ operation is based on [TACHO, Appendix 10, chap. 4.3.2] and [JILTACHO, ver. 1.12, sec. 2.6, pos. 50].

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

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

Application note:

The security attributes USER_GROUP is defined in [TACHO, Appendix 10, chap. 4.2.1] and does not belong to the TOE, but to the Activity Data (ACD).

ACT_301 The TOE shall hold permanent identification data.

ACT_302 There shall be an indication of the time and date of the TOE's personalization. This indication shall remain unalterable.

Although the time and date of personalization are not explicitly mentioned in the definitions of [TACHO, Appendix 10, chap. 2.2], we will consider them as identification and user data to be secured.

5.1.4.3 Data authentication (FDP_DAU)

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

FDP_DAU.1.2 The TSF shall provide *[assignment: any subjects]* with the ability to verify evidence of the validity of the indicated information.

5.1.4.4 Export of user data without security attributes (FDP_ETC)

FDP_ETC.1.1 The TSF shall enforce the *[assignment:*

1. The TOE does not export any user data without security attributes to a vehicle unit VU. (GenST 4.8).

2. The TOE except Control and Company Cards does not export user data without security attributes to a Non_VU (Gen-ST 4.2.2).

3. Control and Company Cards export any user data without security attributes except identification data to a Non_VU.

] when exporting user data, controlled under the SFP(s), outside of the TSC.

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

The download function shall be implemented as stated below (see also [JILTACHO], Annex B):

FDP_ETC.2.1 The TSF shall enforce the *[assignment: AC_SFP]* when exporting user data, controlled under the SFP, outside of the TSC.

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

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

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC:

[assignment: [TACHO], Appendix 10

DEX_305 The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient.

DEX_306 The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified.].

5.1.4.5 Import of user data without security attributes (FDP_ITC)

FDP_ITC.1.1 The TSF shall enforce the *[assignment*: *none]* when importing user data, controlled under the SFP, from outside of the TSC

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

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

Application note:

The TOE does not import any user data without security attributes (cf. [TACHO, Appendix 10 chap. 4.8]).

5.1.4.6 Subset residual information protection (FDP_RIP)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[selection: de-allocation of the resource]* from the following objects: *[assignment: EQT.SK, SMK]*.

5.1.4.7 Stored data integrity monitoring and action (FDP_SDI)

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for *[assignment: integrity error]* on all objects, based on the following attributes*: [assignment: integrity checked stored data].*

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

[assignment:

- *prohibit the use of the altered data*
- *generate an error message about integrity error and warn the entity connected]*.

5.1.5 Identification and authentication (FIA)

5.1.5.1 Authentication failure handling (FIA_AFL)

FIA_AFL.1.1 The TSF shall detect when *[assignment: 1]* unsuccessful authentication attempts occur related to *[assignment: authentication of a card interface device]*.

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

If the TOE is used as a workshop card then the following requirements apply:

FIA_AFL.1.1/WS-Card The TSF shall detect when *[assignment: 5]* unsuccessful authentication attempts occur related to *[assignment: PIN checks]*.

FIA_AFL.1.2/WS-Card When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *[assignment: warn the entity connected, block the PIN check procedure and indicate to subsequent users the reason of blocking]*.

5.1.5.2 User attribute definition (FIA_ATD)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users *[assignment: USER_GROUP (i.e. S.VU, S.Non-VU), USER_ID (i.e. Vehicle Registration number and registering Member State Code, known for S.VU only)].*

5.1.5.3 Timing of authentication (FIA_UAU)

FIA_UAU.1.1 The TSF shall allow *[assignment: All cards: reset, card identification, VU identification; Driver and Workshop Cards: export user data with security attributes (card data download function); Control and Company Cards: export user data without security attributes, except cardholder identification data]* on behalf of the user to be performed before the user is authenticated.

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

Application note: This fulfills the following specifications in Appendix 10:

UIA_301 Authentication of a vehicle unit shall be performed by means of proving that it possesses security data that only the system could distribute.

UIA_302 The Workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the vehicle unit to ensure the identity of the card holder, it is not intended to protect workshop card content).

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

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

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to *[assignment: any authentication mechanism(s)].*

Description: The authentication mechanisms are: the authentication of a vehicle unit and the PIN authentication for workshop cards. It is obviously from [TACHO] that the workshop card PIN is not intended to be changed after using. Therefore we interpret this requirement as being applicable for the mutual device authentication only.

5.1.5.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow *[assignment: none*] 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: Any user is identified either as VU or at least as Non-VU by just putting the Tachograph card in a card reader, and therefore no TSF mediated actions are possible before identification [JILTACHO].

5.1.5.5 User-subject binding (FIA_USB)

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

5.1.6 Security management (FMT)

As the TOE defined in the tachograph card specification [TACHO] requires no management of TSF, security attributes and TSF data, the application of the FMT components of [PP9911] is restricted.

5.1.6.1 Management of functions (FMT_MOF)

FMT_MOF.1.1 The TSF shall restrict the ability to *[selection*: *disable, modify the behavior of]* the functions *[assignment*: *TSF]* to *[assignment*: *NoRoles].*

Application note: The roles that may be considered here are S.VU and S.NON_VU only (see section 5.1.6.4). *NoRoles* is the list of roles containing none of them, i.e. the empty list (neither S.VU nor S.NON_VU).

5.1.6.2 Management of security attributes (FMT_MSA)

FMT_MSA.1.1 The TSF shall enforce the *[assignment: AC_SFP]* to restrict the ability to *[selection*: *modify, delete]* the security attributes *[assignment*: *read, write, modify]* to *[assignment: NoRoles]*.

Application note:

The security attributes are implicitly defined by AC_SFP (see section 5.1.4.2).

