DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

Common Criteria Protection Profile

Digital Tachograph – Tachograph Card (TC PP)

Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C)

Version 1.0, 9 May 2017

Foreword

This Protection Profile (PP) has been developed to outline the IT security requirements as defined in Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 [5], Annex 1C using the Common Criteria (CC) language and format (CC version 3.1 [1], [2], [3], Revision 4). This is to enable developers of tachograph cards to create their specific Security Target document according to CC, in order for the products to undergo a CC evaluation and certification process. The CC tachograph card certificate is one pre-requisite to obtain type approval for a tachograph card.

The development of the PP has been sponsored by the Joint Research Centre of the European Commission. The PP has been approved by the governmental IT security certification bodies organised within the Joint Interpretation Working Group (JIWG), which supports the mutual recognition of certificates under the umbrella of the European SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates).

The authors are grateful to Bundesamt für Sicherheit in der Informationstechnik (BSI) for permission to use text from BSI-CC-PP-0070 in preparation of this protection profile.

The PP supports the intent of the European Commission to ensure a common and comparable level of assurance for the technical components of the Digital Tachograph System in Europe. This PP reflects the security requirements of the Regulation [5]. Detail is added to the security requirements, but in the event of any conflict the wording of the Regulation shall prevail. The coverage of the requirements of [5] by the CC Security Requirements defined in the current PP is stated in Annex B of this PP.

Notes and comments to this Protection Profile should be referred to:

European Commission
DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

PP Context

This section is informative and does not form part of the protection profile requirements. Reference [5] identifies the need for a family of protection profiles covering the major elements of digital tachograph operation:

- Protection Profile for vehicle unit (VU),
- Protection Profile for tachograph card (TC),
- Protection Profile for motion sensor (MS),
- Protection Profile for external GNSS facility (EGF).

This document contains the protection profile for the tachograph card only. As the tachograph card is required to interface with the vehicle unit there is a need for alignment of the security functional requirements between them. For this reason the security functional requirements are presented in a modular manner, such that the consistency within the set of documents can be more easily determined.

The following diagram illustrates the operational environment, and the relationship between the protection profiles.

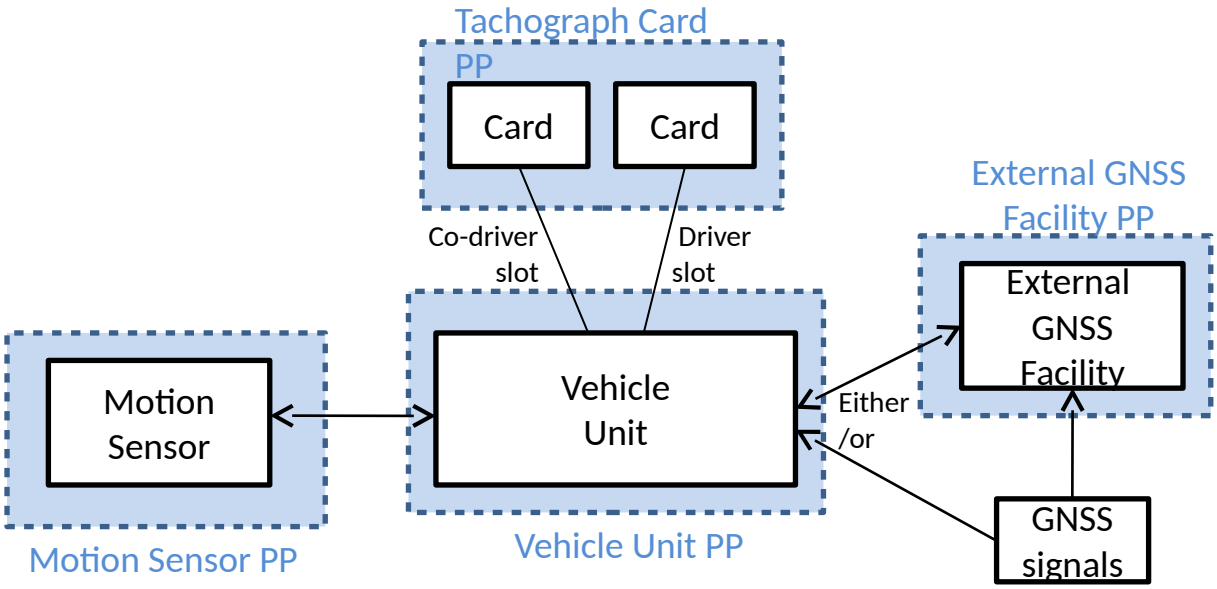

Figure 1: Protection Profile context

This family of protection profiles addresses the evaluation of second generation digital tachograph components only. However, given the need to allow for a gradual migration from first generation to second generation components, it has been necessary to mandate a level of interoperability with first generation components. This necessitates the support (mandatory or optional according to situation) for the communication protocols of the earlier generation to be expressed within the new protection profiles. Again, these security functional requirements have been separated for clarity.

Table of Contents

Table of Tables

Table of Figures

Revision history

Version	Date	Changes
1.0	9 May 2017	

1 PP Introduction

1 This section provides document management and overview information being required to register the protection profile and to enable a potential user of the PP to determine, whether the PP is of interest.

2 [5] Annex 1C requirements not included in this protection profile are not the subject of security certification.

3 The TC construction and functional requirements are specified in Chapter 4 and Appendix 2 of [5] Annex 1C.

1.1 PP Reference

Title:	Common Criteria Protection Profile: Digital Tachograph – Tachograph Card (TC PP)	
	Sponsor:	Joint Research Centre, European Commission
	Editor:	Julian Straw, David Bakker, Jacques Kunegel, Luigi Sportiello
	CC version:	3.1(Revision 4)
	Assurance level:	EAL4 augmented with ATE_DPT.2 and AVA_VAN.5
	Version number:	1.0
	Registration:	BSI-CC-PP-0091
	Keywords:	Digital Tachograph, Tachograph Card

1.2 TOE overview

1.2.1 TOE definition and operational usage

4 The Target of Evaluation (TOE) addressed by this protection profile is a second generation Tachograph Card in the sense of [5] Annex 1C, intended to be used in the digital tachograph system, which contains additionally motion sensors (of the 1st or 2nd generation), vehicle units (of the 1st or 2nd generation), remote early detection communication readers and, if applicable, external GNSS modules and remote communication facilities.

5 A Tachograph Card is a smart card that comprises:

a) The circuitry of the chip, including all IC dedicated software (usually preloaded and often security certified by the Chip Manufacturer) being active in the operational phase of the TOE (the integrated circuit, IC);
b) The IC Embedded Software (operating system, usually – together with IC – completely implementing executable functions);
c) The 2 tachograph applications (1st and 2nd generation); and
d) The associated guidance documentation.

