Giesecke & Devrient

Tachograph Certification

ASE Security Target Lite

STARCOS 3.6 ID Tachograph C1

Version 1.0

Released 18.08.2016

Giesecke & Devrient
Prinzregentenstr. 159
81677 Munich
PO Box 80 07 29

ID No.18.08.2016

Giesecke & Devrient
Prinzregentenstr. 159
81677 Munich
PO Box 80 07 29

Table of Contents

Tables

Figures

1 Introduction

Topics

1.1 ST Identification

Information about the ST

Title	Security Target Lite STARCOS 3.6 ID Tachograph C1
Reference	ASE_STARCOS 3.6 ID Tachograph C1
Version Number	Version 1.0 / Status 18.08.2016
Origin	Giesecke & Devrient GmbH
Author	MSRD34 / HSc
Compliant to	Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, BSI-CC-PP-0070 PP0070
Assurance Level	EAL4-augmented with the following assurance components: ATE_DPT.2 and AVA_VAN.5.
CC Version	3.1 (Revision 4)

TOE Reference

TOE	STARCOS 3.6 ID Tachograph C1
TOE documentation	[GUI Pre] : Preparative Guidance STARCOS 3.6 ID Tachograph C1 [GUI Ope] : Operative Guidance STARCOS 3.6 ID Tachograph C1 [AGD InitGuide] : Initialization Guide STARCOS 3.6 ID Tachograph C1

	[AGD PersoGuide] : Personalization Guide STARCOS 3.6 ID Tachograph C1
HW-Part of TOE	Infineon, M7892 B11 (Certificate: BSI-DSZ-CC-0782-V2-2015) STLite

1.2 ST Overview

In the following chapters the STARCOS 3.6 ID Tachograph C1 Card stands for the product.

STARCOS 3.6 ID Tachograph C1 Card contains the TOE consisting of the:

- STARCOS 3.6 ID operating system,
- Tachograph C1 application

and depends on the secure Infineon, M7892 B11 chip being certified according to CC EAL6+ STLite.

STARCOS 3.6 ID Tachograph C1 contains the IC and the Embedded SW ('Composite Evaluation').

1.3 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the TOE overview in sections 2.1 - 2.4 and the TOE description in section 2.5.

Section 3 contains the conformance claims for the TOE.

Section 4 contains the security problem definition.

Section 5 contains the security objectives for the TOE and its environment, including the security objectives rationale.

Section 6 contains the extended components definition.

Section 7 contains the security functional requirements, including the security requirements rationale.

Section 8 contains the TOE summary specification.

Section 9 provides a statement of compatibility between the composite TOE and the hardware TOE.

Section 10 contains references, abbreviations and a glossary.

1.4 Typographic Conventions

- This typeface is used to highlight assignments and selections for SFRs completed by the ST author.
- This typeface is used to highlight assignments and selections for SFRs defined in the PP.
- **This typeface** is used to highlight refinements for SFRs defined in the PP.
- The iteration operation for SFRs is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component

identifier. In order to trace elements belonging to a component, the same slash “/” with iteration indicator is used behind the elements of a component.

1.5 Change History

Version	Date	Changes	Responsible
1.0	18.08.2016	Final Version	HSc

1.6 Application Notes of the PP

When applicable the application notes of the PP are discussed in Notes.

2 TOE Overview and TOE Description

Topics

2.1 TOE definition and operational usage

The Target of Evaluation (TOE) is a Tachograph Smart Card in the sense of Annex I(B) [EC_AN], [EC_COR] intended to be used in the Digital Tachograph System which contains additionally Motion Sensors and Vehicle Units as recording equipment.

A Tachograph Card is a smart card which comprises:

- the circuitry of the chip incl. all IC Dedicated Software which is preloaded and security certified by the Chip Manufacturer (Infineon M7892 B11 chip; certificate: BSI-DSZ-CC-0782-V2-2015) being active in the operational phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (STARCOS 3.6 ID operating system),
- the tachograph application depending on the Tachograph Card type
  - — driver card application: the file structure is in accordance with [EC_AP2], section 4.1
  - — workshop card application: the file structure is in accordance with [EC_AP2], section 4.2
  - — control card application: the file structure is in accordance with [EC_AP2], section 4.3 or
  - — company card application: the file structure is in accordance with [EC_AP2], section 4.4

  and the associated guidance documentation.

In the initialisation the Tachograph Card type is determined. The TOE comprises four initialisation files which are used to create the file structure and the corresponding access rules of an application. Each initialisation file contains the instructions for one of the tachograph card applications.

The basic functions of the Tachograph Card are:

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

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

Concerning the write access, during the end-usage phase of a Tachograph Card life- cycle (phase 7 of life-cycle as described in section 2.3 of this ST), only Vehicle Units may write user data to the card.

The functional requirements for a Tachograph Card are specified in Annex I(B) body text [EC_AN], [EC_COR] and Appendix 2 [EC_AP2], the common security mechanisms are specified in Appendix 11 [EC_AP11].

The Generic Security Target, Appendix 10 [EC_AP10] requires that the TOE shall comply with PP/9806 [PP98] completely and with PP/9911 [PP99] as refined in [EC_AP10] (see in particular subsections EC_AP10 – EC_AP10 of [EC_AP10]).

For the underlying PP PP0070, the following approach is chosen in accordance to JIL [JIL], sec. 2.3 and Annex C: This ST covers all aspects and requirements defined in the PPs PP/9806 [PP98] and PP/9911 [PP99] but does not require CC conformance to these PPs. The coverage of [PP99] is reached through appropriate security functional and assurance requirements, all on the basis of the requirements and refinements outlined in [EC_AP10] , chap. 3 and 4.

The compliance requirement related to [PP98] is replaced by the necessity of a CC conformance claim to the Security IC Platform Protection Profile [PP0035]. The latter PP describes a comparable and acceptable set of (security) functionality for use as a basis for a Tachograph Card.

2.2 TOE major security features for operational use

The main security features of the TOE are as specified in [EC_AP10]:

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

Specifically the Tachograph Card protects

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

The main security features stated above are provided by the following major security services (please refer to [EC_AP10], chap. 4):

- User and Vehicle Unit identification and authentication,
- Access control to functions and stored data,
- Accountability of stored data,
- Audit of events and faults,
- Accuracy of stored data,
- Reliability of services,
- Data exchange with a Vehicle Unit and export of data to a non-Vehicle Unit,
- Cryptographic support for ‘identification and authentication’ and ‘data exchange’ as well as for key generation and distribution in corresponding case according to [EC_AP10], sec. 4.9.

All cryptographic mechanisms including algorithms and the length of corresponding keys are implemented exactly as required and defined in EU documents [EC_AP10] and [EC_AP10].

