Security Target Lite STARCOS 3.4 ID Tachograph C2

Version 2.0 / Status 29.06.2010

Author CSRD22/stut
Status Open
File y:\cc_evaluation_int\eval_tachograph\15000-evaluation_documentation\15100-ase_security_target\gdm_sta34_tacho_ase.doc

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Contents

1 ST Introduction

1.1 ST Reference

Title: Security Target Lite STARCOS 3.4 ID Tachograph C2
Reference: GDM_STA34_TACHO_ASE

Version Number: Version 2.0 / Status 29.06.2010

Origin: Giesecke & Devrient GmbH

Author: Dr. Ulrich Stutenbäumer

CC Version: 3.1 (Revision 2)

Assurance Level: EAL4-augmented with the following assurance components: ADV_IMP.2, ALC_DVS.2 and AVA_VAN.5.

TOE: STARCOS 3.4 ID Tachograph C1

TOE documentation:

- Preparative procedures STARCOS 3.4 ID Tachograph C2, [GUI Pre]
- Operational user guidance STARCOS 3.4 ID Tachograph C2, [GUI Ope]

HW-Part of TOE: ATMEL AT90SC24036RCU [STL]. This TOE was evaluated against Common Criteria Version 2.3.

1.2 ST Overview

The aim of this document is to describe the Security Target for STARCOS 3.4 ID Tachograph C2**.** In the following chapters STARCOS 3.4 ID Tachograph C2 stands for the Target of Evaluation (TOE).

The related product is the **STARCOS 3.4 ID Tachograph C1Card**.
In the following chapters, STARCOS 3.4 ID Tachograph C1Card stands for the product.

STARCOS 3.4 ID Tachograph C1Card contains the TOE consisting of the:

- STARCOS 3.4 ID operation system
- Tachograph C2 application

and depends on the secure ATMEL AT90SC24036RCU chip being certified according to CC EAL5+ [STL] .

STARCOS 3.4 ID Tachograph C2 consists of the related software in combination with the underlying hardware ('Composite Evaluation').

The TOE complies with the Tachograph Card Specification Annex 10 and Annex 11 of EC regulation 1360/2002 [TACH]. This implies the compliance with PP9911 [PP9911] and PP0002 [PP0002]. All issues related with the ATMEL AT90SC24036RCU security controller have already been covered by a hardware evaluation [STL] .

This document describes:

- the Target of Evaluation (TOE): STARCOS 3.4 ID Tachograph C2
- the security environment of the TOE: Security Problem Definition
- the security objectives of the TOE and its environment: Security Objectives
- the TOE security functional and assurance requirements: Security Functional Requirements, Security assurance requirements

The assurance level for the TOE is CC **EAL4 augmented**.

1.2.1 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the conformance claims for the Security Target.

Section 3 provides a discussion of the security problems for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment and the security objective rational to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 5 contains the security functional requirements and assurance requirements derived from the Common Criteria [CC1], Part 2 [CC2] and Part 3 [CC3], which must be satisfied and the security functional requirements rational. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 6 contains the TOE Summary Specification.

Section 7 provides information on used acronyms and definitions and the used references.

1.3 Typographic Conventions

- **<u>This typeface</u>** is used to highlight assignments and selections for SFRs completed by the ST author.
- **This typeface** or ***this typeface*** is used to highlight assignments and selections for SFRs defined in the PP.

1.4 Change History

Version	Date	Changes	Responsible
2.0	29.06.10	TOE name updated	stut

1.5 Tables

1.6 TOE Overview

This section presents the architecture and the common usages of the Target of Evaluation (TOE).

The TOE is a Smart Card with an operating system (STARCOS 3.4 ID Tachograph C2) and a dedicated filesystem according to the intended type of the tachograph card.

The components of the TOE are therefore the underlying hardware (IC), the operating system STARCOS 3.4 ID Tachograph C2 (ES) and the dedicated filesystem (FS).

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

- 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.

1.6.1 List of Security Featrures

The following list the main security features and the security behaviour of the TOE:

- unauthorised authentication attempts (Workshop card) are detected by a PIN check procedure that uses a Retry Counter,
- a mutual device authentication mechanism is established based on a Challenge-response Protocol,
- a secure communication channel between the TOE and the S.VU. is established by secure messaging,
- the integrity and authenticity of data imported from a S.VU. is verified and
- the entity connected upon detection of a data integrity error of the user data is warned,
- the generation and export of digital signatures is possible,
- specific EEPROM data is checked for integrity at every start-up and
- analyzing, debugging or modifying TOE's software in the field is not possible.

1.6.2 TOE life cycle

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. [[TACH], Appendix 10] formulated in the current ST is valid only for phase 7.

The correct delivery and the correct personalization are covered by the Preparative procedures document. 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 during phase 6 of the TOE life cycle after initialization, testing of the OS and creation of the dedicated filesystem with security attributes has taken place.

1.6.3 Intended environment, intended method of use

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

During the end-usage phase of a tachograph card life-cycle (phase 7 of life-cycle), vehicle units only may write user data to the card.

The functional requirements for a tachograph card are specified in Annex 1B body text and Appendix 2 [TACH].

A more detailed description can also be found in those and other documents from the EU ordinance [EU Ord]. Annex I (B) gives a complete overview of what functionality each part of a digital tachograph system (recording equipment, tachograph card) has to provide. From this description it becomes clear that the functionality provided by the tachograph card is appropriate for the intended method of use.

1.7 TOE Description

1.7.1 Physical scope of the TOE

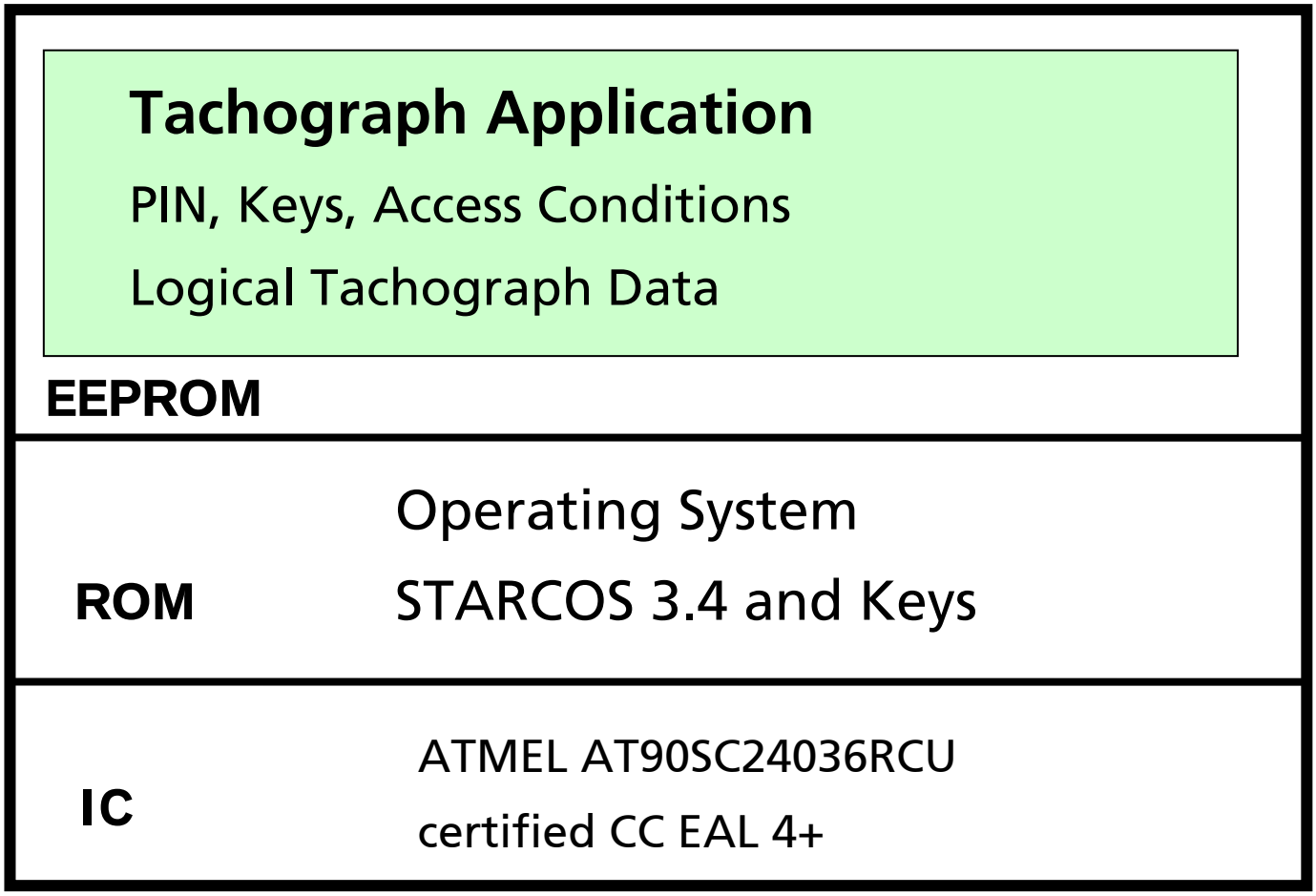
The tachograph card consists of the tachograph card hardware (chip), the tachograph card software (chip operating system and tachograph application) and the accompanying guidance documentation. The hardware consists of the chip ATMEL AT90SC24036RCU that has already been evaluated according to EAL 4 [STL]. The software consists of the chip operating system STARCOS 3.4 ID Tachograph C2 and one appropriate application out of the four applications (data structure and data) defined in Appendix 2 (driver, company, workshop, control) [TACH][TACH]. Although the TOE is defined as being hardware (ATMEL AT90SC24036RCU) and software (STARCOS 3.4 ID Tachograph C2 plus application); for this evaluation we will base upon the existing certificate of the chip to cover the hardware aspects and focus on the software.