The roles that may be considered here are S.VU and S.NON_VU only (see section 5.1.6.4). *NoRoles* is the list of roles containing none of them, i.e. the empty list (neither S.VU nor S.NON_VU). Therefore the assignment of security attributes is not required.

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

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

Application note:

Security attributes must be always defined. There are no default values assigned.

FMT_MSA.3.2 The TSF shall allow the *[assignment*: *NoRoles]* to specify alternative initial values to override the default values when an object or information is created.

Application note: The roles that may be considered here are S.VU and S.NON_VU only (see section 5.1.6.4). *NoRoles* is the list of roles containing none of them, i.e. the empty list (neither S.VU nor S.NON_VU).

5.1.6.3 Management of TSF data (FMT_MTD)

FMT_MTD.1.1 The TSF shall restrict the ability *[selection: modify, delete, clear]* the *[assignment: any TSF data]* to *[assignment: NoRoles].*

Application note: The roles that may be considered here are S.VU and S.NON_VU only (see section 5.1.6.4). *NoRoles* is the list of roles containing none of them, i.e. the empty list (neither S.VU nor S.NON_VU).

5.1.6.4 Specification of management functions (FMT_SMF)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *[assignment: none].*

5.1.6.5 Security roles (FMT_SMR)

FMT_SMR.1.1 The TSF shall maintain the roles *[assignment: S.VU and S.Non-VU]*.

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

5.1.7 Privacy (FPR)

5.1.7.1 Unobservability (FPR_UNO)

FPR_UNO.1.1 The TSF shall ensure that *[assignment: S.OFFCARD]* are unable to observe the operation *[assignment: cryptographic operation] on [assignment: security data]* by *[assignment: any user]*.

The security data objects are defined in [TACHO, Appendix 10, chap. 2.2].

5.1.8 Protection of the TSF (FPT)

5.1.8.1 Failure with preservation of secure state (FPT_FLS)

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

This fulfils the following:

RLB_306 The TOE shall preserve a secure state during power supply cut-off or variations.

RLB_307 If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.

5.1.8.2 TSF physical protection (FPT_PHP)

FPT_PHP.3.1 The TSF shall resist *[assignment: physical manipulation and physical probing]* to the *[assignment: TSF]* by responding automatically such that the TSP is not violated.

Application note: This requirement is partially fulfilled by the underlying hardware, cf. [SLE66CX322P], SEF3.

5.1.8.3 Domain separation (FPT_SEP)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

After [JILTACHO] this requirement fulfils the specification of RLB_304 and RLB_305 in [TACHO], Appendix 10:

RLB_304 There shall be no way to analyze, debug or modify TOE's software in the field.

RLB_305 Inputs from external sources shall not be accepted as executable code.

5.1.8.4 Inter-TSF basic data consistency (FPT_TDC)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *[assignment: certificates, digital signatures]* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *[assignment: [TACHO], Appendix 11, CSM_020]* when interpreting the TSF data from another trusted IT product.

5.1.8.5 TSF testing (FPT_TST)

FPT_TST.1.1 The TSF shall run a suite of self tests *[selection: during initial start, periodically during normal operation]* to demonstrate the correct operation of the TSF.

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

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

This fulfils the following requirements from [TACHO], Appendix 10:

RLB_301 The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM.

RLB_302 Upon detection of a self test error the TSF shall warn the entity connected.

RLB_303 After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.

5.1.9 Trusted path/channels (FTP)

5.1.9.1 Inter-TSF trusted channel (FTP_ITC)

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

FTP_ITC.1.2 The TSF shall permit *[selection: the remote trusted IT product]* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[assignment: none]*.

This fulfils the following requirements from [TACHO], secure messaging:

DEX_301 The TOE shall verify the integrity and authenticity of data imported from a vehicle unit.

DEX_302 Upon detection of an imported data integrity error, the TOE shall:

- warn the entity sending the data,
- not use the data.

DEX_303 The TOE shall export user data to the vehicle unit with associated security attributes, such that the vehicle unit will be able to verify the integrity and authenticity of data received.

5.2 TOE Security Assurance Requirements

Assurance Requirements: EAL 4 augmented

Assurance Class	**Assurance Components**
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.2 (E3hAP)
ADV	ADV_FSP.2 ADV_HLD.2

	ADV_IMP.2 (E3hAP) ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.2 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.2 (E3hAP) ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4 (E3hAP)

Table 5.2.T1

The package E3hAP is defined in [JILTACHO], Annex A. In the Table T1 only those assurance classes are marked with "E3hAP" where augmentations above EAL 4 level are necessary. The detailed description of the E3hAP can be found in [JILTACHO].

5.2.1 Configuration management (ACM)

Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.1 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan. The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.2 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS)

ADO_IGS.2.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.2.1C The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.2.2C The installation, generation and start-up documentation shall describe procedures capable of creating a log containing the generation options used to gene-

rate the TOE in such a way that it is possible to determine exactly how and when the TOE was generated.

Application note [JILTACHO, A3, Note 2]: The term “generation” is always interpreted as “installation”. While installing the TOE, any configuration options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how the TOE was initially configured and when the TOE was installed.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3 Implementation of the TSF (ADV_IMP.2)

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Life cycle support (ALC)

5.2.5.1 Sufficiency of security measures (ALC_DVS.2)

ALC_DVS.2.1D The developer shall produce development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2 Testing: high-level design (ATE_DPT.2)

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

5.2.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Validation of analysis (AVA_MSU.3)

AVA_MSU.3.1D The developer shall provide guidance documentation.

AVA_MSU.3.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Application note: In [JILTACHO, A3 Note 9]: AVA_MSU.2 was selected, as it is most obvious. The AVA_MSU.3 is a higher hierarchical component to EAL4 (which includes AVA_MSU.2) (see section 8.3).

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3 Highly resistant (AVA_VLA.4)

AVA_VLA.4.1D The developer shall perform a vulnerability analysis.