6 The basic functions of the Tachograph Card are:

a) To store card identification and user identification data. This data is used by the Vehicle Unit to identify the human user, provide functions and data access rights accordingly;
b) To store data related to the human user, among which are user activities data, events and faults data and control activities.

7 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. connected to a personal computer) if it has the appropriate access rights.

8 Concerning write access, during the end-usage phase of a Tachograph Card life-cycle (phase 7 of life-cycle as described in section 1.2.3 of this PP), only Vehicle Units may write user data to the card.

9 The functional requirements for a Tachograph Card are specified in [5] Annex 1C, Chapter 4 and Appendix 2, and the common security mechanisms are specified in Appendix 11.

1.2.2 TOE major security features for operational use

10 The main security features of the TOE are as follows:

a) The TOE must preserve card identification data and user identification data stored during the card personalisation process;
b) The TOE must preserve user data stored in the card by Vehicle Units
c) The TOE must allow certain write operations onto the cards to only an authenticated VU.

11 Specifically the Tachograph Card aims to protect:

a) The data that is stored in such a way as to prevent unauthorised access to and manipulation of the data, and to detect any such attempts;
b) The integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

12 The main security features stated above are provided by the following major security services:

a) User identification and authentication;
b) Access control to functions and stored data;
c) Alerting of events and faults;
d) Integrity of stored data;
e) Reliability of services;
f) Data exchange with a Vehicle Unit and export of data to other IT entities;
g) Cryptographic support for VU-card mutual authentication and secure messaging as well as for key generation and key agreement according to [5] Annex 1C, Appendix 11.

13 All cryptographic mechanisms, including algorithms and the length of corresponding keys, have to be implemented exactly as required and defined in [5] Annex 1C, Appendix 11, Part B for second generation mechanisms, and in [5] Annex 1C, Appendix 11, Part A for first generation mechanisms. Cryptographic mechanisms supported by all cards include mutual authentication towards VUs. Additional cryptographic mechanisms, as applied within the different types of card are:

a) Driver cards – creation of signatures over data downloads;
b) Workshop cards – PIN verification, verification of MACs over Remote Tachograph Monitoring data and decryption of such data, creation of signatures over data downloads from workshop cards;

c) Control cards - verification of MACs over Remote Tachograph Monitoring data and decryption of such data, verification of signatures over data downloaded from VUs, driver cards or workshop cards.

Application note 1: 1st generation VU (compliant with Annex I B [6]) will not have to be replaced, following the application of the new [5] Annex 1C. They will continue to be used in the field, until their end of life. 2nd generation VU (compliant with [5] Annex 1C) will then be gradually introduced in the field, starting from the introduction date defined in Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 [5].

The main differences between the 2nd generation Digital Tachograph System and the 1st generation are:

- the security mechanisms, which have been changed,
- new functions that have been added (support for GNSS and remote communication, optional ITS interface),
- the stored data structure, which has been changed due to the new functions added.

In the 2nd generation Digital Tachograph System, the recording equipment includes:

- a Vehicle Unit (in which Tachograph Cards are inserted),
- a 2nd generation Motion Sensor,
- a remote communication facility, either internally to the vehicle unit or as a separate unit,
- a GNSS receiver (either internally to the vehicle unit or in an External GNSS facility).

Tachograph cards need to be interoperable with both Digital Tachograph Systems. So Tachograph Cards complying with this PP will be able to be used in both 1st and 2nd generation VUs. Therefore such Tachograph Cards will contain two applications, the first application being usable within the 1st generation Digital Tachograph System, the second one being usable within the 2nd generation system. Both applications are fully specified in [5] Annex 1C and its appendices.

Cards inserted in a 1st generation VU will be authenticated using 1st generation security mechanisms. The VU will have access to EF IC, ICC and to the 1st generation application (DF Tachograph).

Cards inserted in a 2nd generation VU will be authenticated using 2nd generation security mechanisms. The VU will have access to EF IC, ICC and to both the 1st and 2nd generation applications. Before the card is extracted from the VU, the VU will record the data both in the 2nd generation tachograph card application and in the 1st generation application.

This enables both 1st and 2nd generation VUs to have a complete view of the card history.

1.2.3 TOE type

14 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 [5] Annex 1C, Appendix 2, Appendix 10 and Appendix 11. In particular, this implies the compliance with the following standards:

a) ISO/IEC 7810 Identification cards – Physical characteristics;
b) ISO/IEC 7816 Identification cards - Integrated circuit cards
   i) Part 1: Physical characteristics
   ii) Part 2: Dimensions and location of the contacts
   iii) Part 3: Electronic signals and transmission protocols
   iv) Part 4: Organisation, security and commands for interchange
   v) Part 8: Commands and mechanisms for security operations;
c) ISO/IEC 10373 Identification cards – Test methods.

15 The typical smart card product life-cycle is decomposed in 7 phases as follows:

a) Phase 1: Smart Card Embedded Software Development
b) Phase 2: IC Design and IC Dedicated Software Development
c) Phase 3: IC Manufacturing
d) Phase 4: IC Packaging and Testing
e) Phase 5: Smart Card Product Finishing Process
f) Phase 6: Smart Card Personalisation
g) Phase 7: Smart Card Product End-usage

16 The CC (and this PP) do 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:

a) TOE development (including the development as well as the production of the TOE)
b) TOE delivery
c) TOE operational use

17 For the evaluation of a Tachograph Card, phases 1 to 4 are part of the TOE development in the sense of the CC. Phase 7 is explicitly in focus of the current PP and is part of the operational use in the sense of the CC. 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[1]. The ST author must define the exact boundary. However, this Protection Profile requires that the following conditions have to be met:

a) All executable software in the TOE has to be covered by the evaluation;
b) The data structures and the access rights to these data as defined in [5] Annex 1C, in particular the personalisation data itself and its creation and handling, are covered by the evaluation.

18 Phase 5 (Smart Card Product Finishing Process) consists of the loading of the smart card operating system on the packaged IC, thereby finishing the smart card as a platform on which software implementing the functionality specified in [5] Annex 1C may be installed.

1 Therefore in the remaining text of this PP the TOE Manufacturer will be the subject responsible for everything up to and including TOE delivery.

19 Phase 6 (Smart Card Personalisation Phase) can be divided into two steps: initialisation and personalisation of the user data. Initialisation involves the installation of the applet or embedded software implementing the functionality defined in [5], and the creation of the application file structure defined in [5]. With regard to functionality, the TOE (driver card, workshop card, control card or company card) is finished after initialisation. Where the architecture of the TOE does not have a clear distinction between the operation system and applets, in practice there may be little distinction between phases 5 and 6.