2.3 TOE Type

The TOE is a smart card, the Tachograph Card, which is configured and implemented as a driver card, workshop card, control card or company card in accordance with the specification documents Annex I(B) body text [EC_AN], [EC_COR], Appendix 2 [EC_AP2], Appendix 10 [EC_AP10] and Appendix 11 [EC_AP11]. In particular, this implies the conformance with the following standards:

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

As described in detail in the Security IC Platform Protection Profile [PP0035], the typical smart card product life-cycle is decomposed in 7 phases as follows:

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

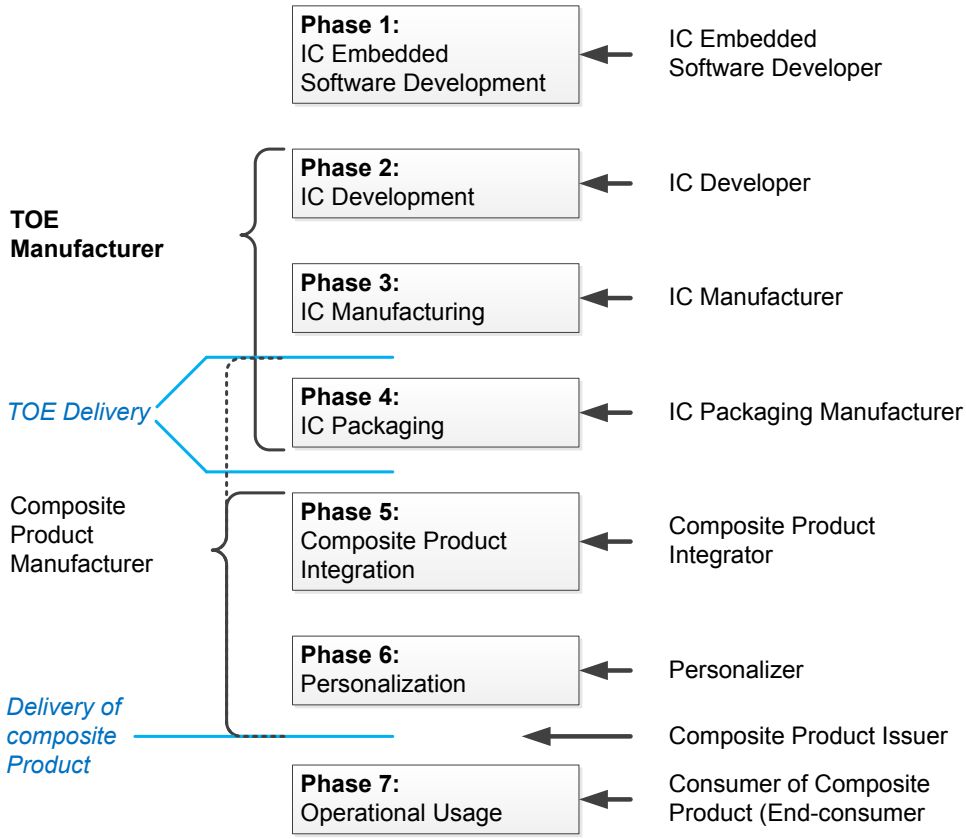


Figure 1: Definition of “TOE Delivery” and responsible parties [PP0035]

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

- TOE development (including the development as well as the production of the TOE)
- TOE delivery
- TOE operational use

For the evaluation of the Tachograph card the phases 1 up to 5 as defined in [PP0035][1] are part of the TOE development in the sense of the CC. The phase 7 - end-usage of the TOE is explicitly in focus of the current ST and is part of the operational use in the sense of the CC.

As defined in [PP0070] phases 5 and 6 may be part of one of these CC phases or may be split between them depending on the specific model used by the TOE Manufacturer[2]. For the TOE the following specific model is applied:

The TOE delivery takes place after Phase 5a so that the evaluation process is limited to Phases 1 to 5a (see below).

All the executable software in the TOE is included in the evaluation.

The data structures and access rights, in particular the initialisation files and their creation and handling are covered by the evaluation guidance AGD InitGuide.

- **Phase 5a** – Loading the executable software "O/S = Operating System" is included in the evaluation.
- **Phase 5b** – Loading the initialisation files (tables) is **not** included in the evaluation

2.4 Required non-TOE hardware/software/firmware

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

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

1 *PP0035 does not distinguish between Phases 5a/b because at the time of its creation, the cards were ROM-based and hence the process did not distinguish between O/S loading (Phase 5a) and Initialization (Phase 5b)*

2 *Therefore in the remaining text of this ST the TOE Manufacturer will be the subject responsible for everything up to TOE delivery.*

2.5 TOE Description

2.5.1 Physical scope of TOE

The TOE consists of the following parts:

- the hardware platform Infineon, M7892 B11 (Certificate: BSI-DSZ-CC-0782-V2-2015) with the following configurations according [STLite]:
  - Flash: up to 404 kByte
  - ROM: not available
  - RAM for the user: 1-8 kByte
  - SCP: accessible
  - Crypto2304T: accessible
  - Interfaces: ISO/IEC 7816
- The STARCOS 3.6 ID OS platform
- The Tachograph C1 application
- The accompanying guidance documentation which consists of the preparative procedures [GUI Pre] and the operational user guidance documents[AGD InitGuide], [AGD PersoGuide] and [Gui OPE].

2.5.2 TOE Reference

Infineon provides the Chip as configurable platform. The Infineon platform specification is "M7892 B11".

The chip platform will be configured customer specifically. The configuration specifies

- Chip Functions
- Persistent Storage Size

The configuration is specified by the 6- byte Short ROM code ("SRC"). The short ROM code is generated by Infineon and is used as unique identifier for all chips delivered upon a specific order of a specific customer.

In addition to the Short ROM code an SP-Number uniquely identifies the particular chip.

Note: The configuration is performed by Infineon during chip production and cannot be changed by G&D.

2.5.2.1 Sales Code

The TOE is ordered in the sales-code configuration SLE78CFX2400P. The sales code specifies the available features. Features not available by the definition of the sales code cannot be configured through any other configuration.

- **S**LE = S: Solitary Digital Circuits
- S**L**E = L: Free selectable
- SL**E** = E: Temperature Range (-25°C to +85°C)
- **C**FX = C: Card with Contacts acc. ISO/IEC 7816 Part 2 and 3. (CL would be the contactless solution)
- C**F**X = F: Solid Flash™
- CF**X** = X: Crypto Coprocessor: Crypto@2304T
- **240**0 = NVM Size in kbytes = 240KB
- 240**0** = Ordinal Number = 0
- **P** = Product Family "Plus"

The ordered sales code SLE78CFX2400P excludes the contactless configuration which therefore is not technically available in the TOE.