AVA_VLA.4.2D The developer shall provide vulnerability analysis documentation.

AVA_VLA.4.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6C The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3 Security Requirements for the IT Environment

For the IT Environment no requirements are defined.

5.4 Security Requirements for the Non-IT Environment

R.Administrator_Guide (Application of Administrator Guidance)

The personalization of the initialized and tested tachograph card require a secure environment. This is outside the scope of the TOE development. The administrator guidance must address that and allow the personalization only after establishing a trusted communication. This procedure may based on session keys or the external authentication with challenge-response.

R.VU: The Vehicle Unit shall be certified either according to ITSEC E3 high (cf. [TACHO], Appendix 10) or according to CC [JILTACHO], sec. 2.2 and Annex A, assurance package E3hAP.

R.Process-Card (Protection during Packaging, Finishing and Personalisation): The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

5.5 Strength of Function

The minimum strength of functional requirements claimed is SOF high.

6 TOE Summary Specification

6.1 TOE Security Functions

Additionally to the security functions of the IC described in the ST of evaluation of the Infineon chip SLE66XC322P [SLE66C322P] the following TSF are defined:

6.1.1 SF1: Authentication based on PIN verification and retry counter

The SF1 provides for the workshop card a human user authentication by verifying of the PIN code (FIA_UAU.1).

For the Workshop card, the SF1 detects each unsuccessful authentication attempt of the human user. Whenever an unsuccessful attempt is detected, the Retry Counter for the PIN is decreased. When 5 consecutive unsuccessful authentication attempts have occurred, SF1:

- warns the entity connected,
- blocks the PIN check procedure such that any subsequent PIN check attempt will fail, and
- is able to indicate to subsequent users the reason of the blocking (FIA_AFL.1/WS-Card).

The SOF claimed for SF1 is high.

Note that identification of the human user occurs simultaneously with his authentication: If the authentication failed, the TOE supposes the subject S.OFFCARD.

6.1.2 SF2: Identification and Authentication based on Challenge-Response

SF2 allows the identification of a technical user (FIA_UID.1). The default identity of a technical user immediately after the ATR is S.NON-VU. After a successful authentication (using the mechanisms according to Appendix 11) has taken place, the user S.VU is recognized by the TOE (FIA_ATD.1). SF2 recognizes the following two subjects: S.VU and S.NON-VU. In case the subject S.VU has been recognized, an additional attribute USER_ID will be maintained (FIA_ATD.1, FIA_USB.1).

SF2 allows the authentication of a technical user. Even before authentication has taken place, the following actions are allowed for this user:

- All cards: reset, card identification, VU identification,

Driver and Workshop cards: Export user data with or without security attributes (card data download function),

Control and Company card: Export user data without security attributes except card-holder identification data (FIA_UAU.1).

Application note: Although the *List of TSF mediated actions* in the requirement FIA_UAU.1.1 of the generic security target [TACHO, p. 207] only mentions export of user data with security attributes (i.e. signatures), a user can, of course, also export unsigned user data (without security attributes).

SF2 stores appropriate keys and verifies appropriate certificates [TACHO, Appendix 11] to ensure that only security data are being used that have been distributed by the system (FIA_UAU.3, FPT_TDC.1).

SF2 uses a mutual device authentication mechanism, that is based on a Challenge-Response-Protocol, which makes use of random numbers during the authentication process. The challenge contains the random number and will be send from one party to the other. The latter answers with a response that can be verified by the first. A mutual authentication is a combination of two Challenge-Response procedures, where both parties act as claimant and verifier. "Authentication data" in FIA_UAU.4.1 are the complete set of data which are exchanged during the mutual device authentication process.

SF2 detects each unsuccessful external device authentication attempt. In such a case it warns the entity connected and assumes the user S.NON-VU as current user (FIA_AFL.1).

The SOF claimed for SF2 is high.

6.1.3 SF3: Data exchange under secure messaging

A communication channel between the TOE and S.VU will be encrypted with a randomly generated session key, such that the vehicle unit is able to verify the integrity and authenticity of data received (FTP_ITC.1, FCS_COP.1 (3DES), FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FDP_RIP.1). The channel will be closed if an

unrecognized message (malformed cryptogram) appears. Each message is protected by a Retail-MAC (see [TACHO, Appendix 11, CSM_022 and section 5.3]).

The TOE verifies the integrity and authenticity of data imported from a vehicle unit.

Upon detection of an imported data integrity error, the TOE:

- warns the entity sending the data,
- does not use the data.

The cryptographic operations are implemented in such a way that an observation does not yield any useful information about security data (FPR_UNO.1).

Note that object reuse (FDP_RIP.1) is not required by the EU legislative.

There are no sensitive data being imported without security attributes (FDP_ITC.1).

The SOF claimed for SF3 is high.

6.1.4 SF4: Data exchange with digital signature

The tachograph card is able to *generate a digital signature* (FCO_NRO.1, FCS_COP.1, FDP_DAU.1). The tachograph card is able to *export digital signatures* (and corresponding certificates) as well as the related *data* (FDP_ETC.2).

The cryptographic operations are implemented in such a way that an observation does not yield any useful information about security data (FPR_UNO.1).

There are no sensitive data being exported without security attributes (FDP_ETC.1).

The SOF claimed for SF4 is high.

Note that import and destruction of the static keys are out of scope.

6.1.5 SF5: Access Control of stored data objects

The TOE distinguishes the following subjects: S.VU and S.Non-VU (FDP_ACC.2, FMT_SMR.1). The different objects and their access types can be seen in [TACHO Annex I (B)] and are specified in more details in [TACHO Appendix 2].

The global security policy becomes apparent from

Annex I (B), chapter II *General characteristics and functions of the recording equipment*, section 4. *Security* (i.e. paragraph 012 and the previous one) as well as from

Annex I (B), chapter III *Construction and functional requirements for recording equipment*, sections 13. *Reading from tachograph cards* and 14. *Recording and storing on tachograph cards* (paragraphs 106 to 110).