20 However, a TOE which is only initialised does not contain specific application data, and is not ready for the end-usage phase. The product can be used as a Tachograph Card (driver card, workshop card, control card or company card) only after personalisation, in which application data including Tachograph Card-specific cryptographic keys are stored.

21 As mentioned above, the end-usage of the TOE is explicitly the focus of the current PP. Nevertheless, the Security Target authors have to define the procedure for TOE delivery exactly. TOE delivery could take place before the initialisation and/or personalisation are finished. Depending on the approach adopted for TOE delivery, the corresponding guidance for initialisation and personalisation has to be prepared and delivered for evaluation, and made available for those who must use it. It is assumed in this PP that all of the initialisation and personalisation activities will take place in secure environments.

22 The Security Target authors may extend the TOE security functionality with respect to initialisation and personalisation if these take place after delivery. If not, and since the specific production steps of initialisation and/or personalisation are of major security relevance, these have to form part of the CC evaluation under the ALC activities. The relevant certification body must decide on a case by case basis under which evaluation activity (ALC or AGD) the initialisation and personalisation process should be examined. All production, generation and initialisation procedures after TOE delivery, up to entering use, have to be considered in the product evaluation process under the AGD assurance activities.

23 The following examples and remarks may help ST authors to define the boundary of TOE development.

a) The following variations for the boundary of the TOE development are acceptable:
   i) Phases 5 and 6 completely belong to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card, and containing all software, all data structures as defined in [5] Annex 1C and all card-specific data.
   ii) Phase 5 completely belongs to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software and at least the data structures as defined in [5] Annex I C.
   iii) The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in [5] Annex 1C, but is not yet embedded in a plastic card.
   iv) The TOE is delivered in (at least) two parts: The hardware as a module or already embedded in a plastic card on the one hand, and an initialisation file on the other. Both parts together again contain all software, and at least the data structures as defined in [5] Annex 1C (which in particular means that all of this is evaluated during ADV activities). In this case the evaluation

must also show as a result that the functions used by the customer (initialiser/personaliser/card issuer) for loading the initialisation data into the hardware provide sufficient protection against modification and (where applicable) disclosure of these data. The hardware must be authenticated before software loading, and this process of authentication is subject to evaluation under the ALC activity.

b) The following remarks may show how some CC assurance activities apply to parts of the life-cycle[2]
   i) The ALC class, which deals with security measures in the development environment of the TOE, applies to all development and production environments of phases 1 to 4, and to those parts of phases 5 and 6 belonging to TOE development, as defined in the ST for a TOE. In particular, the sites where the software of the TOE is developed, as well as the hardware development and production sites, are subject to this CC class (for example with regard to site visits). In the context of a composite evaluation some of the phases may already be covered by an IC hardware evaluation.
   ii) The measures for delivery of the TOE to the initialiser/personaliser/card issuer are subject to ALC_DEL.
   iii) If the fourth model described in "a." above is used (delivery of hardware and initialisation file), the loading of the initialisation data can be interpreted as part of installation, and is therefore covered by assurance class ALC and ADV.
   iv) The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures is covered by AGD_PRE. Since the initialiser/personaliser/card issuer is the first “user” of the TOE after delivery, the guidance documentation is mainly directed to them. They may be defined as the administrator of the TOE, or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:

      - Secure handling of the initialisation of the TOE including security measures needed for the initialisation and secure handling of the initialisation file.
      - Secure handling of the personalisation of the TOE.
      - Secure handling of delivery of the personalised TOE from the personaliser/card issuer to the human user.
      - Security measures for end-usage, which the personaliser/card issuer needs to communicate to the human user. A simple example for this may be the requirement for the human user of a workshop card to handle their PIN(s) securely. Since the documents accompanying the card during transport from card issuer to human user will probably not be available at the time of evaluation, the guidance documents for the

2 These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However, these explicit notes may serve as a help for ST writers and TOE developers to understand the connection between the life-cycle model and some CC requirements.

personaliser/card issuer need to contain this information connected with the requirement that the card issuer covers all such issues in his delivery documents.

1.2.4 Non-TOE hardware/software/firmware

24 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.

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

2 Conformance Claims

2.1 CC conformance claim

26 This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3]

as follows:

Part 2 extended (with FCS_RNG.1 and FPT_EMS.1),

Part 3 conformant (EAL4 augmented by ATE_DPT.2 and AVA_VAN.5).

2.2 PP claim

27 This protection profile does not claim conformance to any other protection profile.

28 The underlying integrated circuit of the TOE has to be successfully evaluated and certified in accordance with the Security IC Platform Protection Profile [8].

2.3 Package claim

29 This protection profile claims conformance to the assurance package defined in [5] Annex 1C, Appendix 10, as follows:
“SEC_006 The assurance level for each Protection Profile shall be EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5”.

2.4 Conformance claim rationale

30 This protection profile does not claim any conformance with other protection profiles. Therefore, no conformance claim rationale is provided here.

2.5 Conformance statement

31 This protection profile requires *strict* conformance of any security target or protection profile claiming conformance to this protection profile.

3 Security Problem Definition

Application note 2: Although each of the Tachograph Card types (driver card, workshop card, control card or company card) is used for a different purpose, this PP describes the Security Problem Definition in general terms for the Tachograph Card, considering the whole Digital Tachograph System, and the corresponding usage of the Tachograph Cards.

3.1 Introduction

3.1.1 Assets

32 The assets to be protected by the TOE and its environment within phase 7 of the TOE's life-cycle are the application data defined in the table below[3].

No.	Asset	Definition
1	Identification data (IDD)	Card identification data, user identification data (see Glossary for more details).
2	Activity data (ACD)	Activity data (see Glossary for more details).

Table 1 – Primary assets to be protected by the TOE and its environment

No.	Asset	Definition
3	Application (APP)	Tachograph application.
4	Keys to protect data (KPD)	Enduring private keys and session keys used to protect security data and user data held within and transmitted by the TOE, and as a means of authentication.
5	Signature verification data (SVD)	Public keys certified by Certification Authorities, used to verify electronic signatures.
6	Verification authentication data (VAD)	Authentication data provided as input for authentication attempt as authorised user (i.e. entered PIN on workshop cards).
7	Reference authentication data (RAD)	Data persistently stored by the TOE for verification of the authentication attempt as authorised user (i.e. reference PIN on workshop cards).
8	Data to be signed (DTBS)	The complete electronic data to be signed (including both user message and signature attributes).