The accompanying guidance documentation consists of the preparative procedures [GUI Pre] and the operational user guidance [GUI Ope].

1.7.2 Logical scope of the TOE

The basic functions of the tachograph card are:

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



2 Conformance claims

2.1 CC conformance Claim

This TOE claims conformance to Common Criteria V3.1 as follows:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2006-09-001, Version 3.1, Revision 1, September 2006, [CC1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2007-09-002, Version 3.1, Revision 2, September 2007, [CC2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2007-09-003, Version 3.1, Revision 2, September 2007, [CC3].

as follows

- Part 2 extended,

- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2007-09-004, Version 3.1, Revision 2, September 2007, [CEM].

and the

- JIL (Joint Interpretation Library) document “Security Evaluation and Certification of Digital Tachographs” [JIL]

have to be taken into account.

2.2 PP Claim

This ST is compliant with [PP9911]and [PP0002].

Since the HW-Part of TOE: ATMEL AT90SC24036RCU [STL] 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.

2.3 PP Additions and Refinements

There are no PP additions and refinements used in this ST.

2.4 Package Claim

The current ST is conformant to the following security requirements package:

– Assurance package EAL4 augmented with ADV_IMP.2, ALC_DVS.2 and AVA_VAN.5 as defined in the CC, part 3 [CC3].

2.5 Conformace Claim Rationale

2.5.1 TOE Type

The TOE type stated in chapter 1.1 is obviously commensurate with the current TOE type in the claimed PPs [PP9911] and [PP0002] without any additional items.

2.5.2 SPD Statement

The security problem definition (SPD) of the current ST in chapter 3 contains the security problem definition of the claimded PPs [PP9911] and [PP0002] without any additional items.

2.5.3 Security Objectives Statement

The security objectives statement for the TOE in the current ST includes all the security objectives for the TOE of the PPs [PP9911] and [PP0002] without any additional items.

2.5.4 Security Requirements Statement

The SFR statement for the TOE in the current ST includes all the SFRs for the TOE of the PPs [PP9911] and [PP0002]..

2.6 Conformance Statement

This ST *claims* conformance to the PPs [PP9911] and [PP0002] .

3 Security Problem Definition

3.1 Assets

Assets are security-relevant elements to be directly protected by the TOE.

The primary and secondary assets defined in Atmel [STL], 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), this corresponds to the User Data in Atmel [STL].

The TOE itself and its correct operation, including the additional asset from [STL], the random number generator, are assets.

Assets have to be protected in terms of confidentiality, and integrity. The assets to be protected by the TOE are listed below.

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 and storage.
5. SVD (Signature Verification Data): public keys certified by Certification Authorities, to verify electronic signatures (i.e. of certificates).
6. VAD (Verification authentication data): authentication data provided as input by knowledge (PIN).
7. RAD (Reference authentication data): data persistently stored by the TOE for verification of the authentication attempt as authorized user.
8. DTBS (Data to be signed): 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.

3.2.1 S.Administrator

It is installing the security data and identification data.

3.2.2 S.VU

It is the vehicle unit (activity data recording device) with a UserID.

3.2.3 S.Non-VU

It is the non vehicle unit (without a UserID).

3.2.4 S.OFFCARD

An attacker is a threat agent. It is a human or 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.

3.3 Assumptions

The assumption A.Process-Card is defined in Atmel [STL] . 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 assumption A.Process-Card also applies 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.

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 following chapter) but they are relevant only for phase 6.

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

3.3.1 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 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 [[TACH_GST], CSM_014].

Note: 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. $2^{1023} < x < 2^{1024}$.

3.4 Threats

The following threats are described in Atmel, [STL]:

- T.Phys-Manipulation
- T.Phys-Probing
- T.Malfunction
- T.Leak-Inherent
- T.Leak-Forced
- T.Abuse-Function
- T.Mem-Access
- T.RND

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

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, T.CLON, T.DIS_INFO, T.DIS_DEL, T.T.DEL, T.MOD_DEL, T.MOD_SOFT.[1]

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 classe ALC.

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

3.4.1 T.Ident_Data

A successful modification of identification data held by the TOE (IDD (see 3.1.1) e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.

The threat agent for T.Ident_Data is S.OFFCARD.

3.4.2 T.Activity_Data

A successful modification of activity data stored in the TOE (ACD, see 3.1.1) would be a threat to the security of the TOE.

The threat agent for T.Activity_Data is S.OFFCARD.

3.4.3 T.Data_Exchange

A successful modification of activity data (ACD, see 3.1.1 addition, deletion, modification) during import or export would be a threat to the security of the TOE.

The threat agent for T.Data_Exchange is S.OFFCARD.

3.4.4 T.Disclosure

An unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or Application Data (see 3.1.1) would be a threat to the security of the TOE.

The threat agent for T.Disclosure is S.OFFCARD.

---

[1] T.CLON is addressed by O.CLON, T.DIS_INFO by O.DEV_DIS_ES, T.DIS_DEL by O.DEV.TOOLS, O.DEV_DIS_ES, O.SOFT_DLV and O.INIT_ACS, T.T.DEL by O.SOFT_DLV, T.MOD_DEL by # O.DEV_DIS_ES, O.SOFT_DLV and O.INIT_ACS, T.MOD_SOFT by O.TAMPER_ES, O.OPERATE, O.FLAW and O.MOD_MEMORY.

3.5 Organisational 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 Atmel, [STL]. However, these policies are not needed for this composite ST.

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 Atmel [STL] , the security objectives for the embedded software (OS) are referenced in the [PP9911].

The following objectives are taken over from the Atmel [STL] 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.DEV_DIS_ES*
- O.OPERATE*
- O.FLAW*
- O.DEV_DIV_ES*
- O.DIS_MECHANISM2
- O.DIS_MEMORY*
- O.MOD_MEMORY*

All objectives taken from the Atmel [STL] 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:

4.1.1 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.

4.1.2 OT.DIS_MECHANISM2

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

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

4.1.3 OT.Card_Identification_Data

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

4.1.4 OT.Card_Activity_Storage

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

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

4.1.5 OT.Data_Access

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

4.1.6 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.

4.1.7 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 Operational Environment

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

- 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.

4.2.1 OE.Secure_Communication

The environment shall support secure communication protocols and procedures.

4.2.2 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 [[TACH_GST], CSM_014].

4.2.3 OE.Non_Disclosure

During the smart card embedded software development phase the ES and/or Application Data shall be protected against unauthorized disclosure.

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 T.Ident_Data

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

4.3.1.2 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.

4.3.1.3 T.Data_Exchange

The threat of modification of data transferred to the TOE from an 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.