SF5 enforces the Security Policy AC_SFP for the subjects S.VU and S.NON_VU. SF5 enforces the rules as required in FDP_ACF.1.

All security attributes are defined and implemented during the TOE developing. No security attributes can be modified (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1, FMT_MTD.1). The behavior of the security functions is once defined by the TOE developer and cannot be changed (FMT_MOF.1).

6.1.6 SF6: Accuracy and Audit

SF6 monitors the following events:

- cardholder authentication failure for the Workshop card (5 consecutive unsuccessful PIN checks),
- self test error,
- stored data integrity error (checksum over data stored in files),
- activity data input integrity error (Secure Messaging with VU).

Each part of the program code not stored in ROM as well as every file stored in the file system is protected by integrity checks. If an integrity check for program code fails, then the TOE enters a secure state. If an integrity check of a file fails, then the binary data is still accessible, but the status word indicates the data integrity error and thus warns the entity connected. An update or writing of a corrupted file is no more possible.

SF6 warns the entity connected upon detection of a data integrity error of the user data stored within the TSC.

This implements the requirement FAU_SAA.1, FDP_SDI.2.

6.1.7 SF7: Reliability

The requirements RLB_301 and RLB_302 from [TACHO] are considered as explaining component FPT_TST.1. Requirement RLB_303 [TACHO} uses the term “test” in a different context: RLB_303 considers tests during the development and generation of the TOE, while requirements RLB_301 and RLB_302 consider recurring self tests in the operational phase of the TOE.

The TOE contains tests at startup (power-on) as well as tests during normal operation. At every start-up the corresponding code stored in EEPROM is checked for integrity. An integrity check for all integrity-protected data (including keys) is applied every time such data is being used (i.e. if the data is read, the checksum is calculated and compared to the stored one). Upon detection of a self test error the TOE warns the entity connected (FPT_TST.1.1).

FPT_TST.1.2 is realized by the fact that some tests are performed after each reset – a user can trigger a reset at any time and doing so cause the power-on self tests (RLB_301) – and by the fact that for other data integrity is checked at every use of that data – simply reading integrity-protected data will cause the integrity check for these data to be performed. Thus it is not necessary to have a special command that triggers integrity checks.

Note: It is very important, that the tachograph card reports the outcome of the self tests back to the terminal. This is done by sending the respective return codes and ATR responses. The terminal can rely on the fact that if no error is being reported, the integrity is given. This fact also helps to demonstrate the correct operation of the TSF (see FPT_TST.1.1).

Note: Since every terminal and every user can trigger the self tests by resetting the card or by reading integrity-protected data, every terminal and every user is an authorized user in the sense of FPT_TST.1.2 (i.e. no additional authorization is necessary).

FPT_TST.1.3 is implemented by testing of executable code not stored in ROM is also required by (RLB_301). This requirement is fulfilled by an integrity check of all executable code stored in EEPROM which is performed after every reset.

After personalization phase is completed, all testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use. Commands associated exclusively with one life cycle phase can never be executed successfully during another phase (RLB_303).

The TOE does not allow to analyze, debug or modify TOE’s software in the field. Inputs from external sources will not be accepted as executable code (FPT_SEP.1).

The TOE preserves a secure state during power supply cut-off or variations. If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE will be reset cleanly (FPT_FLS.1).

The software part of the TOE reacts properly to all security relevant events being generated by the chip in response to any physical attack attempts as required by the chip evaluation results (cf. [SLE66CX322P], SEF3). This fulfils the SW-part of FPT_PHP.3.

Note that this functionality is partially implemented by the underlying hardware, cf. [SLE66CX322P, SEF3].

The TOE ensures that the content of temporarily allocated resources are made unavailable after de-allocation by overwriting this content with zeros (FDP_RIP.1).

6.2 SOF claim for TSF

For TSF identified in section 6.1 the SOF-high is claimed. The following TSF base on probabilistic or permutational mechanisms:

SF1 Authentication based on PIN verification and retry counter

The length of a free selectable PIN and the maximal value of the retry counter define the strength of this probabilistic mechanism.

SF2 Identification and Authentication based on Challenge-Response and retry counter

The source of randomness for the challenge and the maximal value of the retry counter define the strength of this probabilistic mechanism.

SF3 Data exchange under secure messaging

The source of randomness for the session key and the strength of the encryption algorithm define the strength of this probabilistic and permutational mechanism.

SF4 Data exchange with digital signature

The strength of the signature algorithm defines the strength of this probabilistic and permutational mechanism.

6.3 Assurance Measures

The documentation is produced compliant to the CC. The following documents provide the necessary information to fulfil the assurance requirements listed in 5.2.

ACM_AUT.1, ACM_CAP.4, ACM_SCP.2: Documentation for Configuration Management

ADO_DEL.2, ADO_IGS.2: Documentation for Delivery and Operation

ADV_FSP.2: Functional Specification for TCOS-Tacho-Card 3.0

ADV_HLD.2: High-Level Design for TCOS-Tacho-Card 3.0

ADV_IMP.2: Source Code for TCOS-Tacho-Card 3.0

ADV_LLD.1: Low-Level Design for TCOS-Tacho-Card 3.0

ADV_RCR.1: Correspondence Demonstration for TCOS-Tacho-Card 3.0

ADV_SPM.1: Security Policy Model for TCOS-Tacho-Card 3.0

AGD_ADM.1: Administrator Guidance for TCOS-Tacho-Card 3.0

AGD_USR.1: User Guidance for TCOS-Tacho-Card 3.0

ALC_DVS.2: Documentation for development security

ALC_LCD.1: Life-cycle model documentation

ALC_TAT.1: Documentation of the development tools

ATE.COV.2: Test Documentation for TCOS-Tacho-Card 3.0

ATE_DPT.2: Test Documentation for High-Level Design for TCOS-Tacho-Card 3.0

ATE_FUN.1: Test Documentation of the Functional Testing for TCOS-Tacho-Card 3.0

AVA_MSU.3: Analysis of the guidance documentation and testing for insecure states

AVA_SOF.1: Analysis of Strength of TSF for TCOS-Tacho-Card 3.0

AVA_VLA.4: Vulnerability Analysis for TCOS-Tacho-Card 3.0

The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developers master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

The implementation is based on a informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. The correspondence of the abstract specification of TSF in 6.1 with less abstract representations will be demonstrated in a separate document. This addresses ADV_FSP, ADV_HLD, ADV_LLD. ADV_IMP and ADV_RCR.