3 The security properties to be maintained for each asset are defined in [5] Annex 1C, especially Appendices 2 and 11.

No.	Asset	Definition
9	TOE file system, including specific identification data	File structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation

Table 2 – Secondary assets to be protected by the TOE and its environment

33 All primary assets represent User Data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF and TSF-data in the sense of the CC. Security data and user data, stored by the Tachograph Card, need to be protected against unauthorised modification and disclosure. User data include card and human user identification data and activity data (see Glossary for more details), and match User Data in the sense of the CC. Security data are defined as specific data needed to support security enforcement, and match the TSF data in the sense of the CC.

3.1.2 Subjects and external entities

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

No.	Role	Definition
1	Administrator	Usually active only during Initialisation/Personalisation (Phase 6) – listed here for the sake of completeness.
2	Vehicle Unit[4]	Vehicle Unit (authenticated[5]), to which the Tachograph Card is connected (S.VU).
3	Other Device[6]	Other device (not authenticated) to which the Tachograph Card is connected (S.Non-VU).
4	Attacker	A human or a process located outside the TOE and trying to undermine the security policy defined by the current PP, especially to change properties of the maintained assets. For example, a driver could be an attacker if he misuses the driver card. An attacker is assumed to possess at most a *high* attack potential.

Table 3 - Subjects and external entities

Application note 3: This table defines the subjects in the sense of [1] which can be recognised by the TOE independently of their nature (human or process). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entities except the Attacker, who is listed for completeness – an ‘image’ inside and ‘works’ then with this

4 Tachograph cards may be inserted in 1st generation or 2nd generation Vehicle Units.
5 Authenticated to the tachograph card by the method specified in [5] Annex 1C, Appendix 11, Chapter 4 (for 1st generation VU) and Chapter 10 (for 2nd generation VU).
6 A specific device among these other devices is the remote early detection communication reader. A control card connected to such equipment shall decipher data sent by a VU, and also allow for verification of the authenticity and integrity of such data.

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

Application note 4: The subject Administrator is not included in the security functional requirements because this PP describes the TOE only for the end-usage phase - after personalisation. The ST author may decide to include the personalisation process into the scope of the ST. In this case additional security functional requirements, which involve the subject Administrator, have to be included.

3.2 Threats

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

36 The threats are defined in the following tables.

Label	Threat
T.Identification_Data	**Modification of Identification Data** - A successful modification of identification data held by the TOE (IDD, see sec. 3.1, e.g. the type of card, or the card expiry date or the user identification data) would allow an attacker to misrepresent driver activity.
T.Application	**Modification of Tachograph application -** A successful modification or replacement of the Tachograph application stored in the TOE (APP, see sec. 3.1), would allow an attacker to misrepresent human user (especially driver) activity.
T.Activity_Data	**Modification of Activity Data** - A successful modification of activity data stored in the TOE (ACD, see sec. 3.1,) would allow an attacker to misrepresent human user (especially driver) activity.
T.Data_Exchange	**Modification of Activity Data during Data Transfer** - A successful modification of activity data (ACD deletion, addition or modification, see sec. 3.1) during import or export would allow an attacker to misrepresent human user (especially driver) activity.
T.Clone	**Cloning of cards** – An attacker could read or copy secret cryptographic keys from a Tachograph card and use it to create a duplicate card, allowing an attacker to misrepresent human user (especially driver) activity.

Table 4 - Threats addressed by the TOE

3.3 Assumptions

37 This section describes the assumptions that are made about the operational environment in order to be able to provide the security functionality. If the TOE is placed in an operational environment that does not uphold these assumptions it may be unable to operate in a secure manner.

38 The assumptions are provided in the following table.

Label	Assumption
A.Personalisation_Phase	**Personalisation Phase Security -** All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation are correct according to [5] Annex 1C, and are handled correctly so as to preserve the integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE.

Table 5 - Assumptions

Application note 5: For the definition of the terms 'Personalisation Phase', 'initialisation' and 'personalisation' refer to section 1.2.3. Depending on the life-cycle model and delivery model chosen for the TOE the assumption A.Personalisation_Phase has to be adapted appropriately (in particular in view of the security objective OE.Personalisation_Phase) by the ST author.

3.4 Organisational security policies

39 This section shows the organisational security policies that are to be enforced by the TOE, its operational environment, or a combination of the two.

40 The organisational security policies are provided in the following table.

Label	Organisational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [5] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

Table 6 – Organisational security policies

4 Security Objectives

41 This section identifies the security objectives for the TOE and for its operational environment. The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- Provide a high-level, natural-language solution of the problem;
- Divide this solution into two part-wise solutions, that reflect that different entities each have to address a part of the problem;
- Demonstrate that these part-wise solutions form a complete solution to the problem.

4.1 Security objectives for the TOE

42 The TOE security objectives address the protection to be provided by the TOE, independent of the TOE environment, and are listed in the table below. All security objectives are expressed in the context of the requirements of [5] and [6].

Label	Security objective for the TOE
O.Card_Identification_Data	**Integrity of Identification Data** - The TOE must preserve the integrity of card identification data and user identification data stored during the card personalisation process.
O.Card_Activity_Storage	**Integrity of Activity Data -** The TOE must preserve the integrity of user data stored in the card by Vehicle Units.
O.Protect_Secret	**Protection of secret keys** – The TOE must preserve the confidentiality of its secret cryptographic keys, and must prevent them from being copied.
O.Data_Access	**User Data Write Access Limitation** - The TOE must limit user data write access to authenticated Vehicle Units.
O.Secure_Communications	**Secure Communications** - The TOE must support secure communication protocols and procedures between the card and the Vehicle Unit when required.
O.Crypto_Implement	**Cryptographic operation** – The cryptographic functions must be implemented as required by [5] Annex 1C, Appendix 11.
O.Software_Update	**Software updates** - Where updates to TOE software are possible, the TOE must accept only those that are authorised.[7]

Table 7 – Security objectives for the TOE

7 Where software update is implemented in the TOE the ST author must add iterations of FCS components to describe the approach employed to protect the authenticity and integrity of the update. The ST author must also specify what elements of the TOE software can be updated by this means (e.g. operating system, tachograph application).

4.2 Security objectives for the operational environment

43 The security objectives for the operational environment address the protection that must be provided by the TOE environment, independent of the TOE itself, and are listed in the table below.

Label	Security objective for the environment
OE.Personalisation_Phase	**Secure Handling of Data in Personalisation Phase -** All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation must be correct according to [5] Annex 1C, and must be handled so as to preserve the integrity and confidentiality of the data. The Personalisation Service Provider must control all materials, equipment and information that are used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality.
OE.Crypto_Admin	**Implementation of Tachograph Components** – All requirements from [5] concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.
OE.EOL	**End of life** - When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that the confidentiality of symmetric and private cryptographic keys has to be safeguarded.