4.3.1.4 T.Disclosure

The threat of an unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or Application Data is countered by the security objective for the operational environment OE.Non_Disclosure. The ES and the application data are secured by the secure environment in that the ES and the Application Data is created an transferred to the TOE mask and by the security guidelines and their compliance by the development team.

4.3.1.5 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).

4.3.1.6 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).

4.3.1.7 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.

4.3.1.8 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 (OT.TAMPER_ES).

4.3.1.9 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 countered by the Embedded Software security mechanisms' protection against unauthorized disclosure (OT.DIS_MECHANISM2) and the security measures before the personalization (OT.Personalization).

4.3.2 Assumptions

4.3.2.1 A. Personalization

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.

4.3.3 Organisational security policies

There are no organizational policies in this composite ST that have to be covered by security objectives.

Threats - Security objectives	OT.TAMPER_ES	OT.DIS_MECHANISM2	OT.Card_Identification_Dat	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication	OT.Personalization	OE.Secure_Communication	OE.Non_Disclosure
T.Ident_Data			X						
T.Activity_Data			X	X	X	X			
T.Data_Exchange						X		X	
T.Disclosure									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 1 Threats versus security objectives rationale

5 Security Requirements

5.1 Security Functional Requirements

5.1.1 Security Functional Requirements for the TOE

5.1.1.1 FAU Security Audit

This group is focused on requirements from [PP9911], TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, Chap. 4.5 [TACH_GST].

FAU SAA	Security Audit Analysis

5.1.1.1.1 FAU_SAA.1 Potential Violation Analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.1.1.1 *FAU_SAA.1.1*

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

5.1.1.1.1.2 *FAU_SAA.1.2*

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

a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation;

b) [assignment: any other rules].

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

a) Accumulation or combination of

- **card holder authentication failure,**
- **self test error,**
- **stored data integrity error,**
- **activity data input integrity error,**

known to indicate a potential security violation;

b) **none**.

5.1.1.2 FCO Communication

This group is focused on requirements from TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, [TACH_GST] Chap. 4.8.2.

FCO_NRO	Non-Repudiation of Origin

5.1.1.2.1.1 *FCO_NRO.1 Selective Proof of Origin*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

5.1.1.2.1.2 *FCO_NRO.1.1*

The TSF shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].

The TSF shall be able to generate evidence of origin for transmitted [download data] at the request of the [recipient].

Refinement

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

5.1.1.2.1.3 *FCO_NRO.1.2*

The TSF shall be able to relate the [assignment: list of attributes] of the originator of the information, and the [assignment: list of information fields] of the information to which the evidence applies.

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

Refinement

DEX_306 The TOE shall be able to download data to external storage media (attached to an IFD) with associated security attributes (=digital signature) such that downloaded data integrity can be verified.

5.1.1.2.1.4 *FCO_NRO.1.3*

The TSF shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin].

The TSF shall provide a capability to verify the evidence of origin of information to [the recipient] given [no limitation].

Refinement

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

5.1.1.3 FCS Cryptographic Support

This group is focused on requirements from TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, Chap. 4.9 [TACH_GST].

FCS_CKM Cryptographic Key Management

5.1.1.3.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation,

FCS_CKM.4 Cryptographic key destruction

5.1.1.3.1.1 FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [generation of a 3-DES session key] and specified cryptographic key sizes [of double length (128 bits with 112 bits entropy, no parity bits set)] that meets the following:

[

- ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998

- EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 3.1.3 (CSM_012), 3.2 (CSM_015) and 4 (CSM_020)

].

Refinement

CSP_301 If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms (see: Appendix 11, chapter 4 [TACH]) and specified cryptographic key sizes. (…)

5.1.1.3.2 FCS_CKM.2 Cryptographic Key Distribution

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

5.1.1.3.2.1 *FCS_CKM.2.1*

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards].

5.1.1.3.2.1.1 FCS_CKM.2.1.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [3-DES session key agreement by an internal-external authentication mechanism] that meets the

following:

[

- **ISO/IEC 9798-3 Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 2: Entity Authentication Using a Public Key Algorithm, Second Edition 1998**
- **EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 3.1.3 (CSM_012) and 4 (CSM_020), Appendix 2, chapter 3.6.8 and 3.6.9**

].

Refinement

CSP_302 If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods (see: Appendix 11, chapter 3.1 [TACH]).

5.1.1.3.2.1.2 FCS_CKM.2.1.2

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [import of public RSA-keys by certificates (non self-descriptive card verifiable certificates in conformance with ISO/IEC 7816-8(] that meets the

following:

[

EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 3.1.3 (CSM_012) and 4 (CSM_020), Appendix 2, chapter 3.6.8 and 3.6.9

].

Refinement

CSP_302 If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods (see: Appendix 11, chapter 3.1 [TACH]).

5.1.1.3.2.1.3 FCS_CKM.2.1.3

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [import of key material] that meets the following:

[

Cryptographically secured import (encryption using the public part of a dedicated RSA-key pair of the card)

].

Refinement

CSP_302 If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods (see: Appendix 11, chapter 3.1 [TACH]).

5.1.1.3.3 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FDP_ITC.1.1 Import of user data without security attributes

5.1.1.3.3.1 FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

5.1.1.3.3.1.1 FCS_CKM.4.1.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [by physical deletion by overwriting the memory data with zeros or random data of 3-DES session keys] that meets the following:

[

EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 3.1.3 (CSM_013), Apendix 2, chapter 3.6.8 (TCS_353)

].

5.1.1.3.3.1.2 FCS_CKM.4.1.2

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [by physical deletion by overwriting the memory data with zeros or random data of private RSA keys] that meets the following:

[

EU Tachograph Specification [TACH] , Annex 1B, Appendix 2, chapter 3.6.10 (TCS_363)

].

FCS_COP Cryptographic Operation

5.1.1.3.4 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

5.1.1.3.4.1 FCS_COP.1.1

The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

5.1.1.3.4.1.1 FCS_COP.1.1.1

The TSF shall perform [the explicit signature generation and verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [of 1024 bits] that meet the following:

[

- **PKCS#1 (with SHA-1) signature generation / verification scheme, RSA Encryption Standard Version 2.0, October 1998**
- **SHA-1, FIPS Pub. 180-1, NIST, April 1995**
- **EU Tachograph Specification [TACH] , Appendix 11, chapter 2.2.1 (CSM_003), 2.2.2 (CSM_004), 6.1 (CSM_034) and 6.2 (CSM_035)**

].

5.1.1.3.4.1.2 FCS_COP.1.1.2

The TSF shall perform [the implicit signature generation and verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [of 1024 bits] that meet the following:

[

- **ISO/IEC 9796-2 Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2 : Mechanisms Using a Hash Function, First Edition, 1997**
- **SHA-1, FIPS Pub. 180-1, NIST, April 1995**
- **EU Tachograph Specification [TACH] , Appendix 11, chapter 2.2.1 (CSM_003), 2.2.2 (CSM_004), 4 (CSM_020), 3.3.2, 3.3.3**

]

5.1.1.3.4.1.3 FCS_COP.1.1.3

The TSF shall perform [the implicit encryption and decryption operations concerning asymmetric cryptograhy] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [of 1024 bits] that meet the following:

[

EU Tachograph Specification [TACH] , Appendix 11, chapter 2.2.1 (CSM_003), 4

].

5.1.1.3.4.1.4 FCS_COP.1.1.4

The TSF shall perform [the encryption and decryption operations concerning symmetric cryptograhy] in accordance with a specified cryptographic algorithm [3-DES in CBC mode with ICV=0] and cryptographic key sizes [of 128 bits] that meet the following:

[

- **DATA Encryption Standard, FIPS Pub. 46-3, NIST, Draft 1999**
- **ANSI X9.52 Triple Data Encryption Algorithm Modes of Operations 1998**
- **EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 2.2.3 (CSM_005), 5.4 (CSM_031)**

].

5.1.1.3.4.1.5 FCS_COP.1.1.5

The TSF shall perform [the MAC calculation concerning symmetric cryptograhy] in accordance with a specified cryptographic algorithm [DES Retail-MAC] and cryptographic key sizes [of 128 bits] that meet the following:

[

- **ANSI X9.19 Financial Institution Retail Message Authentication 1986**
- **EU Tachograph Specification [TACH] , Annex 1B, Appendix 11, chapter 2.2.3 (CSM_005), 5.4 (CSM_031)**

].