The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well–defined and use semiformal methods, i.e. a security model.

The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at TeleSec.

As the evaluation is identified as a composite evaluation based on the CC evaluation of the Infineon chip SLE66CX322P/m1484xx, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

7 PP Claims

The ST for the TOE claims conformance with the Protection Profile [PP9911] „Smartcard Integrated Circuit with Embedded Software“ and compliance with the Protection Profile [PP9806] as required in [TACHO]. According to the JIL interpretations and requirements in [JILTACHO] the compliance with [PP9806] is replaced by the evaluation of the IC against the Protection Profile BSI-PP-0002 [PP0002], i.e. **this ST claims conformance with [PP0002]**.

The evaluation is a composite evaluation and uses the results of the CC evaluation [BSI2003] provided by Infineon Technologies AG. The IC and its primary embedded software is evaluated at level EAL 5 with a minimum strength level for its security functions of SOF-high.

Additional to [PP9911] the following security objectives:

- **OT.Card_Identification_Data,**
- **OT.Card_Activity_Storage,**
- **OT.Data_Access,**
- **OT.Secure_Communication,**
- **OE.Secure_Communication**
- **OE.Personalization**

and the following security functional requirements are added to the ST:

- **FCO_NRO.1** (Selective proof of origin)
- **FCS_CKM.1** (Cryptographic key generation)
- **FCS_CKM.2** (Cryptographic key distribution)
- **FDP_ETC.2** (Export of user data without security attributes)
- **FIA_AFL.1/WS-Card** (Authentication failure handling for WS-Card)
- **FMT_SMF.1** (Specification of managment functions)

- **FTP_ITC.1** (Inter-TSF trusted channel).

The following assurance requirements are added

- **ADO_IGS.2** (Generation log)
- **ATE_DPT.2** (Testing low level design)
- **AVA_MSU.3** (Analysis and Testing for Insecure States).

This fulfils requirements from [TACHO].

8 Rationale

8.1 Security Objectives Rationale

The security objective rationale are traceable to all of the aspects in the TOE security environment and are suitable to cover them. It demonstrates that the security objectives are appropriate to counter the identified threats. The Security Objective Rationale of the TCOS-Tacho-Card 3.0 is based on the Security Objective Rationale of the [PP9911] and the [PP0002], which is referenced here, and therefore only the tachograph specific assumptions, threats, OSP's and objectives are covered in the present document and those in phase 6 from hardware evaluation that are not covered there.

8.1.1 Threats vs. Security Objectives

The following matrix give the rationale for the mapping of tachograph specific threats to security objectives

Threats – Security objectives	**OT.Card_Identification_Data**	**OT.Card_Activity_Storage**	**OT.Data_Access**	**OT.Secure_Communication**	**OT.TAMPER_ES**	**OT.DIS_MECHANISM2**	**OT.Personalization**	**OE.Secure_Communication**
T.Ident_Data	x							
T.Activity_Data		x	x	x				
T.Data_Exchange				x				x
T.DIS_ES2					x	x		
T.T_ES					x			
T.T_CMD					x			
T.MOD_LOAD					x			
T.MOD_EXE					x			
T.MOD_SHARE					x			
T.DIS_DEL1						x	x	
T.DIS_DEL2						x	x	
T.MOD_DEL1						x	x	
T.MOD_DEL2						x	x	

Table 8.1.1.T1

The following explanation of the table shows how the threats are related to the security objectives.

T.Ident_Data

The identification data (card data and cardholder data) stored during personalization can not be changed as described in OT.Card_Identification_Data, and that counters the threat of any modification (including deletion) of identification data.

T.Activity_Data

The activity data can be written by authenticated VU only, and the activity data is protected by a secure communication channel. The stored data can not be changed, because the file access is restricted to authenticated VU only. This means that the combination of the objectives OT.Card_Activity_Storage, OT.Data_Access and OT.Secure_Communication counters the threat T.Activity_Data.

T.Data_Exchange

The threat of modification of data transferred to the TOE from a authenticated VU and from the TOE to any user or an authenticated VU is countered by the security objective OT.Secure_Communication and OE.Secure_Communication. The data is secured by a secure channel and the application of a signature function with card specific keys.

T.DIS_ES2

Unauthorized disclosure of Embedded Software and Application Data is countered by tamper resistance of the TOE (OT.TAMPER_ES) and also countered by the fact that the Embedded Software's security mechanisms are protected against disclosure (OT.DIS_MECHANISM2).

T.T_ES

Theft or unauthorized use of TOE is also countered by the TOE's tamper resistance (OT.TAMPER_ES) as well as by the Embedded Software security mechanisms' protection against unauthorized disclosure (OT.DIS_MECHANISM2).

T.T_CMD

Unauthorized use of instructions or commands or sequence of commands sent to the TOE is countered by the fact that the TOE prevents tampering with its security critical

parts (OT.TAMPER_ES). Of course also the fact that the TOE is implemented correctly (as it will be proven by the evaluation) supports OT.TAMPER_ES in countering this threat.