Table 8 - Threats addressed by the operational environment.

5 Extended Components Definition

44 For this protection profile the security functional requirements in CC Part 2 have been extended to cover part of the TOE functionality that cannot otherwise clearly be expressed.

45 This protection profile uses two components defined as an extension to CC Part 2. Family FPT_EMS (TOE Emanation) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. Family FCS_RNG (Random number generation) is fully defined and justified in [7] Chapter 3. This PP defines a restricted set of ways in which the extended component can be used in a security target. These are set out in Annex B, and further information is provided in [7].

5.1 Class FCS: Cryptographic support

5.1.1 Generation of random numbers (FCS_RNG)

Rationale

46 CC Part 2 [2] defines two components FIA_SOS.2 and FCS_CKM.1 that are similar to FCS_RNG.1. However, FCS_RNG.1 allows the specification of requirements for the generation of random numbers in a manner that includes necessary information for intended use, as is required here. These details describe the quality of the generated data that other security services rely upon. Thus by using FCS_RNG a PP or ST author is able to express a coherent set of SFRs that include the generation of random numbers as a security service.

Family behaviour

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

Component levelling

FCS_RNG: Generation of random numbers	1

48 FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

49 There are no management activities foreseen.

Audit: FCS_RNG.1

50 There are no auditable events foreseen

FCS_RNG.1 Generation of random numbers

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

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

5.2 Class FPT: Protection of the TSF

5.2.1 TOE Emanation (FPT_EMS)

Rationale

51 Family FPT_EMS (TOE Emanation) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. This requirement is not covered by CC Part 2 [2].

Family behaviour

52 This family defines requirements to prevent attacks against TSF data and user data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

Component leveling

53 FPT_EMS TOE emanation requires that the TOE does not produce intelligible emissions that enable access to TSF data or user data.

Management

54 There are no management activities foreseen.

Audit

55 There are no actions defined to be auditable.

5.2.1.1 FPT_EMS.1 TOE emanation

Hierarchical to: -
Dependencies: -

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

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

6 TOE Security Requirements

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

57 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 [1] of the CC. Each of these operations is used in this PP.

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

59 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted by underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

60 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted by underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicised. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this text is *underlined and italicised*.

61 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator.

6.1 Security functional requirements for the TOE

62 This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications. This is to facilitate comparison of the communication requirements between this PP and others in the PP family. Section 6.1.1 addresses requirements for the tachograph card. Section 6.1.2 addresses the communication requirements for 2nd generation vehicle units to be used with the TOE. Section 6.1.3 addresses the communication requirements for 1st generation vehicle units to be used with the TOE.

6.1.1 Security functional requirements for the TC

6.1.1.1 Class FAU Security Audit

6.1.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: -
Dependencies: FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1 The TSF shall take [the following actions:
a) For user authentication failures and activity data input integrity errors – respond to the VU through SW1 SW2 status words, as defined in [5] Annex 1C, Appendix 2;

b) For self test errors and stored data integrity errors - respond to any VU command with an SW1 SW2 status word indicating the error]

upon detection of a potential security violation.

Application note 6: The ST author must identify in the ST the messages through which the errors in b) above are communicated.

6.1.1.1.2 FAU_SAA.1 Potential violation analysis

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation

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

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

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

known to indicate a potential security violation;

b) [assignment: *any other rules*].

Application note 7: The events user authentication failure, self test error, stored data integrity error and activity data input integrity error may occur in combination or as single failure event. The vehicle unit is informed of such events through the SW1 SW2 status words in responses to vehicle unit requests. The vehicle unit then stores events indicated by the TOE.

6.1.1.2 Class FCO Communication

6.1.1.2.1 FCO_NRO.1 Selective proof of origin

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [data to be downloaded to external media] at the request of the [recipient] **in accordance with [5] Annex 1C, Appendix 11, sections 6.1 and 14.2**.

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

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [recipient] given [that the digital certificate used in the digital signature for the downloaded data has not expired (see [5] Appendix 11, sections 6.2 and 14.3].

Application note 8: Note that FCO_NRO.1 applies only to driver cards and workshop cards, as those are the only cards capable of creating a signature over downloaded data. See [5] Appendix 11, sections 6 and 14.

6.1.1.3 Class FDP User data protection

6.1.1.3.1 FDP_ACC.2 Complete access control

Hierarchical to: -
Dependencies: FDP_ACF.1 Access control functions

FDP_ACC.2.1 The TSF shall enforce the [AC SFP] on [
Subjects:
- S.VU (a vehicle unit in the sense of [5] Annex 1C)
- S.Non-VU (other card interface devices)

Objects

- User data
  - User Identification data
  - Activity data
- Security data
  - Cryptographic keys (see Table 16, Table 17, Table 19 and Table 20)
  - PIN (for Workshop card)
- TOE application code
- TOE file system
- Card identification data
- Master file contents]

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.

6.1.1.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: -
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [AC SFP] to objects based on the following: [Subjects:
- S.VU (in the sense of [5] Annex 1C)
- S.Non-VU (other card interface devices)

Objects

- User data
  - User identification data
  - Activity data
- Security data
  - Cryptographic keys (see Table 16, Table 17, Table 19 and Table 20)
  - PIN (for Workshop card)

- TOE application code
- TOE file system (Attribute: access conditions)
- Card identification data
- Master file contents].

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 user identification data stored in the 1st generation tachograph application, which may be read by S.VU only

IDENTIF_WRITE

- All card types: card identification data and user identification data may only be written once and before the end of Personalisation
- No user may write or modify identification data during the end-usage phase of the card life-cycle

ACTIVITY_WRITE

- All card types: activity data may be written to the card by S.VU only

SOFT_UPGRADE

- All card types: TOEapplication code may only be upgraded following successful authentication

FILE_STRUCTURE

- All card types: files structure and access conditions shall be created before Personalisation is completed and then locked from any future modification or deletion by any user without successful authentication by the party responsible for card initialisation].

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [
SECRET KEYS

- The TSF shall prevent access to secret cryptographic keys other than for use in the TSF's cryptographic operations, or in case of a workshop card only, for exporting the SensorInstallationSecData to a VU, as specified in [5] Annex 1C, Appendix 2].

6.1.1.3.3 FDP_DAU.1 Basic data authentication

Hierarchical to: -
Dependencies: -

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity[8] of [activity data].
FDP_DAU.1.2 The TSF shall provide [S.VU and S.Non-VU] with the ability to verify evidence of the validity of the indicated information.