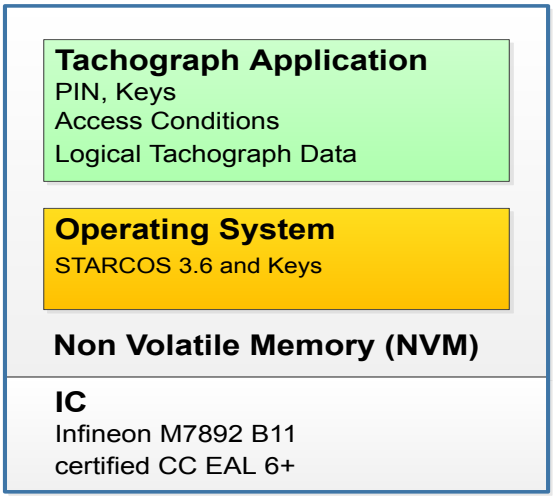
2.5.2.2 Short ROM Code (SRC)

The Short ROM Code specifies the particular configuration of the features available through the Sales Code. It does not allow adding features that are already excluded by the Sales Code.

2.5.3 Logical scope of TOE

The TOE provides the following services:

- 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.



3 Conformance Claims

Topics

3.1 CC conformance claims

This ST claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, version 3.1, revision 4, CCMB-2012-09-001 [CC1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, version 3.1, revision 4, CCMB-2012-09-002 [CC2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, version 3.1, revision 4, CCMB-2012-09-003 [CC3].

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

has to be taken into account.

3.2 Conformance claim to a PP

This ST claims strict conformance to the Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, BSI-CC-PP-0070 [PP0070].

3.3 Conformance claim to a package

This ST claims conformance to the following security requirements package:

- Assurance package E3hCC31_AP as defined in the PP [PP0070], sec. 6.2

This assurance package is specified in dependence of JIL [JIL] , Annex A, which defines a CC assurance package called E3hAP. The latter assurance package is intended to reach an equivalent assurance level in the framework of a CC certification as reached with an ITSEC E3 high certification (as required in [EC_AP10]) and maps adequately (i.e. in particular in conjunction with the Digital Tachograph System) all assurance requirements from ITSEC E3 high into comparable CC requirements.

Here, the assurance package E3hCC31_AP does not define a new security assurance level, but only directly switches the requirements in E3hAP, which are related to the older CC version 2.1 to the current version 3.1 of the CC CC3).

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see sec. 6.2 of the PP [PP0070]).

3.4 Conformance Claim Rationale

This security target is strict conformant to the claimed PP [PP0070].

The TOE type described in Chapter 2 is consistent with the TOE type described in the PP [PP0070] chapter 1.2.

4 Security Problem Definition

Chapter 3 of the PP [PP0070] is adopted without changes.

5 Security Objectives

Chapter 4 of the PP [PP0070] is adopted without changes.

6 Extended Components Definition

Chapter 5 of the PP [PP0070] is adopted without changes.

7 Security Requirements

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [CC1] of the CC. Each of these operations is used in this ST.

For the typographic conventions used for these operations see Chapter 1.4.

Topics

7.1 Security Functional Requirements for the TOE

The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in chap. 4 of the ITSEC based Tachograph Card GST in [EC_AP10].

Each of the SFRs includes in curly braces {…} a reference to the relevant SEFs (reference number or chapter of [EC_AP10] resp. other documents).

This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from [EC_AP10]. The main advantage of this approach is avoiding redundancy, and, more important, any ambiguity.

The complete coverage of the security enforcing functions required in [EC_AP10] is documented in the PP Annex A, chap. 9.

7.1.1 Security Function Policy

The **Security Function Policy Access Control (AC_SFP)** for Tachograph Cards in the end-usage phase based on the Tachograph Cards Specification [EC_AP2], sec. 3 and 4, GST [EC_AP10], sec. 4.3.1 and 4.3.2 as well as JIL [JIL], sec. 2.6 is defined as follows:

The SFP AC_SFP is only relevant for the end-usage phase of the Tachograph Card, i.e. after the personalisation of the card has been completed.

Subjects:

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

Security attributes for subjects:

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

Objects:

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

Security attributes for objects:

- Access Rules based on defined Access Conditions (see below) for:
  - user data
  - security data
  - identification data of the TOE
  - identification data of the TOE's personalisation

  Digital signature for each data to be signed

Operations:

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

Access Rules

The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object.

The possible commands are described in the Tachograph Card specification [EC_AP2], sec. 3.6.

Following Access Conditions are defined in the Tachograph Card specification [EC_AP2], sec. 3.3.:

- **NEV (Never)** - The command can never be executed.
- **ALW (Always)** - The command can be executed without restrictions.
- **AUT (Key based authentication)** - The command can be executed only if the preceding external authentication (done by the command External Authenticate) has been conducted successfully.
- **PRO SM (Secure Messaging providing data integrity and authenticity for command resp. response)** - The command can be executed and the corresponding response can be accepted only if the command/response is secured with a cryptographic checksum using Secure Messaging as defined in the Tachograph Card Specification [EC_AP2], sec. 3.6 and Tachograph Common Security Mechanisms [EC_AP11], sec. 5.
- **AUT and PRO SM** (combined, see description above)

For each type of Tachograph Card the Access Rules (which make use of the Access Conditions described above) for the different objects are implemented according to the requirements in the Tachograph Card Specification [EC_AP2], sec. 4 and GST [EC_AP10], sec. 4.3. These access rules cover in particular the rules for the export and import of data.

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

7.1.2 Class FAU Security AuditClass

FAU_SAA Security audit analysis

FAU_SAA.1 Potential Violation Analysis {chapter 4.5 of [EC_AP10]}

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to **detect failure events as cardholder authentication failures, self test errors, stored data integrity errors and activity data input integrity errors**[3], to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

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

- a) Accumulation or combination of
  - — cardholder authentication failure,
  - — self test error,
  - — stored data integrity error,
  - — activity data input integrity error[4]

  known to indicate a potential security violation;
- b) none[5].

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

7.1.3 Class FCO Communication

FCO_NRO Non-Repudiation of Origin

FCO_NRO.1 Selective proof of origin {chapter 4.8.2 of [EC_AP10], DEX_304, DEX_305, DEX_306}

Hierarchical to: No other components.

3 *[refinement]*
4 *[assignment: subset of defined auditable events]*
5 *[assignment: any other rules]*

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted data to be downloaded to external media[6] at the request of the recipient[7].

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.2 The TSF shall be able to relate the card holder identity by means of digital signature[8] of the originator of the information, and the hash value over the data to be downloaded to external media[9] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to recipient[10] given in accordance with the Tachograph Common Security Mechanisms [EC_AP11] , sec. 6, CSM_035[11].

7.1.4 Class FCS Cryptographic support

FCS_CKM Cryptographic key management

FCS_CKM.1 Cryptographic key generation {chapter 4.9 of [EC_AP10], CSP_301}

Hierarchical to: No other components.

Dependencies:

- FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation
- FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm cryptographic two-keys TDES derivation algorithms[12] and specified cryptographic key sizes 128 bits with 112 effective bits[13] that meet the following: Tachograph Common Security Mechanisms [EC_AP11] , sec. 3, CSM_012, CSM_013, CSM_015, CSM_020 [assignment: list of standards].