T.MOD_LOAD, T.MOD_EXE and T.MOD_SHARE

Unauthorized loading of programs, unauthorized execution of programs and unauthorized modification of program behavior by interaction of different programs are all countered by the TOE's tamper resistance. Again this is supported by the correct implementation of the TOE.

T.DIS_DEL1, T.DIS_DEL2, T.MOD_DEL1, T.MOD_DEL2

Unauthorized disclosure and modification of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery to the IC designer is supported by the Embedded Software security mechanisms' protection against unauthorized disclosure (OT.DIS_MECHANISM2) and the security measures before the personalization (OT.Personalization).

8.1.2 Assumptions vs. Security Objectives

The tachograph specific assumption A.Personalization for the environment of the TOE is completely covered by the security objective OE.Personalization, because OE.Personalization requires the identification data, certificates and secret keys to be written to the TOE's filesystem under the control of the Administrator. The confidentiality of keys shall be further maintained during generation, transport and storage. This is what the assumption states, so A.Personalization is covered by the objective OE.Personalization.

The assumption A.Process-Card defined in [SLE66CX322P, section 3.2] is covered by OE.Process-Card as justified in [PP0002, section 7.1, paragraph 246].

8.1.3 Organizational Security Polices vs. Security Objectives

The IC hardware security target [SLE66CX322P] lists the two policies P.Process-TOE and P.Add-Functions:

- P.Process-TOE requires that "the TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to TOE Delivery) is secure so that no information is unintentionally made available for

the operational phase of the TOE"(cf. [PP0002]). In this composite ST, this fact has been formulated as assumptions A.Plat-Appl, A.Resp-Appl and A.Personalization (see section 3.4) instead of as a security policy. The assumptions mentioned already cover policy P.Process-TOE, so that no policy is necessary for this composite ST.

- P.Add-Functions states that the IC hardware "shall provide the following specific security functionality to the Smartcard Embedded Software: Area based Memory Access Control, Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Rivest-Shamir-Adleman (RSA)" (cf. [SLE66CX322P]). The IC hardware does provide this functionality, as has been proven during the hardware evaluation. The composite TOE, which already includes Smartcard Embedded Software, is not intended to provide such security functionality to other Smartcard Embedded Software.

Therefore there are no organizational policies in this composite ST that have to be covered by security objectives (cf. section 3.6).

8.2 Security Requirements Rationale

The mapping of the Functional and Assurance Requirements to Security Objectives demonstrates that the security requirements can be met and are traceable to security objectives.

8.2.1 Security Functional Requirement Rationale

The objectives taken from the [PP0002] are fulfilled by the IC hardware part of the composite TOE. A rationale for this can be found in [SLE66CX322P, section 8.2] for O.Add-Functions and in the PP [PP0002, section 7.2.1] for the other objectives.

Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication	OT.TAMPER_ES	OT.DIS_MECHANISM2
FAU_SAA.1	x					
FCO_NRO.1				x		
FCS_COP.1				x		
FCS_CKM.1				x		
FCS_CKM.2				x		
FCS_CKM.3				x		
FCS_CKM.4				x		
FDP_ACC.2	x	x	x			
FDP_ACF.1	x	x	x			
FDP_DAU.1			x			
FDP_ETC.1			x			
FDP_ETC.2			x	x		
FDP_ITC.1			x			
FDP_RIP.1			x			
FDP_SDI.2		x				
FIA_AFL.1			x			
FIA_AFL.1/WS-Card			x			
FIA_ATD.1			x			
FIA_UAU.1			x			
FIA_UAU.3			x			
FIA_UAU.4			x			
FIA_UID.1			x			
FIA_USB.1			x			
FMT_MOF.1			x			
FMT_MSA.1			x			
FMT_MSA.2			x			
FMT_MSA.3			x			
FMT_MTD.1			x			

TOE Security Functional Requirement / TOE Security objectives	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication	OT.TAMPER_ES	OT.DIS_MECHANISM2
FMT_SMF.1			x			
FMT_SMR.1			x			
FPR_UNO.1				x		
FPT_FLS.1			x		x	
FPT_PHP.3	x	x			x	x
FPT_SEP.1			x		x	x
FPT_TDC.1		x				
FPT_TST.1	x				x	x
FTP_ITC.1				x		

Table 8.2.1.T1

OT.Card_Identification_Data (Integrity of card identification data and cardholder identification data)

Integrity is provided by the security assurance requirements ALC_DVS.2, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE, which are not the operational phases of the TOE (only phase 7 is operational). The resistance to physical attack FPT_PHP.3 protects the data integrity from physical attacks. The TSF testing FPT_TST.1 and provides the authorized user with the capability to verify the integrity of the TSF-data i.e. the identification data. The potential violation analysis FAU_SAA.1 applies the accumulation or combination rule to stored data integrity errors for monitoring. In addition the Policy AC_SFO (FDP_ACC.2 and FDP_ACF.1) prevents the data to be modified by any subject (IDENTIF_WRITE rule).

OT.Card_Activity_Storage(Integrity of user data)

According to this security objective the TOE preserves user data written by authenticated VU. Within the phase 7 the access is controlled by the policy AC_SFP (FDP_ACC.2 and FDP_ACF.1, rule ACTIVITY_WRITE) and in connection with stored data integrity and action (FDP_SDI.2, FPT_TDC) the integrity and consistency is gua-

ranteed. The resistance to physical attack FPT_PHP.3 protects the data integrity from physical attacks.

OT.Data_Access (Data write access for authenticated vehicle units only).