6.1.1.3.4 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: -
Dependencies: FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control
FDP_ETC.1.1 The TSF shall enforce the [AC SFP] when exporting user data controlled under the SFP(s), outside the TOE.
FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.1.3.5 FDP_ETC.2 Export of user data with security attributes

Hierarchical to: -
Dependencies: FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control
FDP_ETC.2.1 The TSF shall enforce the [AC SFP] when exporting user data controlled under the SFP(s), outside 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].

6.1.1.3.6 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: -
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] 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].

6.1.1.3.7 FDP_ITC.2 Import of user data with security attributes

Hierarchical to: -
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FPT_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1 The TSF shall enforce the [Input Sources SFP] when importing user data, controlled under the SFP, from outside of the TOE.

8 In the context of this PP "validity" means integrity and authenticity.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE: [
- unauthenticated inputs from external sources shall not be accepted as executable code;
- if application software updates are permitted they shall be verified using cryptographic security attributes before being implemented].

Application note 9: If application software can be updated only in the manufacturing environment then the requirement for verified software updates is not applicable. Where applicable the cryptographic security attributes employed must be described in the security target.

6.1.1.3.8 FDP_RIP.1 Subset residual information protection

Hierarchical to: -

Dependencies: -

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

6.1.1.3.9 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: -

Dependencies: -

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

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

6.1.1.4 Class FIA Identification and authentication

6.1.1.4.1 FIA_AFL.1 Authentication failure handling (1: C)

Hierarchical to: -

Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2(1:C) When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [
a) warn the entity connected,
b) assume the user to be S.Non-VU].

6.1.1.4.2 FIA_AFL.1 Authentication failure handling (2:WC)

Hierarchical to: -
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1(2:WC) The TSF shall detect when [5] unsuccessful authentication attempts occur related to [PIN verification of Workshop Card].
FIA_AFL.1.2(2:WC) When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [
a) warn the entity connected,
b) block the PIN check procedure such that any subsequent PIN check attempt will fail,
c) be able to indicate to subsequent users the reason for the blocking].

6.1.1.4.3 FIA_ATD.1 User attribute definition

Hierarchical to: -
Dependencies: -
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:[
a) User_group (Vehicle_Unit, Non_Vehicle_Unit);
b) User_ID (VRN and registering member state for subject S.VU)].

6.1.1.4.4 FIA_UAU.3 Unforgeable authentication

Hierarchical to: -
Dependencies: -
FIA_UAU.3.1 The TSF shall [prevent] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2 The TSF shall [prevent] use of authentication data that has been copied from any other user of the TSF.

6.1.1.4.5 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: -
Dependencies: -
FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [key based authentication mechanisms as defined in [5] Appendix 11, Chapters 4 and 10].

6.1.1.4.6 FIA_UID.2 User authentication before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: -
FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application note 10: The identification of the user is initiated following insertion of the card into a card reader and power-up of the card.

6.1.1.4.7 FIA_USB.1 User-subject binding

Hierarchical to: -
Dependencies: FIA_ATD.1 User attribute definition
FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [

a) User_group (Vehicle_Unit for S.VU, Non_Vehicle_Unit for S.Non-VU);
b) User_ID (VRN and registering member state for subject S.VU)].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of the user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

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*].

6.1.1.5 Class FPR Privacy

6.1.1.5.1 FPR_UNO.1 Unobservability

Hierarchical to: -
Dependencies: -

FPR_UNO.1 The TSF shall ensure that [attackers] are unable to observe the operation [any operation involving authentication and/or cryptographic operations] on [security and activity data] by [any user].

6.1.1.6 Class FPT Protection of the TSF

6.1.1.6.1 FPT_EMS.1 TOE emanation

Hierarchical to: -
Dependencies: -

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

FPT_EMS.1.2 The TSF shall ensure [any users] are unable to use the following interface [smart card circuit contacts] to gain access to [private keys or session keys] and [assignment: *list of types of user data*].

Application note 11: The ST author shall perform the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE shall prevent 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.

6.1.1.6.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -
Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state[9] when the following types of failures occur [

a) Reset;

b) Power supply cut-off;

c) Deviation from the specified values of the power supply;

d) Unexpected abortion of TSF execution due to external or internal events (especially interruption of a transaction before completion)].

6.1.1.6.3 FPT_PHP.3 Resistance to physical attack

Hierarchical to: -
Dependencies: -

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

Application note 12: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSF security could not be violated at any time. Hence, automatic response means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.1.1.6.4 FPT_TST.1 TSF testing

Hierarchical to: -
Dependencies: -

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up[10] and periodically during normal operation] to demonstrate the correct operation of [the TSF].

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

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

6.1.2 Security functional requirements for external communications (2nd Generation)

63 The security functional requirements in this section are required to support communications specifically with 2nd generation vehicle units.

6.1.2.1 Class FCS Cryptographic support

6.1.2.1.1 FCS_CKM.1 Cryptographic key generation (1)

Hierarchical to: -

9 A secure state is defined in CC as a state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
10 During initial start-up means before other code is executed.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(1) The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [5] Annex 1C, Appendix 11, Section 10 (for VU authentication and for the secure messaging session key)] and specified cryptographic key sizes [key sizes required by [5] Annex 1C, Appendix 11, Part B] that meet the following: [Reference [7] predefined RNG class [selection: *PTG.2, PTG.3, DRG.2, DRG.3, DRG.4, NTG.1*], [5] Annex 1C, Appendix 11, Section 10].

Application note 13: The ST author selects one of the permitted predefined RNG classes from [7], and completes the operations in FCS_CKM.1(1) and FCS_RNG.1 as required.

6.1.2.1.2 FCS_CKM.2 Cryptographic key distribution (1)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1(1) The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [secure messaging AES session key agreement as specified in [5] Annex 1C, Appendix 11, Part B] that meets the following [[5] Annex 1C, Appendix 11, Part B].

Application note 14: FCS_CKM.1(1) and FCS_CKM.2(1) relate to session key agreement with the vehicle unit.

6.1.2.1.3 FCS_CKM.4 Cryptographic key destruction (1)

Hierarchical to: -

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(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 [

- Requirements in Table 20;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[11]
- [assignment: *list of standards*]].

6.1.2.1.4 FCS_COP.1 Cryptographic operation (1: AES)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

11 Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1:AES) The TSF shall perform [the following:

a) ensuring authenticity and integrity of data exchanged between a vehicle unit and a tachograph card;
b) where applicable, ensuring confidentiality of data exchanged between a vehicle unit and a tachograph card;
c) decrypting confidential data sent by a vehicle unit to a remote early detection communication reader over a DSRC connection, and verifying the authenticity of that data;]

in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128, 192, 256 bits] that meet the following: [FIPS PUB 197: Advanced Encryption Standard, [5] Annex 1C, Appendix 11].