5.1.1.4 FDP User Data Protection

This group is focused on requirements from TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, Chap. 4.3.1, 4.4 [TACH_GST].

FDP_ACC Access control Policy

5.1.1.4.1 FDP_ACC.2 Complete Access Control

Hierarchical to: FDP_ACC.1

Dependencies: FDP_ACF.1.1 Security attribute based access control

5.1.1.4.1.1 FDP_ACC.2.1

The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

5.1.1.4.1.1.1 FDP_ACC.2.1.1

The TSF shall enforce the [AC_SFP] on

[

subjects:

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

objects:

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

]

and all operations among subjects and objects

covered by the SFP.

5.1.1.4.1.1.2 FDP_ACC.2.1.2

The TSF shall enforce the [PERS-AC_SFP] on

[

subjects:

- **personalisation units**
- **other card interface devices (non-personalisation units)**

objects:

- **data fiels for user data:**
  - **identification data**
  - **activity data**
- **data fiels for security data as:**
  - **cards´s signature key pair**
  - **public keys**
  - **PIN (for workshop card)**
  - **static personalisation key (if applicable)**
- **security data:**
  - **card´s private personalisation key**
  - **card´s public personalisation key**
  - **personalisation unit´s public personalisation key**
  - **static personalisation key (if applicable)**
  - **session keys**
  - **card´s private authentication key**
- **TOE software code**
- **TOE file system**
- **identification data of the TOE**
- **data field for identification data of the TOE`s personalisation**

]

and all operations among subjects and objects

covered by the SFP.

5.1.1.4.1.2 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.

FDP_ACF	Access control Functions

5.1.1.4.2 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: no other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.1.1.4.2.1 FDP_ACF.1.1

The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

5.1.1.4.2.1.1 FDP_ACF.1.1.1

The TSF shall enforce the [AC_SFP] to objects based on the following:

[

subjects:

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

objects:

- **user data:**
  - **identification data (card identification data, cardholder identification data)**
  - **activity data (cardholder activities data, events and faults data, control activity data)**
- **security data:**
  - **card´s private signature key**
  - **public keys**
  - **session keys**
  - **PIN (for workshop card)**
  - **nature key, imported public keys)**
- **TOE software code**
- **TOE file system (incl. file structure, add. inter- nal structures, access conditions)**
- **identification data of the TOE (-IC, -ES)**
- **identification data of the TOE´s personalisation**

security attributes for subjects:

- **USER_GROUP**
- **USER_ID**

security attributes for objects:

- **access rules**

].

5.1.1.4.2.1.2 FDP_ACF.1.1.2

The TSF shall enforce the [PERS-AC_SFP] to objects based on the following:

[

subjects:

- **personalisation units**
- **other card interface devices (non-personalisation units)**

objects:

- **data fiels for user data:**
  - **identification data**
  - **activity data**
- **data fiels for security data as:**
  - **cards´s signature key pair**
  - **public keys**
  - **PIN (for workshop card)**
  - **static personalisation key (if applicable)**
- **security data:**
  - **card´s private personalisation key**
  - **card´s public personalisation key**
  - **personalisation unit´s public personalisation key**
  - **static personalisation key (if applicable)**
  - **session keys**
  - **card´s private authentication key**
- **TOE software code**
- **TOE file system**
- **identification data of the TOE**
- **data field for identification data of the TOE`s personalisation**

security attributes for subjects:

- **USER_GROUP**
- **USER_ID**

security attributes for objects:

- **access rules**

]

5.1.1.4.2.2 *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: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

5.1.1.4.2.2.1 FDP_ACF.1.2.1

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

- **GENERAL_READ:**
  - **driver card, workshop card: user data may be read from the TOE by any user**
  - **control card, company card: user data may be read from the TOE by any user, except cardholder identification data which may be read by S.VU only;**
- **IDENTIF_WRITE:**
  all card types: identification data may only be written once and before the end of phase 6;
- **ACTIVITY_WRITE:**
  all card types: activity data may be written to the TOE by S.VU only;
- **SOFT_UPGRADE: software;**
- **IDENTIF_TOE_READ:**
  all card types: identification data of the TOE may be read from the TOE by any user;
- **IDENTIF_TOE_WRITE:**
  all card types: identification data of the TOE may only be written before end of phase 6;
- **IDENTIF_TOE_PERS_WRITE:**
  all card types: identification data of the TOEs personalisation may only be written before end of phase 6.

5.1.1.4.2.2.2 FDP_ACF.1.2.2

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

- **FILE_STRUCTURE:**
  all card types: files structure and access conditions shall be created before end of phase 5.

Refinements

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 personalisation. This indication shall remain unalterable.

5.1.1.4.2.3 FDP_ACF.1.3

The TSF shall explicitily authorise access of subjects to objects based on the following additional rules: [assignements: rules, based on security attributes, that explicitily authorise access of subjects to objects].

5.1.1.4.2.3.1 FDP_ACF.1.3.1

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

5.1.1.4.2.4 FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on secur/ty attr/butes, that expl/c/tly deny access of subjects to objects].

5.1.1.4.2.4.1 FDP_ACF.1.4.1

The TSF shall explicitly deny access of subjects to objects based on the [none].

FDP DAU Data Authentication

5.1.1.4.3 FDP_DAU.1 Basic Data Authentication

Hierarchical to: no other components

Dependencies: none

5.1.1.4.3.1 FAU_DAU.1.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or /nformat/on types].

5.1.1.4.3.1.1 FAU_DAU.1.1.1

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

5.1.1.4.3.2 FDP_DAU.1.2

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

5.1.1.4.3.2.1 FDP_DAU.1 .2-1

The TSF shall provide [any subject (i.e. S.VU and other card interface devices (S.Non-VU)] with the ability to verify evidence of the validity of the indicated information.

FDP_ETC Export to Outside TSF Control

5.1.1.4.4 FDP_ETC.1 Export of User Data without Security Attributes

Hierarchical to: no other components

Dependencies: [FDP ACC.1 Subset access control or FDP IFC.1 Subset information flow control]

5.1.1.4.4.1 *FDP_ETC.1.1*

The TSF shall enforce the [assignment: access control SFR(s) and/or information flow control SFR(s)] when exporting user data, controlled under the SFP(s), outside of the TOE.

5.1.1.4.4.1.1 FDP_ETC.1.1.1

The TSF shall enforce the [for phase 6 of the products Iife-cycle: PERS-AC_SFP; for phase 7 of the products Iife-cycle: AC_SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

5.1.1.4.4.2 *FDP_ETC.1.2*

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

5.1.1.4.5 FDP_ETC.2 Export of User Data with Security Attributes

Hierarchical to: no other components

Dependencies: - [FDP ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

5.1.1.4.5.1 *FDP_ETC.2.1*

The TSF shall enforce the [assignment: access control SFR(s) and/or information flow control SFR(s)] when exporting user data, controlled under the SFP(s), outside of the TOE.

5.1.1.4.5.1.1 FDP_ETC.2.1.1

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

5.1.1.4.5.2 *FDP_ETC.2.2*

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

5.1.1.4.5.3 *FDP_ETC.2.3*

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

5.1.1.4.5.4 *FDP_ETC.2.4*

The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: additional exportation control rules].

5.1.1.4.5.4.1 FDP_ETC.2.4.1

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

FDP_ITC Import from Outside

5.1.1.4.6 FDP_ITC.1 Import of User Data without Security Attributes

Hierarchical to: no other components

Dependencies: [FDP ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

[FDP MSA.3 Static attribute initialisation]

5.1.1.4.6.1 *FDP_ITC.1.1*

The TSF shall enforce the [assignment: access control SFR(s) and/or Information flow control SFR(s)] when importing user data, controlled under the SFP, from outside of the TOE.

5.1.1.4.6.1.1 FDP_ITC.1.1.1

The TSF shall enforce the [for phase 6 of the products Iife-cycle: PERS-AC_SFP; for phase 7 of the products Iife-cycle: AC_SFP] when importing user data, controlled under the SFP, from outside of the TOE.