The write access to designated data in the TOE is restricted to authenticated S.VU. Within the phase 7 the access is controlled by the policy AC_SFP (FDP_ACC.2 and FDP_ACF.1, rule ACTIVITY_WRITE). The components FDP_DAU.1, FIA_AFL.1, FIA_AFL.1/WS-Card, FIA_ATD.1 FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UID.1 and FIA_USB.1 ensure that the S.VU on the base of FMT_SMR.1 is identified and authorized prior to granting any access. The data itself can be authenticated (FDP_DAU.1) and the export and import of data is controlled under FDP_ETC.1, FDP_ETC.2 and FDP_ITC.1. The data domain for trusted subjects is secured by FPT_SEP.1. If an object with security attributes is allocated to a resource, then it can not be used after de-allocation (FDP_RIP.1). After a failure during operation the TOE enters a secure state FPT_FLS.1 with no access to the security domain FPT_SEP.1. No security attributes can be modified (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MOF.1, FMT_SMF.1).

OT.Secure_Communication

This security objective covers the integrity and confidentiality of exchanged data between the TOE and the card interface. It is controlled by the cryptographic support components FCS, FPR_UNO.1 and FTP_ITC.1. The TOE can export data with security attributes FDP_ETC.2, which provide capability to verify the evidence of origin, which is in addition required by selective proof of origin FCO_NRO.1

OT.TAMPER_ES

This security objective aims at preventing tampering with the TOE’s security critical parts. Security mechanisms have to prevent unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys. The embedded software must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.

The preservation of a secure state even when failures occur is required by FPT_FLS.1, thus covering the last aspect of OT.TAMPER_ES. Tampering and unauthorized modification of parameters through physical attacks is prevented by FPT_PHP.3. Unauthorized changes that occur as a result of interference and tampering by untrusted subjects is avoided through the separation of security domains, i.e. by FPT_SEP.1. Tampering can also be detected through TOE self tests as required by FPT_TST.1.

OT.DIS_MECHANISM2

This security objective aims at ensuring that the embedded software security mechanisms are protected against unauthorized disclosure.

Disclosure that occurs as a result of physical attacks is prevented by FPT_PHP.3. Disclosure as a result of interference and tampering by untrusted subjects is avoided by FPT_SEP.1. Since all testing-specific commands and actions shall be disabled or removed after OS testing is complete (see RLB_303), also FPT_TST.1 helps to protect the embedded software's security mechanisms from unauthorized disclosure.

OT.PERSONALIZATION

This security objective is not realized by functional requirements. The set of commands to be used for personalization is tested by the manufacturer of the TOE, the interface is described in FSP and in the Administrator guidance. The process of personalization will be considered in ADO_IGS and ADO_DEL.

8.2.2 Security Requirements are mutually supportive

The security target contains the following security functional requirements FCO_NRO.1, FCS_CKM.1, FCS_CKM.2, FDP_ETC.2, FIA_AFL.1/WS-Card and FPT_ITC.1 which are added to the security requirements from the PP9911. Therefore the following arguments for mutual support of the requirements are given only for the additional requirements (further evidence is given by fulfilment of the dependencies).

The FCO_NRO.1 requires the TOE to be able to generate the evidence of origin. This is attained by the creation of digital signature by the FCS_COP.1 operation for the RSA.

The FTP_ITC.1 requires the TOE to be able to establish trusted channel. The trusted channel will be established by cryptography FCS_COP.1 which uses sessions keys created according to FCS_CKM.1 and used according to FCS_CMK.2.

The FDP_ETC.2 requires the TOE to enforce the access policy AC_SFP when exporting user data. This is achieved by establishing a trusted channel to a VU. The trusted channel will be established by cryptography FCS_COP.1 which uses sessions keys created according to FCS_CKM.1 and used according to FCS_CMK.2. The generation of evidence of origin as required by [TACHO, DEX_305] is based on digital signatures FCS_COP.1 for RSA. The verification of origin is always possible because an unique secret RSA key is assigned to the TOE. The security parameters of the RSA

function FCS_COP.1 prevent the generation of a an evidence of origin by anybody else than the TOE.

The FIA_AFL.1/WS-Card requires the TOE initialized as a workshop card to detect and react on unsuccessful authentication attempts. This the same security requirement as for FIA_AFL.1 and do not need further analysis.

No detailed analysis is necessary for the assurance requirements because EAL4 is an established set of mutually supportive and internally consistent assurance requirements, the dependencies analysis in 8.3.5 for the additional assurance components shows that the assurance requirements are mutually supportive and internally consistent (all dependencies are satisfied).

8.2.3 Security Functional Requirements Dependencies

Some of the dependencies of the functional security requirements are not fulfilled in the PP9911. A rationale for this fact is given in the PP itself. The following table lists only requirements additional to this PP.

SFR	Dependencies	Comment
FCO_NRO.1	FIA_UID.1	fulfilled in this ST
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	fulfilled in this ST by FCS_COP.1, FCS_CKM.4 and FMT_MSA.2
FCS_CKM.2	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	fulfilled in this ST by FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	fulfilled in this ST by FDP_ACC.2
FMT_MSA.1	FMT_SMF.1	fulfilled in this ST
FMT_MTD.1	FMT_SMF.1	fulfilled in this ST
FMT_SMF.1	none	implicitly fulfilled
FTP_ITC.1	none	implicitly fulfilled
FIA_AFL.1/WS-Card	FIA_UAU.1	fulfilled in this ST

Table 8.2.3.T1

All other dependencies are completely fulfilled as the table above shows.

8.2.4 Non IT-Environment Security Requirement Rationale

The security objective for the non-IT-environment **OE.Secure_Communication** is covered by the non-IT-environment security requirement **R.VU.**

The security objective for the non-IT-environment **OE.Personalization** is covered by the non-IT-environment security requirement **R.Administrator_Guide**.

The security objective for the non-IT-environment **OE.Process-Card** is covered by the non-IT-environment security requirement **R.Process-Card**.

8.3 Evaluation Assurance Level Rationale

The assurance level for the TOE is EAL4 augmented. EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this ST is just such a product.