6.1.2.1.5 FCS_COP.1 Cryptographic operation (2:SHA-2)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of 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(2:SHA-2) The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS), [5] Annex 1C, Appendix 11].

6.1.2.1.6 FCS_COP.1 Cryptographic operation (3: ECC)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of 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(3:ECC) The TSF shall perform [the following cryptographic operations:

a) digital signature generation;
b) digital signature verification;
c) cryptographic key agreement;
d) mutual authentication between a vehicle unit and a tachograph card;
e) ensuring authenticity, integrity and non-repudation of data downloaded from a tachograph card]

in accordance with a specified cryptographic algorithm [[5] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [5], Appendix 11, Part B] that meet the following: [[5] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-

03111 – Elliptic Curve Cryptography – version 2, and the standardized domain parameters in Table 9

Name	Size (bits)	Object identifier
NIST P-256	256	secp256r1
BrainpoolP256r1	256	brainpoolP256r1
NIST P-384	384	secp384r1
BrainpoolP384r1	384	brainpoolP384r1
BrainpoolP512r1	512	brainpoolP512r1
NIST P-521	521	secp521r1

Table 9 - Standardised domain parameters

].

Application note 15: Where a symmetric algorithm, an asymmetric algorithm and/or a hashing algorithm are used together to form a security protocol, their respective key lengths and hash sizes shall be of (roughly) equal strength. Table 10 shows the allowed cipher suites. ECC keys sizes of 512 bits and 521 bits are considered to be equal in strength for all purposes within this PP.

Cipher suite Id	ECC key size (bits)	AES key length (bits)	Hashing algorithm	MAC length (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Table 10 - Cipher suites

6.1.2.1.7 FCS_RNG.1 Random number generation

Hierarchical to: -
Dependencies: -
FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6.1.2.2 Class FIA Identification and authentication

6.1.2.2.1 FIA_UAU.1 Timing of authentication (1)

Hierarchical to: -
Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1(1) The TSF shall allow [

a) Driver card, workshop card – export of user data with security attributes (card data download function) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2;

b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2]

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

FIA_UAU.1.2(1) The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Chapter 10** before allowing any other TSF-mediated actions on behalf of that user.

Application note 16: FIA_UAU.1.1(1) a) allows non secured readers to get signed downloaded data from driver and workshop cards, without any previous authentication. This can be used by company download tools, which are considered as "other devices" in the sense of this PP. Such download tools, and also vehicle units, are also allowed to read driver and workshop card data in a non secured mode (without any previous authentication). This is allowed by [5] Annex 1C, Appendix 2 access rules (see section 4, access rules = 'ALW').
Similarly, FIA_UAU.1.1(1) b) allows "other devices" (without having performed any authentication) to access data from control and company cards, following [5] Annex 1C, Appendix 2, Section 4 access rules.

6.1.2.3 Class FPT Protection of the TSF

6.1.2.3.1 FPT_TDC.1 Inter-TSF basic TSF data consistency (1)

Hierarchical to: -
Dependencies: -

FPT_TDC.1.1(1) The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [5] Annex 1C, Appendix 11] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

FPT_TDC.1.2(1) The TSF shall use [the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit**.

6.1.2.4 Class FTP Trusted path/channels

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

Hierarchical to: -
Dependencies: -

FTP_ITC.1.1(1) The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **the vehicle unit** 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(1) The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall ~~initiate communication via~~ **use** the trusted channel for [all commands and responses exchanged with a vehicle unit after successful chip authentication and until the end of the session].

Application note 17: The requirements for establishing the trusted channel are given in [5] Appendix 11, Chapter 10 (for 2nd generation vehicle units).

6.1.3 Security functional requirements for external communications (1st generation)

64 The following requirements shall be met only when the TOE is communicating with 1st generation vehicle units.

6.1.3.1 Class FCS Cryptographic support

6.1.3.1.1 FCS_CKM.1 Cryptographic key generation (2)

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [5] Annex 1C, Appendix 11, Section 4 (for the secure messaging session key)] and specified cryptographic key sizes [112 bits] that meet the following: [two-key TDES as specified in [5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.3.1.2 FCS_CKM.2 Cryptographic key distribution (2)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1(2) The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [for triple DES session keys as specified in [5] Annex 1C, Appendix 11 Part A] that meets the following [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.3.1.3 FCS_CKM.4 Cryptographic key destruction (2)

Hierarchical to: -

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(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following [

- Requirements in Table 16 and Table 17;

- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[12]
- [assignment: *list of further standards*]].

6.1.3.1.4 FCS_COP.1 Cryptographic operation (4:TDES)

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of 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(4:TDES) The TSF shall perform [the cryptographic operations (encryption, decryption, Retail-MAC)] in accordance with a specified cryptographic algorithm [Triple DES] and cryptographic key sizes [112 bits] that meet the following: [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.3.1.5 FCS_COP.1 Cryptographic operation (5:RSA)

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of 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(5:RSA) The TSF shall perform [the cryptographic operations (encryption, decryption, signing, verification)] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [1024 bits] that meet the following: [[5] Annex 1C, Appendix 11 Part A, Chapter 3].

6.1.3.1.6 FCS_COP.1 Cryptographic operation (6:SHA-1)

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of 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(6:SHA-1) The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS)].

6.1.3.2 Class FIA Identification and authentication

6.1.3.2.1 FIA_UAU.1 Timing of authentication (2)

Hierarchical to: -
Dependencies: FIA_UID.1 Timing of Identification
FIA_UAU.1.1(2) The TSF shall allow [

12 Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

a) Driver card, workshop card – export of user data with security attributes (digital signature used in card data download function, see [5] Annex 1C, Appendix 11, Chapters 6 and 14)) and export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2;

b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [5] Annex 1C, Appendix 2]

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

FIA_UAU.1.2(2) The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Chapter 5** before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 Class FPT Protection of the TSF

6.1.3.3.1 FPT_TDC.1 Inter-TSF basic TSF data consistency (2)

Hierarchical to: -
Dependencies: -

FPT_TDC.1.1(2) The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [5] Annex 1C, Appendix 11 Chapter 5] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

FPT_TDC.1.2(2) The TSF shall use [the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11 Part A, Chapter 5] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit**.

6.1.3.4 Class FTP Trusted path/channels

6.1.3.4.1 FTP_ITC.1 Inter-TSF trusted channel (2)

Hierarchical to: -
Dependencies: -

FTP_ITC.1.1(2) The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **the vehicle unit** 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(2) The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall ~~initiate communication via~~ **use** the trusted channel for [data import from and export to a vehicle unit in accordance with [6] Appendix 2].

Application note 18: The requirements for establishing the trusted channel are given in [5] Appendix 11, Chapter 5 (for 1st generation vehicle units).