5.1.1.4.6.2 *FDP_ITC.1.2*

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

5.1.1.4.6.3 *FDP_ITC.1.3*

The TSF shall enforce the following rules when importing user data controlled under the SFP from out side the TOE: [assignment: additional importation control rules].

5.1.1.4.6.3.1 FDP_ITC.1.3.1

The TSF shall enforce the following rules when importing user data controlled under the SFP from out side the TOE: [none].

FDP_RIP Residual Information Proteetion

5.1.1.4.7 FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: no other components

Dependencies: not applicable

5.1.1.4.7.1 FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocat/on of the resource to, deallocat/on of the resource from] the following objects: [assignment: list of objects].

5.1.1.4.7.1.1 FDP_RIP.1.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [cryptographic KEYs and PINs].

FDP_SDI Stored Data Integrity

5.1.1.4.8 FDP_SDI.2 Stored Data lntegrity Monitoring and Action

Hierarchical to: no other components

Dependencies: not applicable

5.1.1.4.8.1 FDP_SDI.2.1

The TSF shall monitor user data stored within the TSC for [assignment: /ntegr/tyerrors] on all objects, based on the following attributes: [assignment: user data attr/butes].

5.1.1.4.8.1.1 FDP_SDI.2.1.1

The TSF shall monitor user data stored within the TSC for [integrity error before access and processing] on all objects, based on the following attributes: [user data attributes].

5.1.1.4.8.2 FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [assignement: action to be taken].

5.1.1.4.8.2.1 FDP_SDI.2.2.1

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

5.1.1.5 FIA Identification and Authentication

This group is focused on requirements from TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, Chap. 4.2.3 [TACH_GST].

FIA_AFL Authentication Failures

5.1.1.5.1 FIA_AFL.1 Authentication Failure Handling

Hierarchical to: no other components

Dependencies: FIA_UAU.1 Timing of authentication

5.1.1.5.1.1 *FIA_AFL.1.1*

The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]“] unsuccessful authentication attempts occur related to [assignment: list ofauthentication events].

5.1.1.5.1.1.1 FIA_AFL.1.1.1

The TSF shall detect when [1] unsuccessful authentication attempt occurs related to [authentication of a card interface device].

5.1.1.5.1.1.2 FIA_AFL.1.1.2

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

5.1.1.5.1.2 *FIA_AFL.1.2*

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list ofactions].

5.1.1.5.1.2.1 FIA_AFL.1.2.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [warn the entity connected, assume the user as S.Non-VU (phase 7 of products lifecycle) resp. NON_PERSO_UNIT (phase 6 of products life-cycle)].

5.1.1.5.1.2.2 FIA_AFL.1.2.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [warn the entity connected, block the PIN check procedure such that any subsequent PIN check attempt will fail, be able to indicate to subsequent users the reason of the blocking (of the workshop card)].

FIA_ATD User Attribute Definition

5.1.1.5.2 FIA_ATD.1 User Attribute Definition

Hierarchical to: no other components

Dependencies: not applicable

5.1.1.5.2.1 *FIA_ATD.1.1*

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

5.1.1.5.2.1.1 FIA_ATD.1.1.1

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

[

phase 6 of the products Iife-cycle:

- **USER_GROUP**
  (PERSO_UNIT, NON_PERSO_UNIT)

phase 7 of the products Iife-cycle:

- **USER_GROUP**
  (S.VU, NON_S.Non-VU)
- **USER_ID**
  (VRN and Reg. MSC, where USER_ID is only known to USER_GROUP = S.VU)

]

FIA_UAU User Authentication

5.1.1.5.3 FIA_UAU.1 Timing of Authentication

Hierarchical to: no other components

Dependencies: . FIA_UID.1-1 Timing of identification

5.1.1.5.3.1 *FIA_UAU.1.1*

The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

5.1.1.5.3.1.1 FIA_UAU.1.1.1

The TSF shall allow

[

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

]

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

5.1.1.5.3.2 *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.

Refinements

UIA 301: Authentication of a S.VU 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 S.VU to ensure the identity of the card holder; it is not intended to protect workshop card content).

5.1.1.5.4 FIA_UAU.3 Unforgeable Authentication

Hierarchical to: no other components

Dependencies: none

5.1.1.5.4.1 *FIA_UAU.3.1*

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

5.1.1.5.4.1.1 FIA_UAU.3.1.1

The TSF shall [prevent] use of authentication data that has been forged by any user of the TSF.

5.1.1.5.4.2 *FIA_UAU.3.2*

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

5.1.1.5.4.2.1 FIA_UAU.3.2.1

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

5.1.1.5.5 FIA_UAU.4 Single-use Authentication Mechanisms

Hierarchical to: no other components

Dependencies: none

5.1.1.5.5.1 *FIA_UAU.4.1*

The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].

5.1.1.5.5.1.1 FIA_UAU.4.1.1

The TSF shall prevent reuse of authentication data related to [key based authentication mechanisms].

FIA_UID User Identification

5.1.1.5.6 FIA_UID.1 Timing of Identification

Hierarchical to: no other components

Dependencies: none

5.1.1.5.6.1 *FIA_UID.1.1*

The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is identified.

5.1.1.5.6.1.1 FIA_UID.1.1.1

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

5.1.1.5.6.2 *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.

FIA_USB User-Subject Binding

5.1.1.5.7 FIA_USB.1 User-Subject Binding

Hierarchical to: no other components

Dependencies: FIA_ATD.1 User attribute definition

5.1.1.5.7.1 *FIA_USB.1.1*

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].

5.1.1.5.7.1.1 FIA_USB.1.1.1

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

[

phase 6 of the products Iife-cycle:

- **USER_GROUP**
  (PERSO_UNIT, NON_PERSO_UNIT)

phase7 of the products Iife-cycle:

- **USER_GROUP**
  (S.VU, S.Non-VU)
- **USER_ID**
  (VRN and Reg. MSC, where USER ID is only known for USER_GROUP = S.VU)

]

5.1.1.5.7.2 *FIA_USB.1.2*

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initiaI association of attributes].

5.1.1.5.7.2.1 FIA_USB.1.2.1

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment in the framework of the TOEs access rule mechanism].

5.1.1.5.7.3 *FIA_USB.1.3*

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

5.1.1.5.7.3.1 FIA_USB.1.3.1

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [no change of user security attributes possible].

5.1.1.6 FMT Security Management

This group is focused on requirements from [PP9911].

FMT_MOF Management of Functions in TSF

5.1.1.6.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: no other components

Dependencies: FMT_SMF.1 Specification of management functions,
- FMT_SMR.1 Security roles

5.1.1.6.1.1 *FMT_MOF.1.1*

The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].

5.1.1.6.1.1.1 FMT_MOF.1.1.1

The TSF shall restrict the ability to [disable, modify the behavior of] the functions [TSF] to [No Roles].

FMT_MSA Management of Security Attributes

5.1.1.6.2 FMT_MSA.1 Management of Security Attributes

Hierarchical to: no other components

Dependencies: [FDP_ACC.1 Subset access control
or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

5.1.1.6.2.1 *FMT_MSA.1.1*

The TSF shall enforce the [assignment: access control SFR, information flow control SFR] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

5.1.1.6.2.1.1 FMT_MSA.1.1.1

The TSF shall enforce the [AC_SFP] to restrict the ability to [modify, delete] the security attributes [read and write access] to [assignment: No Roles].

5.1.1.6.3 FMT_MSA.2 Secure Security Attributes

Hierarchical to: no other components

Dependencies: ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow cintrol]
FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.1.1.6.3.1 *FMT_MSA.2.1*

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

5.1.1.6.4 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: no other components

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.1.6.4.1 *FMT_MSA.3.1*

The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

5.1.1.6.4.1.1 FMT_MSA.3.1.1

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

5.1.1.6.4.2 *FMT_MSA.3.2*

The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.

5.1.1.6.4.2.1 FMT_MSA.3.2.1

The TSF shall allow the [No Roles] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD Management of TSF Data

5.1.1.6.5 FMT_MTD.1 Management of TSF Data

Hierarchical to: no other components

Dependencies: none

5.1.1.6.5.1 FMT_MTD.1.1

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

5.1.1.6.5.1.1 FMT_MTD.1.1.1

The TSF shall restrict the ability [modify, delete, clear] the [any TSF data] to [No Roles].