FCS_CKM.2 Cryptographic key distribution {chapter 4.9 of [EC_AP10], CSP_302}

Hierarchical to: No other components.

Dependencies:

- FDP_ITC.1 Import of user data without security attributes, **or**
- FDP_ITC.2 Import of user data with security attributes, **or**
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction

6 *[assignment: list of information types]*
7 *[selection: originator, recipient, [assignment: list of third parties]]*
8 *[assignment: list of attributes]*
9 *[assignment: list of information fields]*
10 *[selection: originator, recipient, [assignment: list of third parties]]*
11 *[assignment: limitations on the evidence of origin]*
12 *[assignment: cryptographic key generation algorithm]*
13 *[assignment: cryptographic key sizes]*

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method TDES session key agreement by an internal-external authentication mechanism[14] that meets the following: Tachograph Common Security Mechanisms [EC_AP11] , sec. 3, CSM_012, CSM_013, CSM_015, CSM_020 and Tachograph Card Specification[EC_AP2], sec. 3.6[15].

FCS_CKM.4 Cryptographic key destruction {chapter 4.9 of [EC_AP10], CSP_301}

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.4.1 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[16] that meets the following: Tachograph Common Security Mechanisms [EC_AP11] , sec. 3, CSM_013 and Tachograph Card Specification [EC_AP2], sec. 3.6[17].

Note: As required in sec. 4.9 of [EC_AP10] session keys shall have a limited (not more than 240) number of possible use. This is considered by FCS_CKM.4.1 and fulfils the requirement CSM_013 in [EC_AP11] .

FCS_COP Cryptographic operation

FCS_COP. 1/RSA Cryptographic operation {CSM_003 and further chapters of [EC_AP11] }

Hierarchical to: No other components.

Dependencies:

- FDP_ITC.1 Import of user data without security attributes, **or**
- FDP_ITC.2 Import of user data with security attributes, **or**
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction

FCS_COP. 1.1/RSA The TSF shall perform the cryptographic operations (encryption, decryption, signature creation and signature verification as well as certificate verification for the authentication between the Tachograph Card and the Vehicle Unit and signing for downloading to external media)[18] in accordance with a specified cryptographic algorithm RSA[19] and cryptographic key sizes of 1024 bits[20] that meet the following: Tachograph Common Security Mechanisms [EC_AP11], sec. 2-6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_016, CSM_017, CSM_018, CSM_019, CSM_020, CSM_033, CSM_034, CSM_035 and Tachograph Card Specification [EC_AP2], sec. 3[21].

14 *[assignment: cryptographic key distribution method]*
15 *[assignment: list of standards]*
16 *[assignment: cryptographic key destruction method]*
17 *[assignment: list of standards]*
18 *[assignment: list of cryptographic operations]*
19 *[assignment: cryptographic algorithm]*
20 *[assignment: cryptographic key sizes]*
21 *[assignment: list of standards]*

FCS_COP.1/ TDES	Cryptographic operation {CSM_002 and further chapters of [EC_AP11] } **Hierarchical to**: No other components. **Dependencies**: • FDP_ITC.1 Import of user data without security attributes, **or** • FDP_ITC.2 Import of user data with security attributes, **or** • FCS_CKM.1 Cryptographic key generation • FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ TDES	The TSF shall perform the cryptographic operations (encryption and decryption respective Retail-MAC generation and verification) concerning symmetric cryptography[22] in accordance with a specified cryptographic algorithm TDES[23] and cryptographic key sizes of 128 bits with 112 effective bits[24] that meet the following: Tachograph Common Security Mechanisms [EC_AP11] , sec. 2, CSM_005, sec. 3, CSM_015, sec. 5, CSM_021-CSM_031 and Tachograph Card Specification [EC_AP2], sec. 3[25].

7.1.5 Class FDP User Data Protection

FDP_ACC Access control policy

FDP_ACC.2	Complete access control {chapter 4.3.1, ACT_301, ACT_302, chapter 4.4 of [EC_AP10] as well as JIL [JIL], sec. 2.6} **Hierarchical to**: FDP_ACC.1 Subset access control **Dependencies**: • FDP_ACF.1: Security attribute based access control • FDP_ACC.2.1: The TSF shall enforce the AC_SFP[26] on subjects: — S.VU (in the sense of the Tachograph Card specification)

22 *[assignment: list of cryptographic operations]*
23 *[assignment: cryptographic algorithm]*
24 *[assignment: cryptographic key sizes]*
25 *[assignment: list of standards]*
26 *[assignment: access control SFP]*

S.Non-VU (other card interface devices)

- objects:
  - user data:
    - identification data
    - activity data
  - security data:
    - cards´s private signature key
    - public keys
    - session keys
    - PIN (for workshop card)
  - TOE software code
  - TOE file system
  - identification data of the TOE
  - identification data of the TOE`s personalisation[27] and all operations among subjects and objects covered by the SFP.

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

FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control {chapters 3.3 and 4 of [EC_AP2], chapter 4.3.2, ACT_301, ACT_302, chapter 4.4 of [EC_AP10] as well as JIL [JIL], sec. 2.6}

Hierarchical to: No other components.

27 *[assignment: list of subjects and objects]*

Dependencies:

- FDP_ACC.1: Subset access control
- FMT_MSA.3: Static attribute initialisation
- FDP_ACF.1.1: The TSF shall enforce the AC_SFP[28] to objects based on the following:
- subjects:
  - S.VU (in the sense of the Tachograph Card specification)
  - S.Non-VU (other card interface devices)
- objects:
  - user data:
    - identification data
    - activity data
  - security data:
    - cards´s private signature key
    - public keys
    - session keys
    - PIN (for workshop card)
  - TOE software code
  - TOE file system
  - identification data of the TOE
  - identification data of the TOE`s personalisation
  - security attributes for subjects:
    - USER_GROUP
    - USER_ID
  - security attributes for objects:
    - Access Rules[29].

[28] *[assignment: access control SFP]*
[29] *[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]*

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

- GENERAL_READ:
  - driver card, workshop card: user data may be read from the TOE by any user
  - control card, company card: user data may be read from the TOE by any user, except cardholder identification data which may be read by S.VU only;
- IDENTIF_WRITE: all card types: identification data may only be written once and before the end of Personalisation; no user may write or modify identification data during end-usage phase of card's life-cycle;
- ACTIVITY_WRITE: all card types: activity data may be written to the TOE by S.VU only;
- SOFT_UPGRADE: all card types: no user may upgrade TOE's software;
- FILE_STRUCTURE: all card types: files structure and access conditions shall be created before the Personalisation is completed and then locked from any future modification or deletion by any user
- IDENTIF_TOE_READ: all card types: identification data of the TOE and identification data of the TOE's personalisation may be read from the TOE by any user;
- IDENTIF_TOE_WRITE: all card types: identification data of the TOE may only be written once and before the Personalisation; no user may write or modify these identification data during the Personalisation;
- IDENTIF_ TOE_ PERS_WRITE: all card types: identification data of the TOE's personalisation may only be written once and within the Personalisation ; no user may write or modify these identification data during end-usage phase of card's life-cycle[30].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[31].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[32].