Augmentation results from the selection of:

- **ADO_IGS.2** Installation, generation, and start-up procedures
- **ADV_IMP.2** Implementation of the TSF
- **ALC_DVS.2** Development Security Measures
- **ATE_DPT.2** Testing: high-level design
- **AVA_MSU.3** Analysis and testing for insecure states
- **AVA_VLA.4** Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE is intended to function in different systems, it can be used in a PC with a smartcard reader. The TOE will be issued to users and may not be directly under the control of dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The augmentation by **ADO_IGS.2** is required by the JIL interpretation [JILTACHO]. ADO_IGS.2 has dependency with AGD_ADM.1. This dependency is met in the EAL4 assurance package.

The augmentation by **ADV_IMP.2** is also required by the JIL interpretation [JILTACHO] with respect to the evaluation level ITSEC E3. ADV_IMP.2 requires ADV_IMP.1 which is a subset of ADV_IMP.2. It has dependencies with ADV_LLD.1, ADV_RCR:1 and ALC_TAT.1, which are met in the EAL4 assurance package.

The augmentation by **ALC_DVS.2** is required by [PP9911] with no dependencies to other requirements.

The **ATE_DPT.2** is a higher component required by the JIL interpretation [JILTACHO] and needs testing at a low-level description to show the correct realization of all security functions. ATE_DPT.2 requires ATE_DPT.1 which is a subset of ATE_DPT.2. It has dependencies with ADV_HLD.2, ADV_LLD.1 and ATE_FUN.1, all these are met in the EAL4 assurance package.

The **AVA_MSU.3** is a higher hierarchical component to EAL4 (which includes AVA_MSU.2). AVA_MSU.3 has already been part of the HW-ST [SLE66CX322P] and is suggested as augmentation in [JILTACHO, note 9] – otherwise the evaluator's independent testing would have to be done as part of AVA_VLA.4.

AVA_MSU.3 has only dependencies (ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, and AGD_USR.1) that are already part of EAL4 and thus are fulfilled. The augmentation ADO_IGS.2, which is hierarchical to ADO_IGS.1, even exceeds the dependency.

The **AVA_VLA.4** is a higher hierarchical component to EAL4 required by the JIL Interpretation [JILTACHO].

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.Identification_Data and OT.Card_Activity_Storage.

AVA_VLA.4 has the following dependencies:

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

8.4 TOE Summary Specification Rationale

This summary specification shows that the TSF and assurance measures are appropriate to fulfill the TOE security requirements.

8.4.1 Mapping of TOE Security Requirements and TOE Security Functions

TOE Security Functional Requirements / TOE Security Functions	SF 1	SF 2	SF 3	SF 4	SF 5	SF 6	SF 7
FAU_SAA.1						x	
FCO_NRO.1				x			
FCS_COP.1			x	x			
FCS_CKM.1			x				
FCS_CKM.2			x				
FCS_CKM.3			x				
FCS_CKM.4			x				
FDP_ACC.2					x		
FDP_ACF.1					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	
FIA_AFL.1		x					
FIA_AFL.1/WS-Card	x						
FIA_ATD.1		x					
FIA_UAU.1	x	x					
FIA_UAU.3		x					
FIA_UAU.4		x					
FIA_UID.1		x					
FIA_USB.1		x					
FMT_MOF.1					x		
FMT_MSA.1					x		
FMT_MSA.2					x		
FMT_MSA.3					x		
FMT_MTD.1					x		

FMT.SMF.1					x		
FMT_SMR.1					x		
FPR_UNO.1			x	x			
FPT_FLS.1							x
FPT_PHP.3							x
FPT_SEP.1							x
FPT_TDC.1		x					
FPT_TST.1							x
FTP_ITC.1			x				

Table 8.4.1.T1

Each TOE security functional requirement is implemented by at least one security function. How and whether the security functions actually implement the TOE security functional requirement is described in section 6.1.

8.4.2 Assurance measure rationale

Assurance measures from chap 6.3 cover the assurance requirements from 5.2.

8.4.3 Rationale for Minimum Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives of the tachograph specification OT.Identification_Data, OT.Card_Activity_Storage, OT.Data_Access and OT.Secure_Communication and from [PP9911]. The protection against attacks with a high attack potential dictates a high rating for strength of functions in the TOE that are realized by probabilistic or permutational mechanisms.

The SOF of SF is consistent with SOF of the functional requirement because all are selected 'high'.

9 References

[CC]

Common Criteria for Information Technology Security Evaluation, Version 2.1 Incorporated with interpretations as of 2002-02-28, http://www.commoncriteria.org

[ALGO]

Algorithms and Parameters for Secure Electronic Signatures, ETSI Special Report SR 002176 Version 1.1.1 (2003-03)

[BSI2003]

Certification Report BSI-DSZ-0223-2003 for Infineon Smart Card (Security Controller SLE66CX322P with RSA 2048/m1484a24, m 1484a27 and m1484b14 from Infineon Technologies, 2003-10-07

[PP0002]

Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Registered and certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0002

[PP9911]

Smart Card Integrated Circuit With Embedded Software Protection Profile, Version 2.0, June 99. Registered by the French Certification Body under the reference PP/9911

[PP9806]

Protection Profile Smartcard Integrated Circuit, Version 2.0, Issue September 1998, Registered at the French Certification Body under the number PP/9806

[TACHO]

Commission Regulation (EC) No 1360/2002 of 13 June 2002 on recording equipment in road transport, Official Journal L 207, 5.8.2002

[JILTACHO]

JIL Security Evaluation and Certification of Digital Tachographs Version 1.12, JIL Working

Group (BSI, CESG, DCSSI and NLNCSA), June 2003

[SLE66CX322P]

Evaluation Documentation SLE66CX322P with RSA2048/m1484, Security Target, Version 1.0.5, 2002-06-05

[AIS36]

Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 1, Zertifizierungsstelle des BSI, Stand 29.07.2002