FMT SMF Specification of Management Functions

5.1.1.6.6 FMT SMF.1 Specification of Management Functions

Hierarchical to: no other components

Dependencies: none

5.1.1.6.6.1 FMT SMF.1.1

The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

5.1.1.6.6.1.1 FMT SMF.1.1.1

The TSF shall be capable of performing the following management functions: [none].

FMT_SMR Security Management Roles

5.1.1.6.7 FMT_SMR.1 Security Roles

Hierarchical to: no other components

Dependencies: FIA_UID.1 Timing of identification

5.1.1.6.7.1 FMT_SMR.1.1

The TSF shall maintain the roles [assignment: the author/sed /dent/f/ed roles].

5.1.1.6.7.1.1 FMT_SMR.1.1.1

The TSF shall maintain the roles [S.VU and S.Non-VU].

5.1.1.6.7.2 *FMT_SMR.1.2*

The TSF shall be able to associate users with roles.

5.1.1.7 FPR Privacy

This group is focused on requirements from [PP9911].

FPR_UNO Unobservability

5.1.1.7.1 FPR_UNO.1 Unobservability

Hierarchical to: no other components

Dependencies: none

5.1.1.7.1.1 *FPR_UNO.1.1*

The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].

5.1.1.7.1.1.1 FPR_UNO.1.1.1

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

5.1.1.8 FPT Protection of the TSF

This group is focused on requirements from TachAn1b, Appendix 10 [TACH] and Tachograph Card Generic Security Target, Chap. 4.7.3, 4.7.4 [TACH_GST].

FPT_FLS Fail Secure

5.1.1.8.1 FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: no other components

Dependencies: none

5.1.1.8.1.1 *FPT_FLS.1.1*

The TSF shall preserve a secure state when the followin types of failures occur: [assignment: list of types of failures in the TSF].

5.1.1.8.1.1.1 FPT_FLS.1.1.1

The TSF shall preserve a secure state when the following types of failures occur: [

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

]

Refinements

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.

FPT_PHP Physical Protection

5.1.1.8.2 FPT_PHP.3 Resistance to Physical Attack

Hierarchical to: no other components

Dependencies: none

5.1.1.8.2.1 *FPT_PHP.3.1*

The TSF shall resist [assignment: physical tampering scenarios] to the [assignment: list of TSF devices /elements] by responding automatically such that the SFRs are always enforced.

5.1.1.8.2.1.1 FPT_PHP.3.1.1

The TSF shall resist [side channel attacks like SPA-attacks, DPA-attacks, DFA-attacks and timing attacks concerning all critical cryptographic operations] to the [TSF interfaces] by responding automatically such that the SFRs are always enforced.

FPT_TDC Inter-TSF TSF Data Consistency

5.1.1.8.3 FPT_TDC.1 Inter-TSF TSF Data Consistency

Hierarchical to: no other components

Dependencies: none

5.1.1.8.3.1 *FPT_TDC.1.1*

The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.

5.1.1.8.3.1.1 FPT_TDC.1.1.1

The TSF shall provide the capability to consistently interpret [session keys] when shared between the TSF and another trusted lT product.

5.1.1.8.3.2 FPT_TDC.1.2

The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.

5.1.1.8.3.2.1 FPT_TDC.1.2.1

The TSF shall use[rules for the interpretation of session keys within Secure Messaging: Tachograph Card specification [TACH] , Appendix 11, chap. 5,3.2, Appendix 2, chap. 3.6.2.2, 3.6.3.2] when interpreting the TSF data from another trusted IT product.

FPT_TST TSF Self Test

5.1.1.8.4 FPT_TST TSF Testing

Hierarchical to: no other components

Dependencies: none

5.1.1.8.4.1 FPT_TST.1.1

The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request ofthe authorised user, at the conditions [assignment: conditions under which selftest should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].

5.1.1.8.4.1.1 FPT_TST.1.1.1

The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation] to demonstrate the correct operation of [the TSF].

5.1.1.8.4.2 FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data].

5.1.1.8.4.2.1 FPT_TST.1.2.1

The TSF shall provide authorised users with the capability to verify the integrity of [TSF data].

5.1.1.8.4.3 FPT_TST.1.3

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

Refinements

RLB 301: The TOE‘s seif tests shall include the verification of the integrity of any

software code not stored in ROM.
RLB_302: Upon detection of a seif test error the TSF shall warn the entity connected.
RLB_303: After operating system testing is completed, all testing-specific commands and actions shall be disabled or removed. lt 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.
The term “periodically during normal operation“ is understood as follows: lt is assumed that the TOE performs at least one reset-operation each day, so that the self test at each initial start-up suffices the requirement of performing the self test periodically during normal operation.

5.1.1.9 FTP Trusted Path/Channels

FTP_ITC Inter-TSF Trusted Channel

5.1.1.9.1 FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: no other components

Dependencies: none

5.1.1.9.1.1 *FTP_ITC.1.1*

The TSF shall provide a communication channel between itseif and another trusted lT 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.

Refinements
DEX_301: The TOE shall verify the integrity and authenticity of data imported from a S.VU.
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 S.VU with associated security attributes, such that the S.VU will be able to verify the integrity and authenticity of data received.

5.1.1.9.1.2 *FTP_ITC.1.2*

The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

5.1.1.9.1.2.1 FTP_ITC.1.2.1

The TSF shall permit [another trusted lT product] to initiate communication via the trusted channel.

5.1.1.9.1.3 *FTP_ITC.1.3*

The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

5.1.1.9.1.3.1 FTP_ITC.1.3.1

The TSF shall initiate communication via the trusted channel for [activity data import from a remote trusted IT product].

5.1.2 Security Requirements for the Non-IT Environment

5.1.2.1 Req.Admin

The personalization of the initialized and tested tachograph card requires a secure environment. This is outside the scope of the TOE development.

The operational user guidance must address that and allow the personalization only after establishing a trusted communication. This procedure may be based on session keys or the external authentication with challenge-response.

5.1.2.2 Req.VU

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

5.2 Security Requirements 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 [STL] for O.Add-Functions and in the PP [PP0002] for the other objectives.

5.2.1 Rationale tables of security objectives and security requirements

Functional requirements for the TOE	OT.TAMPER_ES	OT.DIS_MECHANISM2	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication

Functional requirements for the TOE	OT.TAMPER_ES	OT.DIS_MECHANISM2	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication
FAU_SAA.1.1 FAU_SAA.1.2			X			
FCO_NRO.1.1 FCO_NRO.1.2 FCO_NRO.1.3						X
FCS_CKM.1.1 FCS_CKM.2.1 FCS_CKM.4.1						X
FCS_COP.1.1						X
FDP_ACC.2.1 FDP_ACC.2.2			X	X	X	
FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4			X	X	X	
FAU_DAU.1.1 FDP_DAU.1.2					X	
FDP_ETC.1.1 FDP_ETC.1.2					X	
FDP_ETC.2.1 FDP_ETC.2.2 FDP_ETC.2.3 FDP_ETC.2.4					X	X
FDP_ITC.1.1 FDP_ITC.1.2 FDP_ITC.1.3					X	
FDP_RIP.1.1					X	
FDP_SDI.2.1 FDP_SDI.2.2				X		
FIA_AFL.1.1 FIA_AFL.1.2					X	
FIA_ATD.1.1					X	
FIA_UAU.1.1 FIA_UAU.1.2					X	

Functional requirements for the TOE	OT.TAMPER_ES	OT.DIS_MECHANISM2	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communication
FIA_UAU.3.1 FIA_UAU.3.2					X	
FIA_UAU.4.1					X	
FIA_UID.1.1 FIA_UID.1.2					X	
FIA_USB.1.1 FIA_USB.1.2 FIA_USB.1.3					X	
FMT_MOF.1.1					X	
FMT_MSA.1.1 FMT_MSA.2.1 FMT_MSA.3.1 FMT_MSA.3.2					X	
FMT_MTD.1.1					X	
FMT SMF.1.1					X	
FMT_SMR.1.1 FMT_SMR.1.2					X	
FPR_UNO.1.1						X
FPT_FLS.1.1	X				X	
FPT_PHP.3.1	X	X	X	X		
FPT_TDC.1.1 FPT_TDC.1.2				X		
FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3	X	X	X			
FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3						X

Table 2 Functional requirements versus security objectives for the TOE

5.2.1.1 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_SFP (FDP_ACC.2 and FDP_ACF.1) prevents the data to be modified by any subject (IDENTIF_WRITE rule).