FDP_DAU Data authentication

FDP_DAU.1 Basic Data Authentication {chapter 4.6.2 of [EC_AP10]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of activity data[33].

30 *[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*
31 *[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]*
32 *[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]*
33 *[assignment: list of objects or information types]*

FDP_DAU.1.2 The TSF shall provide S.VU and S.Non-VU[34] with the ability to verify evidence of the validity of the indicated information.

FDP_ETC Export from the TOE

FDP_ETC.1 Export of user data without security attributes {chapter 4.3.2 of [EC_AP10]}

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or**
- FDP_IFC.1 Subset information flow control
- FDP_ETC.1.1 The TSF shall enforce the AC_SFP[35] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

FDP_ETC.2 Export of user data with security attributes {DEX_304, DEX_305, DEX_306, chapter 4.8 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or**
- FDP_IFC.1 Subset information flow control

  FDP_ETC.2.1 The TSF shall enforce the AC_SFP[36] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: none[37].

FDP_ITC Import from outside of the TOE

FDP_ITC.1 Import of user data without security attributes {chapters 4.3.1 and 4.3.2 RLB_305, chapter 4.7.2 of [EC_AP10]}

Hierarchical to: No other components.

34 *[assignment: list of subjects]*
35 *[assignment: access control SFP(s) and/or information flow control SFP(s)]*
36 *[assignment: access control SFP(s) and/or information flow control SFP(s)]*
37 *[assignment: additional exportation control rules]*

Dependencies:

- FDP_ACC.1 Subset access control, **or**
- FDP_IFC.1 Subset information flow control
- FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the AC_SFP[38] when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[39].

FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {RLB_306, RLB_307, chapter 4.7} of [EC_AP10]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[40] the following objects: the card's private key and PINs[41].

FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action {chapter 4.6.1 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors before access and processing [42] on all objects, based on the following attributes: user data value[43].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall warn the entity connected[44].

38 *[assignment: access control SFP(s) and/or information flow control SFP(s)]*
39 *[assignment: additional importation control rules]*
40 *[selection: allocation of the resource to, deallocation of the resource from]*
41 *[assignment: list of objects]*
42 *[assignment: integrity errors]*
43 *[assignment: user data attributes]*
44 *[assignment: action to be taken]*

7.1.6 Class FIA Identification and Authentication

FIA_AFL Authentication failures

FIA_AFL.1/C Authentication failure handling {UIA_301, chapter 4.2.2 of [EC_AP10], chapter 4.2.3}

Hierarchical to: No other components.

Dependencies:

- FIA_UAU.1 Timing of authentication
- FIA_AFL.1.1/C The TSF shall detect when one[45] unsuccessful authentication attempts occur related to authentication of a card interface device[46].

FIA_AFL.1.2/C When the defined number of unsuccessful authentication attempts has been met or surpassed[47], the TSF shall warn the entity connected; assume the user as S.Non-VU[48].

FIA_AFL.1/WSC Authentication failure handling {UIA_302, chapter 4.2.2 of [EC_AP10], chapter 4.2.3 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies:

- FIA_UAU.1 Timing of authentication
- FIA_AFL.1.1/WSC The TSF shall detect when five[49] unsuccessful authentication attempts occur related to PIN verification of Workshop Card[50].
- FIA_AFL.1.2/WSC When the defined number of unsuccessful authentication attempts has been met or surpassed[51], 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[52].

FIA_ATD User attribute definition

FIA_ATD.1 User attribute definition tchapter 4.2.1 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

45 *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]*
46 *[assignment: list of authentication events]*
47 *[selection: met, surpassed]*
48 *[assignment: list of actions]*
49 *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]*
50 *[assignment: list of authentication events]*
51 *[selection: met, surpassed]*
52 *[assignment: list of actions]*

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

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)
- USER_ID (VRN and Registering MSC for subject S.VU)[53].

FIA_UAU User Authentication

FIA_UAU.1 Timing of authentication {UIA_301, chapter 4.2.2 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

- **driver card, workshop card**: export of user data with security attributes (card data download function),
- **control card, company card**: export of user data without security attributes except export of cardholder identification data[54] on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.3 Unforgeable authentication {UIA_301, chapter 4.2.2 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.3.1 The TSF shall prevent[55] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall prevent[56] use of authentication data that has been copied from any other user of the TSF.

FIA_UAU 4 Single-use authentication mechanisms {UIA_301, chapter 4.2.2 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to key based authentication mechanisms[57].

FIA_UID User identification

FIA_UID.1 Timing of identification {chapter 4.2.1 of [EC_AP10] }

53 *[assignment: list of security attributes]*
54 *[assignment: list of TSF mediated actions]*
55 *[selection: detect, prevent]*
56 *[selection: detect, prevent]*
57 *[assignment: identified authentication mechanism(s)]*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow none of the TSF-mediated actions[58] on behalf of the user to be performed before the user is identified.

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

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

FIA_USB User-subject binding

FIA_USB.1 User-subject binding {chapters 4.3.1, 4.7.2 (RLB_304, RLB_305) of [EC_AP10] }

Hierarchical to: No other components.

Dependencies:

- FIA_ATD.1 User attribute definition
- FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:
  - USER_GROUP (VEHICLE_UNIT for S.VU, NON_VEHICLE_UNIT for S.Non-VU)
  - USER_ID (VRN and Registering MSC for subject S.VU)[59].

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: in the framework of the TOEs access rule mechanism[60].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: no change of user security attributes possible[61].

7.1.7 Class FPR Privacy

FPR_UNO Unobservability

FPR_UNO.1 Unobservability {RLB_304, chapter 4.7.2 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

58 *[assignment: list of TSF-mediated actions]*
59 *[assignment: list of user security attributes]*
60 *[assignment: rules for the initial association of attributes]*
61 *[assignment: rules for the changing of attributes]*

FPR_UNO.1.1 The TSF shall ensure that Attackers[62] are unable to observe the operation with involved authentication and/or cryptographic operations[63] on security and activity data[64] by any user[65].

7.1.8 Class FPT Protection of the TSF

FPT_EMS TOE Emanation

FPT_EMS.1 TOE Emanation {RLB_304, chapter 4.7.2 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit information about IC power consumption, electromagnetic radiation and command execution time[66]in excess of non useful information[67] enabling access to private key(s) and session keys[68] and the EF Sensor_Installation_Data of the workshop card[69].

FPT_EMS.1.2 The TSF shall ensure any users[70] are unable to use the following interface smart card circuit contacts[71] to gain access to private key(s) and session keys[72] and the EF Sensor_Installation_Data of the workshop card[73].

Note: The ST writer has performed the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE.

Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card.

FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state {RLB_306, chapter 4.7.3, RLB_307, chapter 4.7.4 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

62 *[assignment: list of users and/or subjects]*
63 *[assignment: list of operations]*
64 *[assignment: list of objects]*
65 *[assignment: list of protected users and/or subjects]*
66 *[assignment: types of emissions]*
67 *[assignment: specified limits]*
68 *[assignment: list of types of TSF data]*
69 *[assignment: list of types of user data]*
70 *[assignment: type of users]*
71 *[assignment: type of connection]*
72 *[assignment: list of types of TSF data]*
73 *[assignment: list of types of user data]*

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

- reset
- power supply cut-off
- power supply variations
- unexpected abortion of the TSF execution due to external or internal events (esp. break of a transaction before completion)[74].

FPT_PHP TSF physical protection

FPT_PHP.3 Resistance to physical attack {RLB_304, chapter 4.7.3 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[75] to the all TOE components implementing the TSF[76] by responding automatically such that the SFRs are always enforced.

Note: The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements.

Therefore, permanent protection against these attacks is implemented ensuring that the TSF security could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1 Inter-TSF basic TSF data consistency {DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [EC_AP10] , chapter 5.3 of [EC_AP11]}

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TDC.1.1 The TSF shall provide the capability to consistently interprete key material (session keys and certificates)[77] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use rules for the interpretation of key material (session keys and certificates) as defined in Tachograph Common Security Mechanisms [EC_AP11] , and Tachograph Card Specification [EC_AP2], sec. 3.6[78] when interpreting the TSF data from another trusted IT product.

74 *[assignment: list of types of failures in the TSF]*
75 *[assignment: physical tampering scenarios]*
76 *[assignment: list of TSF devices/elements]*
77 *[assignment: list of TSF data types]*
78 *[assignment: list of interpretation rules to be applied by the TSF]*

FPT_TST TSF self test

FPT_TST.1 TSF testing {RLB_301, RLB_302, RLB_303, chapter 4.7.1 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation[79] to demonstrate the correct operation of the TSF[80].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[81].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of the TSF[82].

7.1.9 Class FTP Trusted path/channels

FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel {DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [EC_AP10] }

Hierarchical to: No other components.

Dependencies: No dependencies

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

FTP_ITC.1.2 The TSF shall permit another trusted IT product[83] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for activity data import from a remote trusted product[84].

79 *[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]*
80 *[selection: [assignment: parts of TSF]]*
81 *[selection: [assignment: parts of TSF data]]*
82 *[selection: [assignment: parts of TSF]]*
83 *[selection: the TSF, another trusted IT product]*
84 *[assignment: list of functions for which a trusted channel is required]*

7.2 Security Assurance Requirements

Chapter 6.2 of the PP [PP0070] is adopted without any changes.

7.3 Security Requirements Rationale

Chapter 6.3 of the PP [PP0070] is adopted without changes.

8 TOE summary specification

Topics

8.1 TOE Security functions

8.1.1 SF_PIN

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

1. For the Workshop card, SF_PIN 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 SF_PIN 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.

8.1.2 SF_Identification and Authentication

This security function provides for the identification of a technical user.

1. If the user is not identified no actions are possible for this user. After start-up of the TOE the user is identified as S.Non-VU. Before authentication has taken place, the following actions are allowed for this user:
   - 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. SF_Identification and Authentication stores appropriate keys and verifies appropriate certificates, [EC_AP11], to ensure that only security data are being used that have been distributed by the system. For the certificate verification the TOE verifies an RSA signature and interpretes the content of the certificate.
3. SF_Identification and Authentication 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 sent from one party to the other.

The latter answers with an RSA signed and encrypted response that can be decrypted and the signature verified by the first. Authentication data are the complete set of data which are exchanged during the mutual device authentication process. This protocol prevents the re-use of authentication data from a session with the same card, the forging of authentication data as well as using authentication data from another card.

After a successful authentication the TOE assumes the S.VU as current user and stores a user ID associated to S.VU.

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

8.1.3 SF_Secure Messaging

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

1. The data sent via a communication channel between the TOE and the S.VU is encrypted / MACed with randomly generated session keys.
2. The communication channel is closed if an unrecognized message (malformed cryptogram) is detected. Each message is protected by a Retail-MAC (see [EC_AP11], 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.

8.1.4 SF_Digital Signature

This security function provides for generation and export of digital signatures.

1. The TOE generates a digital signature as evidence of the validity of activity data. For that purpose the activity data is hashed and then signed with the TOE's private RSA key.
2. The TOE is able to export digital signatures (and corresponding certificates) as well as the related data.
3. The TOE verifies a digital signature. For that purpose an RSA public key can be imported by means of a certificate, a hash value and the corresponding signature can be imported.

   The TOE makes use of this public key to check the signature and verifies that the hash value from the signature and the imported hash value match. The certificate content is interpreted by the TOE, i.e. the TOE checks the syntax as well as the values of the certificate's data fields.

8.1.5 SF_Access Control

This security function provides for access control of stored data objects.

1. SF_Access Control enforces the Security Policy AC_SFP for the subjects S.VU and S.Non-VU.
2. 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 SF_Access Control is defined by the TOE developer and cannot be changed.

8.1.6 SF_Integrity

This security function provides for integrity and audit.

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

8.1.7 SF_Security

This security function provides for reliability.

1. At every start-up the executable code stored in Non Volatile Memory is checked for integrity. If this check is not successful the TOE preserves a secure state, i.e. is unresponsive. At every start-up and periodically during the operation the TOE performs self tests in order to determine the correct operation of the software and the underlying hardware. If a self test is not successful the TOE preserves a secure state which depends on the error that occurred.
2. An integrity check for some integrity-protected data (including keys and PIN) 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 and does not use this integrity protected data.
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 breaks down or for other unexpected events. The TOE is unresponsive and a reset is required.
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 (private key, PIN) is made unavailable after de-allocation by overwriting this content with zeros.
9. The TOE does not emit information about IC power consumption, electromagnetic radiation and command execution and therefore enabling access to private and session keys and activity data.
10. The TOE ensures that any users are unable to use the smart card circuit contacts to gain access to private and session keys and activity data.
11. The cryptographic operations of the TOE are implemented so that observation does not yield any useful information about the security data used and the activity data used.

8.2 Assurance measures

This chapter describes the Assurance Measures fulfilling the requirements listed in Chapter 7.2.

The following table lists the Assurance measures and references the corresponding documents describing the measures

Table 1 : Reference of Assurance Measures

Assurance Measures	Description
AM_ADV	The representation of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The evaluator uses the development and guidance documentation by the developer as a basis for his vulnerability analysis.

8.3 Correspondence of SRF and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 8.1 the implementation of the TOE security functional requirements is described in form of the TOE security functions.

9 Statement of compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Hardware Platform Security Target of the Chip Infineon, M7892 B11 STLite. This statement is compliant to the requirements of [SUPP].

Topics

9.1 Matching statement

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

- certified Infineon Microcontroller Infineon, M7892 B11 STLite

The rationale of the HW platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs.