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

5.2.1.3 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. 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.

No security attributes can be modified (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MOF.1, FMT_SMF.1).

5.2.1.4 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 (FCS_COP.1, FCS_CKM.1, FCS_CKM.2 and FCS_CKM.4), 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.

5.2.1.5 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.

Tampering can also be detected through TOE self tests as required by FPT_TST.1.

5.2.1.6 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. 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.

5.2.1.7 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 the FSP and in the Administrator guidance. The process of personalization will be considered in ADO_IGS and ADO_DEL.

5.2.2 Security Requirements for the environment Rationale

Security objectives	Rationale
OE.Secure_Communication	Covered by the non-IT-environment security requirement Req.VU.
OE.Personalization	Covered by the non-IT-environment security requirement Req.Admin.

Table 3 Security objectives versus requirements for the environment rationale

5.2.3 Dependencies of Security Functional Requirements

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.

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

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

Table 4 Security functional requirements and their dependencies

5.3 Security assurance requirements

The security assurance requirements of this security target are those defined for the assurance level EAL4 in part 3 of Common Criteria version 3.1 [CC3].
The EAL is augmented with ADV_IMP.2, ALC_DVS.2 and AVA_VAN.5.

The following table lists the assurance components for the TOE:

Assurance Class	Assurance Components	Description
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification

Assurance Class	Assurance Components	Description
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support (ALC)	ALC_CMC.5	Advanced support
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment (AVA)	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 5 Security Assurance Requirements

The complete text for these requirements can be found in part 3 of Common Criteria version 3.1 [CC3].

5.3.1 Security Assurance Requirements rationale

The Security Assurance Requirements are chosen because [TACH_GST] section 7, p. 236, specifies that the CC 2.3 assurance level EAL 4 is augmented with ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4. With respect to CC 3.1 this will be EAL4 augmented with ADV_IMP.2 and AVA_VAN.5 as used in this document.

5.3.1.1 ADV_IMP.2 Complete mapping of the implementation representation of the TSF

Due to [JIL] the assurance level of the evaluation is EAL4 augmented with ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4. With respect to CC 3.1 this will be EAL4 augmented with ADV_IMP.2 and AVA_VAN.5.

For ADV_IMP.2 the developer makes the implementation representation for the entire TSF available and provides a mapping between the TOE design description and the **entire** implementation representation.

All the dependencies of the ADV_IMP.2 augmentation are satisfied by EAL4 except the dependency on ALC_CMC.5 that is therefore added in Table 5.

5.3.1.2 AVA_VAN.5 Advanced methodical vulnerability analysis

For secure application are loaded onto the TOE it must be highly resistant to the penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information and goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

All the dependencies of the AVA_VAN.5 augmentation are yet satisfied by EAL4.

5.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Atmel Chip [STL]. This statement is compliant to the requirements of [SUPP].

5.4.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functions	**Relevant**	**Not relevant**
SF1: Test Mode Entry		x
SF2: Protected Test Memory Access		x
SF3: Test Mode Disable		x
SF4: RNG	x	
SF5: Data Error Detection	x	
SF6: FireWall	x	
SF7: Event Audit	x	
SF8: Event Action	x	
SF9: Unobservability	x	
SF10: Cryptography	x	
SF11: Package Mode Entry		x

SF12: Test Memory Access in Package Mode		x

Table 6: **Classification of Platform-TSFs**

SF1, SF3 and SF3 are not relevant because it is not possible to move from User Mode to Test Mode [STL] and for this TOE the chip is always in User Mode.

SF11 and SF12 are not relevant for the Composite-ST because the Package Mode is not available for the Smartcard Embedded Software, but reserved for specific purposes fulfilled by the IC Dedicated Software.

All other listed TSFs of the Platform-ST are relevant for the Composite-ST.

5.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Atmel Microcontroller AT90SC24036RCU.
- Cryptographic support based on asymmetric and symmetric key algorithms (RSA and 3-DES) with 1024 bit asymmetric key length and 128 bit symmetric cryptographic key length.

The rationale of the Platform-ST has been used to identify the relevant SFRs, security objectives for the TOE (OTs), security objectives for the operational environment (OEs), threats and assumptions and have been used for the following analysis.

5.4.2.1 Assumptions

The assumptions from the Composite-ST and from the Platform-ST and their relation and mapping and their relevance for the Composite-ST are discussed in chapter 3.3.

There is **no conflict** between **assumptions** of this Composite-ST and the Platform-ST

5.4.2.2 Threats

The threats from the Composite-ST and from the Platform-ST and their relation and mapping and their relevance for the Composite-ST are discussed in chapter 3.4.

There is **no conflict** between **threats** of this Composite-ST and the Platform-ST.

5.4.2.3 Security objctives

The security objectives from the Composite-ST and from the Platform-ST and their relation and mapping and their relevance for the Composite-ST are discussed in chapter 4.

There is **no conflict** between **security objectives** of this Composite-ST and the Platform-ST.

5.4.2.4 Security requirements

5.4.2.4.1 Security Functional Requirements

This Composite-ST has the following platform related SFRs:

- FCS_CKM.1
- FCS_COP.1
- FPT_FLS.1
- FPT_PHP.3

The following Platform-SFRs could be mapped to Composite-SFRs:

- FCS_RND.1
- FCS_COP.1
- FRU_FLT.2
- FPT_FLS.1
- FPT_PHP.3

They will be mapped as seen in the following table.

Platform-ST		FCS_RND.1	FCS_COP.1	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3
Composite-ST	FCS_CKM.1	X				
	FCS_COP.1		X			
	FPT_FLS.1			X	X	X
	FPT_PHP.3			X	X	X

Table 7: **Mapping of SFRs**

FCS_CKM.1 requires sufficient quality of random numbers for the generation of 3-DES session keys, which matches to FCS_RND.1.

FCS_COP.1 requires cryptographic calculations which match to FCS_COP.1.

FPT_FLS.1 and FPT_PHP.3 of the composite ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the platform ST.

5.4.2.4.2 Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R3 augmented by ADV_IMP.2 and AVA_VAN.5.

The Platform-ST requires EAL 5 according to Common Criteria V2.3 augmented by: AVA_VLA.4, ALC_DVS.2, and AVA_MSU.3.

For a composite evaluation according to according to Common Criteria V3.1R2 based on a hardware platform certified according to Common Criteria V2.3 the EALs between the two versions of the Common Criteria have to be regarded as equivalent (i.e. EAL4 according to Common Criteria V2.3 has to be regarded as equivalent to EAL4 according to according to Common Criteria V3.1R2, EAL5 according to Common Criteria V2.3 has to be regarded as equivalent to EAL5 according to according to Common Criteria V3.1R2, etc.).

As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of the Composite-ST will match to the Platform-ST assurance requirements. But also the augmented parts of the Composite-ST match to the Platform-ST:

AVA_VAN.5 according to Common Criteria V3.1Rs selected for the composite TOE has to be regarded as equivalent to AVA_VLA.4 according to Common Criteria V2.3 as selected for the hardware platform.

5.4.3 Overall no contracdictions found

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

6 TOE summary specification

This chapter provides information about the mechanisms that the TOE uses to fulfil the SFRs.

6.1 TOE Mechanisms

6.1.1 M1: PIN

This mechanism provides for the workshop card a human user authentication by verifying the PIN code.

1. For the Workshop card, M1 detects each unsuccessful authentication attempt of the human user.
2. The Retry Counter for the PIN is decreased when an unsuccessful attempt is detected. After 5 consecutive unsuccessful authentication attempts M1 warns the entity connected, blocks the PIN check procedure so that any subsequent PIN check attempt will fail, and is able to indicate to subsequent users the reason of the blocking.

6.1.2 M2: Identification and Authentication

This mechanism provides for the identification of a technical user.