9.1.1 TOE Security Environment

9.1.1.1 Threats, OSPs and Assumptions

The only threats of this composite TOE which are directly related to IC functionality are T.Identification_Data and T.Activity_Data.

They can be mapped to the following HW platform-ST threats STLite:

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

Table 2 : Mapping of threats

	T.Phys-Manipulation	T.Phys-Probing	T.Malfunction	T.Leak-Inherent	T.Leak-Forced	T.Abuse-Func	T.Mem-Access
T.Identification_Data	x	x	x	x	x	x	x
T.Activity_Data	x	x	x	x	x	x	x
T.Data_Exchange	x	x	x	x	x	x	x

The OSP of the composite TOE (P.EU_Specifications) is not applicable to the IC.

The OSPs from the HW platform-ST are as follows STLite:

- P.Process-TOE
- P.Add-Functions

Table 3 : Mapping of hardware OSPs to composite security objectives

OSP	Classification of OSPs	Mapping to Security Objectives of this Composite-ST
P.Process-TOE	not relevant	not applicable
P.Add-Functions	not relevant	not applicable

The assumption from this ST (A.Personalisation_Phase) makes no assumption on the platform but only on the environment of the TOE.

The assumptions from the HW Platform-ST are as follows:

Table 4 : Mapping of assumptions

Assumptions of HW Platform-ST	Classification of significant assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC	not relevant	n/a
A.Plat-Appl	not relevant	n/a
A.Resp-Appl	relevant	OT.Card_Identification_Data, OT.Card_Activity_Storage
A.Key-Function	relevant	OT.Secure_Communications

The assumption **A.Process-Sec-IC** (security procedures to maintain confidentiality and integrity of the hardware TOE) only pertains to the hardware manufacturer.

A.Plat-Appl assumes that the IC embedded software is designed so that the relevant documents from the hardware manufacturer are taken into account. This is an objective which cannot be mapped to composite TOE because it can only be fulfilled by the software manufacturer in his development process. A.Plat-Appl is therefore disregarded.

A.Resp-Appl assumes that all user data owned by the embedded software are treated as defined for their specific application context. This is covered by the objective for the TOE: OT.Card_Identification_Data and OT.Card_Activity_Storage.

They have been entered into Table 4.

A.Key-Function assumes that key-dependent functions in the embedded software are not susceptible to leakage attacks. This is covered by the objective for the TOE: OT.Secure_Communications.

There is no conflict between security environments of this Composite-ST and the Platform-ST STLite.

9.1.1.2 Security objectives

Security objectives see: chapter 4 of [PP0070].

This Composite-ST has the following security objectives for the TOE which are directly related to the Platform-ST:

- OT.Card_Identification_Data
- OT.Card_Activity_Storage
- OT.Data_Access
- OT.Secure_Communications

These objectives will be mapped to the following HW Platform-ST ([STLite], chapter 5.1) objectives:

- O.Phys-Manipulation
- O.Phys-Probing
- O.Malfunction
- O.Leak-Inherent
- O.Leak-Forced
- O.Abuse-Func
- O.Add-Functions
- O.Mem-Access

The mapping is shown below.

Table 5 : Mapping of objectives

		O.Leak-Inherent	O.Add-Functions	O.Mem-Access	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func
Composite-ST	Objectives for TOE_IC								
	OT.Card_Identification_Data	X	X	X	X	X	X	X	X
	OT.Card_Activity_Storage	X	X	X	X	X	X	X	X
	OT.Data_Access	X	X	X	X	X	X	X	X
	OT.Secure_Communications	X	X	X	X	X	X	X	X

OT.Card_Identification_Data and **OT.Card_Activity_Storage** match all listed objectives of the Platform-ST because they provide functionality that supports the well-functioning of the TSFs of the TOE (avoiding they are bypassed or altered).

OT.Data_Access and **OT.Secure_Communications** match to all listed objectives of the Platform-ST because they describe features against physical attacks.

The objectives for the Operational Environment are not linked to the platform and are therefore not applicable to this mapping.

There is no conflict between security objectives of this Composite-ST and the platform-ST STLite.

9.1.1.3 Security requirements

Security Functional Requirements see Chapter 7.1

Table 6 : Mapping of Platform and Composite SFRs and Relevance

HW Platform SFR	Relevance (IP_SFR or RP_SFR)	Correspondence in Composite ST
FPT_FLS.1	RP_SFR	FPT_FLS.1
FRU_FLT.2	IP_SFR	Limited fault tolerance is not applicable for the TOE
FPT_PHP.3	RP_SFR	FPT_PHP.3
FCS_COP.1/DES	RP_SFR	FCS_COP.1.1/TDES, DES coprocessor is used
FCS_COP.1/AES	IP_SFR	IFX Library not used by TOE
FCS_COP.1/RSA	RP_SFR	FCS_COP.1.1/RSA, RSA coprocessor is used
FCS_COP.1/ECDH	IP_SFR	IFX Library not used by TOE
FCS_COP.1/SHA	IP_SFR	IFX Library not used by TOE
FCS_RNG.1	RP_SFR	FIA_UAU.3.2
FAU_SAS	IP_SFR	Test process before TOE Delivery is not used by the composite SFRs
FPT_TST.2	RP_SFR	FPT_TST.1
FDP_ACC.1	RP_SFR	FDP_ACC.2
FDP_ACF.1	RP_SFR	FDP_ACF.1
FMT_MSA.3	RP_SFR	These attributes are set in the development phase and can not be changed afterwards FDP_ACC.2
FMT_MSA.1	IP_SFR	not used by TOE: These attributes are not set at runtime
FMT_SMF.1	IP_SFR	The access for the configuration registers of the MMU is not used by the composite SFRs
FCS_CKM.1/RSA	IP_SFR	IFX Library not used by TOE
FCS_COP.1/ECDSA	IP_SFR	IFX Library not used by TOE
FCS_CKM.1/EC	IP_SFR	IFX Library not used by TOE
FDP_SDI.1	RP_SFR	FDP_SDI.2
FDP_SDI.2	RP_SFR	FDP_SDI.2

Table 6 : Mapping of Platform and Composite SFRs and Relevance

HW Platform SFR	Relevance (IP_SFR or RP_SFR)	Correspondence in Composite ST
FDP_ITT.1	RP_SFR	FPR_UNO.1, FPT_EMS.1
FPT_ITT.1	RP_SFR	FPR_UNO.1, FPT_EMS.1
FDP_IFC.1	RP_SFR	FPR_UNO.1, FPT_EMS.1
FMT_LIM.1	IP_SFR	Internal test features of the IFX platform are not accessible by the Composite TOE
FMT_LIM.2	IP_SFR	Internal test features of the IFX platform are not accessible by the Composite TOE

9.1.1.4 Assurance requirements

The Composite-ST requires EAL 4 augmented by:

ATE_DPT.2
AVA_VAN.5

The HW Platform-ST requires EAL 6 augmented by:

ALC_FLR.1

Therefore, the assurance requirements for the composite TOE and the hardware TOE are equal or better.