1. 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 cardholder identification data.
2. M2 stores appropriate keys and verifies appropriate certificates [[TACH], Appendix 11] to ensure that only security data are being used that have been distributed by the system.
3. M2 uses a mutual device authentication mechanism that is based on a Challenge-Response-Protocol, which uses random numbers during the authentication process. The challenge contains the random number and is send from one party to the other. The latter answers with a response that can be verified by the first. Authentication data are the complete set of data which are exchanged during the mutual device authentication process.

4. M2 detects each unsuccessful external device authentication attempt and then warns the entity connected and assumes the user S.Non-VU as current user.

6.1.3 M3: Secure Messaging

This mechanism provides for a secure communication channel between the TOE and the S.VU.

1. The data send via a communication channel between the TOE and the S.VU is encrypted with a randomly generated session key.
2. The communication channel is closed if an unrecognized message (malformed cryptogram) is detected. Each message is protected by a Retail-MAC (see [[TACH], Appendix 11, CSM_022 and section 5.3]).
3. The TOE verifies the integrity and authenticity of data imported from a S.VU.
4. Upon detection of an imported data integrity error the TOE warns the entity sending the data and does not use the data.
5. The cryptographic operations of the TOE are implemented so that observation does not yield any useful information about security data.
6. No sensitive data of the TOE are exported without security attributes.

6.1.4 M4: Digital Signature

This mechanism provides for generation and export of digital signatures.

1. The TOE generates a digital signature.
2. The TOE is able to export digital signatures (and corresponding certificates) as well as the related data.

6.1.5 M5: Access Control

This mechanism provides for access control of stored data objects.

1. M5 enforces the Security Policy AC_SFP for the subjects S.VU and S.Non-VU.
2. All security attributes are defined and implemented during the TOE developing phase. No security attributes can be modified in the usage phase.
3. The behaviour of M5 is once defined by the TOE developer and cannot be changed.

6.1.6 M6: Integrity

This mechanism provides for accuracy and audit.

1. M6 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).
2. Every file attribute stored in the file system is protected by integrity checks. If an integrity check of a file attribute fails, then reading, updating or writing of a file with corrupted file attributes is no more possible.
3. M6 warns the entity connected upon detection of a data integrity error of the user data stored within the TSC.

6.1.7 M7: Security

This mechanism provides for reliability.

1. At every start-up the executable code stored in EEPROM is checked for integrity.
2. An integrity check for some 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.
3. 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.
4. Commands associated exclusively with one life cycle phase can never be executed successfully during another phase.
5. The TOE does not allow analyzing, debugging or modifying TOE’s software in the field. Inputs from external sources will not be accepted as executable code.
6. The TOE preserves a secure state when the power supply is cut-off or the sytem braeks down or for other unexpected events.
7. 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.
8. The TOE ensures that the content of temporarily allocated resources is made unavailable after de-allocation by overwriting this content with zeros.

6.2 Fulfilment of the SFRs

The following table shows the mapping of the SFRs to mechanisms of the TOE.

	M1: PIN	M2: Identification and Authentication	M3: Secure Messaging	M4: Digital Signature	M5: Access Control	M6: Integrity	M7: Security
FAU_SAA.1.1 FAU_SAA.1.2						1,3	
FCO_NRO.1.1 FCO_NRO.1.2 FCO_NRO.1.3				1			
FCS_CKM.1.1 FCS_CKM.2.1 FCS_CKM.4.1			1, 2, 3, 4				
FCS_COP.1.1			1, 2. 3. 4	1			
FDP_ACC.2.1 FDP_ACC.2.2					1		
FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4					1		
FAU_DAU.1.1 FDP_DAU.1.2				1			
FDP_ETC.1.1 FDP_ETC.1.2				2			
FDP_ETC.2.1 FDP_ETC.2.2 FDP_ETC.2.3 FDP_ETC.2.4				2	3		
FDP_ITC.1.1 FDP_ITC.1.2 FDP_ITC.1.3			6				
FDP_RIP.1.1			1				
FDP_SDI.2.1 FDP_SDI.2.2						2, 3	
FIA_AFL.1.1 FIA_AFL.1.2	2	4					

	M1: PIN	M2: Identification and Authentication	M3: Secure Messaging	M4: Digital Signature	M5: Access Control	M6: Integrity	M7: Security
FIA_ATD.1.1		4					
FIA_UAU.1.1 FIA_UAU.1.2	1	1					
FIA_UAU.3.1 FIA_UAU.3.2		2					
FIA_UAU.4.1		4					
FIA_UID.1.1 FIA_UID.1.2		1, 2, 3, 4					
FIA_USB.1.1 FIA_USB.1.2 FIA_USB.1.3		4					
FMT_MOF.1.1					2		
FMT_MSA.1.1 FMT_MSA.2.1 FMT_MSA.3.1 FMT_MSA.3.2					2		
FMT_MTD.1.1					2		
FMT SMF.1.1					2		
FMT_SMR.1.1 FMT_SMR.1.2					1		
FPR_UNO.1.1			5				
FPT_FLS.1.1							6
FPT_PHP.3.1							7
FPT_TDC.1.1 FPT_TDC.1.2		4					
FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3							1,2,3,4,5,6,7,8
FTP_ITC.1.1			1				

	M1: PIN	M2: Identification and Authentication	M3: Secure Messaging	M4: Digital Signature	M5: Access Control	M6: Integrity	M7: Security
FTP_ITC.1.2 FTP_ITC.1.3							

Table 8 Mapping of SFRs to mechanisms of TOE

6.2.1 Justifications for the correspondence between functional requirements and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 6.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

7 Annexe A: Acronyms and References

7.1 Acronyms and Definitions

ACD	Activity data include cardholder activities data, events and faults data and control activity data
CA	Certification Authority
CC	Common Criteria Version
Card identification data	User data related to card identification
Cardholder identification data	User data related to cardholder identification
Control activity data	User data related to law enforcement controls
DTBS	Data to be Signed
CSM	Common Security Mechanism
EAL	Evaluation Assurance Level
EQT.SK	Equipment Secret Key (SCD)
EQT.PK	Equipment Public Key (SVD)
ES	Embedded Software
Events and faults data	User data related to events or faults
KMWC	Master Key Workshop Card
IDD	Identification data include card identification data and cardholder identification data
MSE	Manage Security Environment
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
RAD	Reference authentication data
SCA	Signature-Creation Application
SCD	Signature-Creation Data (EQT.SK)
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys).
Sensitive Data	Data stored by the tachograph card that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data
SMK	Secret Messaging Keys

SOF	Strength of Function
SVD	Signature-Verification Data (EQT.PK)
TSC	TSF Scope of Control
TOE	Target of Evaluation
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (when not used in the expression “user data”).
User Data	Sensitive data stored in the tachograph card, other than security data. User data include identification data and activity data
Reg.MSC	registering Member State code
VAD	Verification Authentication Data
VRN	Vehicle Registration Number
VU	Vehicle Unit
non-VU	Subject not identified as VU

7.2 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2006-09-001, Version 3.1, Revision 1, September 2006

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2007-09-002, Version 3.1, Revision 2, September 2007

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2007-09-003, Version 3.1, Revision 2, September 2007

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology ; CCMB-2007-09-004, Version 3.1, Revision 2, September 2007

[EU Ord] EU Ordinance 2002/C 126 E/01, adapting Council Regulation (EEC) No 3821/85 on recording equipment in road transport; proposal, 28.05.2002

[GUI Pre] Preparative procedures STARCOS 3.4 ID Tachograph C2, Version 1.1, 2010

[GUI Ope] Operational user guidance STARCOS 3.4 ID Tachograph C2, Version 1.1, 2010

[JIL] JIL Security Evaluation and Certification of Digital Tachographs. Version 1.12, June 2003

[PP0002] Smartcard IC Platform Protection Profile, BSI-PP-0002, Version 1.0, July 2001

[PP9911] Protection Profile – Smartcard Integrated Circuit with Embedded Software, DCSSI PP/9911, Version 2.0, June 1999

[RSA] RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003

[STL] Security Target Lite, ATMEL AT90SC24036RCU, EAL5+, April 2009

[SUPP] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-007-09-001.

[TACH] Annex 1B of Commission Regulation (EC) No. 1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, August 2002

[TACH_GST] Annex 1B of Commission Regulation (EC) No. 1360/2002, [TACH], Annex 10. Tachograph Card Generic Security Target, August 2002

End of Document