9.2 Overall no contradictions found

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

10 References, Acronyms and Glossary

Topics

10.1 References

Table 7 : Local References

BibEnt	Description
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 4, September 2012. CCMB-2012-09-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components. Version 3.1, Revision 4, September 2012. CCMB-2012-09-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components. Version 3.1, Revision 4, September 2012. CCMB-2012-09-003.
[EC_AN]	Annex I(B) of Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)
[EC_COR]	Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport, Official Journal of the European Communities L 71-86, 13.03.2004
[EC_AP2]	Appendix 2 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 – [EC_AN] Tachograph Cards Specification
[EC_AP10]	Appendix 10 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [EC_AN] - Generic Security Targets
[EC_AP11]	Appendix 11 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [EC_AN] - Common Security Mechanisms
[AGD InitGuide].	STARCOS 3.6 ID Tachograph C1 "Initialization Guide", Version 1.3 / Status 30.06.2016
[AGD PersoGuide]	STARCOS 3.6 ID Tachograph C1 " Persoguide – PDI ", Version 1.0 / Date 08.06.2016
[GUI Ope]	Operational user guidance STARCOS 3.6 ID Tachograph C1, Version 1.7 / Date 19.07.2016

Table 7 : Local References

BibEnt	Description
[GUI Pre]	Preparative procedures STARCOS 3.6 ID Tachograph C1, Version 1.8 / Date 21.07.2016
[JIL]	Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1(B), Version 1.12, June 2003
[PP0035]	Security IC Platform Protection Profile, Version 1.0, 15 July 2007, BSI-CC-PP-0035-2007
[PP0070]	Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, BSI-CC-PP-0070, Version 1.02, 15.11.2011
[PP98]	Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806
[PP99]	Smartcard Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 1999. Registered at French certification body under the number PP/9911
[STLite]	Security Target Lite M7892 B11 Recertification Including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Common Criteria CCv3.1 EAL6 augmented (EAL6+), Document version 0.3 as of 2015-10-13
[SUPP]	Joint Interpretation Library: "Composite product evaluation for Smart Cards and similar devices", Version 1.4, August 2015, Senior Officials Group Information Systems Security (SOGIS) → http://www.sogis.org/

10.2 Acronyms

Acronym	Term
AC	Access Condition
ACD	Activity Data
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
DF	Dedicated File
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
GST	Generic Security Target for Tachograph Card as defined in [EC_AP10]
IDD	Identification Data
ICV	Initial Chaining Value
MAC	Message Authentication Code
MF	Master File

Acronym	Term
MSC	Member State Certificate
PP	Protection Profile
PIN	Personal Identification Number
RAD	Reference Authentication Data
RAM	Random Access Memory
ROM	Read Only Memory
SAR	Security Assurance Requirement
SCD	Signature Creation Data
SCP	Symmetric Cryptographic Processor
SFR	Security Functional Requirement
SM	Secure Messaging
SMK	Secret Messaging Keys
SVD	Signature Verification Data
TOE	Target Of Evaluation
TDES	Triple DES
TSF	TOE Security Functionality
VAD	Verification Authentication Data
VRN	Vehicle Registration Number
VU	Vehicle Unit

10.3 Glossary

Term	Definition
Activity data	Activity data include • user activities data, • events and faults data and control activity data (date and time of first use of the vehicle, • vehicle odometer value at that time, • date and time of last use of the vehicle, • vehicle odometer value at that time, • VRN and registering Member State of the vehicle, • date and time the session was opened, • a daily presence counter, • the total distance travelled by the driver during this day, • a driver status at 00.00, information about changed activity, data related to places where daily work periods begin and/or end (the date and time of the entry, • the type of entry, the country and region entered, • the vehicle odometer value), • records of calibrations and/or time adjustments performed as well as counter indicating the number of calibrations performed (workshop card), • date and time of the control, type of the control, • period downloaded (control card), • date and time of the activity, • type of the activity, • period downloaded (company card)).
Application note	Optional informative part of the PP containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Authenticity	Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer
Cardholder	The rightful/legitimated holder of the Tachograph Card.
Certificate chain	Hierarchical sequence of Equipment Certificate (lowest level), Member State Certificate and European Public Key (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level.
Certification authority	A natural or legal person who certifies the assignment of public keys (for example PK.EQT) to serial number of equipment and to this end holds the licence.
Digital Signature	A digital signature is a seal affixed to digital data which is generated by the private signature key of an entity (a private signature key) and establishes the owner of the signature key (the entity) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.
Digital Tachograph	Recording equipment including a Vehicle Unit and a motion sensor connected to it.

Term	Definition
Digital Tachograph System	Equipment, people or organisations, involved in any way with the recording equipment and Tachograph Cards.
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
Identification data	Identification data includes • Card identification data (tachograph application data, • type of Tachograph Card, • IC serial number, • IC manufacturing references, • card number, • card type approval number, • card personalisation identification, • issuing Member state, • issuing authority name, • issue date, • card beginning of validity date, card expire date) and Cardholder identification data (surname and first name, • date of birth, • preferred language, • issuing Member State, • issuing authority name, • driving licence number, • workshop name and address (workshop card), • control body name and address (control card), • company name and address (company card)).
Initialisation	The process by which the card-specific structure data and non-card-specific data are stored in the card: for file based operating systems → the creation of MF and corresponding DF(s); for JavaCard operating systems → the applet instantiation.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. Tachograph Card's chip is an IC.
Motion data	The data exchanged with the Vehicle Unit, representative of speed and distance travelled.
Personal Identification Number (PIN)	A short secret password being only known to the approved workshops, necessary for using of workshop cards.

Term	Definition
Personalisation	The process by which the card-specific data and individual-related data (inclusive the cryptographic keys) are stored in the card.
Personalisation data	The card-specific and individual-related data inclusive the cryptographic keys stored during the Personalisation.
Personalisation Phase	The personalisation phase (Phase 6 of the IC life-cycle) includes the initialisation as well as the personalisation.
Pre-Personalisation	The process by which the chip-specific data are stored in the non-volatile memory of the TOE by the Chip Manufacturer for traceability of the non-personalised Cards and/or to secure shipment within or between the life-cycle phases. During the Pre- Personalisation the non-card-specific data (for example patch code) could be loaded too.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys), see sec. III.12.2 of [EC_AN]. Security data are part of sensitive data.
Sensitive data	Data stored by the recording equipment and by the Tachograph Cards that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data.
Tachograph cards	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A Tachograph Card may be of the following types: driver card, control card, workshop card, company card.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC1]).
User Data	Any data, other than security data (sec. III.12.2 of [EC_AN]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [EC_AN]. User data are part of sensitive data. CC give the following generic definitions for user data: Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [CC1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC2]).
Vehicle Unit	The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The Vehicle Unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.