6.2 Security assurance requirements for the TOE

65 The assurance level for this protection profile is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [3].

66 These security assurance requirements are derived from [5] Annex 1C, Appendix 10 (SEC_006).

7 Rationale

7.1 Security objectives rationale

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

	T.Identification_Data	T. Activity_Data	T.Application	T.Data_Exchange	T.Clone	A.Personalisation_Phase	P.Crypto
O.Card_Identification_Data	x						
O.Card_Activity_Storage		x					
O.Protect_Secret			x	x	x		
O.Data_Access		x					
O.Secure_Communications				x			
O.Crypto_Implement	x	x	x	x			x
O.Software_Update			x				
OE.Personalisation_Phase						x	
OE.Crypto_Admin	x	x		x		x	
OE.EOL			x		x		

Table 11 - Security objectives rationale

68 A detailed justification required for *suitability* of the security objectives to address the security problem definition is given below.

69 **T.Identification_Data** is addressed by O.Card_Identification_Data, which requires that the TOE preserve the integrity of card identification and user identification data stored during the card personalisation process. O.Crypto_Implement and OE.Crypto_Admin require the implementation and management of strong cryptography to support this.

70 **T.Activity_Data** is addressed by O.Card_Activity_Storage, which requires that the TOE preserve the integrity of activity data stored during card operation. O.Data_Access requires that only an authenticated VU may access user data in the TOE. O.Crypto_Implement and OE.Crypto_Admin require the implementation and management of strong cryptography to support this.

71 **T.Application** is addressed by O.Software_Update, which requires any update of the Tachograph application to be authorised. This is supported by O.Crypto_Implement and O.Protect_Secret, which support the integrity checking of software, and the authorisation of any updates, and by OE.EOL, which requires the card to be disposed of in a secure manner when no longer in use.

72 **T.Data_Exchange** is addressed by O.Secure_Communications, which requires that the TOE use secure communication protocols for data exchange with card interface devices, as required by applications. O.Crypto_Implement and OE.Crypto_Admin require the implementation and management of strong cryptography to support this. O.Protect_Secret requires secret keys used in the exchange to remain confidential.

73 **T.Clone** is addressed by O.Protect_Secret. The TOE is required to prevent an attacker from extracting cryptographic keys for cloning purposes by preserving their confidentiality, and preventing them from being copied. This is supported by OE.EOL, which requires the card to be disposed of in a secure manner when no longer in use.

74 **A.Personalisation_Phase** is supported through the corresponding environment objective OE.Personalisation_Phase, which requires that data is correctly managed during that phase to preserve its confidentiality and integrity. OE.Crypto_Admin requires correct management of cryptographic material.

75 **P.Crypto** requires the use of specified cryptographic algorithms and keys, and this is addressed through the corresponding O.Crypto_Implement objective.

7.2 Security requirements rationale

7.2.1 Rationale for SFRs' dependencies

76 The following table shows how the dependencies for each SFR are satisfied.

SFR	Dependencies	Rationale
TC Core		
FAU_ARP.1	FAU_SAA.1	Satisfied by FAU_SAA.1
FAU_SAA.1	FAU_GEN.1	*See note 1 below*
FCO_NRO.1	FIA_UID.1	Satisfied by FIA_UID.2
FDP_ACC.2	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2 *See note 2 below*
FDP_DAU.1	-	-
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2 *See note 2 below*
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1, FPT_TDC.1	Satisfied by FDP_ACC.2, FTP_ITC.1(1 & 2) and FPT_TDC.1(1 & 2)
FDP_RIP.1	-	-
FDP_SDI.2	-	-

SFR	Dependencies	Rationale
FIA_AFL.1(1:C)	FIA_UAU.1	Satisfied by FIA_UAU.1(1 & 2)
FIA_AFL.1(2:WC)	FIA_UAU.1	Satisfied by FIA_UAU.1(1 & 2)
FIA_ATD.1	-	-
FIA_UAU.3	-	-
FIA_UAU.4	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1	Satisfied by FIA_ATD.1
FPR_UNO.1	-	-
FPT_EMS.1[13]	-	-
FPT_FLS.1	-	-
FPT_PHP.3	-	-
FPT_TST.1	-	-
2nd generation specific		
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2(1), FCS_COP.1(1:AES & 3:ECC) and FCS_CKM.4(1)
FCS_CKM.2(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_CKM.4(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1(1)
FCS_COP.1(1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(1) and FCS_CKM.4(1)
FCS_COP.1(2:SHA-2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-2
FCS_COP.1(3:ECC)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4(1)
FCS_RNG.1[14]	-	-
FIA_UAU.1(1)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(1)	-	-
FTP_ITC.1(1)	-	-
1st generation specific		
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2(2), FCS_COP.1(4:TDES &

13 Extended component
14 Extended component

SFR	Dependencies	Rationale
		5:RSA) and FCS_CKM.4(2)
FCS_CKM.2(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_COP.1(4:TDES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.1, FDP_ITC.2, FCS_CKM.1(2) and FCS_CKM.4(2)
FCS_COP.1(5:RSA)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4(2)
FCS_COP.1(6:SHA-1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-1
FIA_UAU.1(2)	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1(2)	-	-
FTP_ITC.1(2)	-	-

Table 12 - SFRs' dependencies

Note 1: The dependency FAU_GEN.1 (Audit Data Generation) is not applicable to the TOE. Tachograph cards do not generate audit records but react with an error response. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.
Note 2: The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the Personalisation Phase, and are fixed over the whole lifetime of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, either during personalization, or within the usage phase of the TOE. This argument holds for both FDP_ACF.1 and FDP_ITC.1.

7.2.2 Security functional requirements rationale

77 The following table provides an overview for security functional requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

		ication_DataO.Card_	rageO.Card_Activity_	O.Protect_Secret	O.Data_Access	nunicationsO.Secure_	ImplementO.Crypto_	O.Software_Update
FAU_ARP.1	Security alarms	x	x			x		
FAU_SAA.1	Potential violation analysis	x	x			x		
FCO_NRO.1	Selective proof of origin					x		

		ication_DataO.Card_	rageO.Card_Activity_	O.Protect_Secret	O.Data_Access	nunicationsO.Secure_	ImplementO.Crypto_	O.Software_Update
FDP_ACC.2	Complete access control	x	x	x	x	x		x
FDP_ACF.1	Security attribute based access control	x	x	x	x	x		x
FDP_DAU.1	Basic data authentication					x	x	
FDP_ETC.1	Export of user data without security attributes					x		
FDP_ETC.2	Export of user data with security attributes					x		
FDP_ITC.1	Import of user data without security attributes					x		
FDP_ITC.2	Import of user data with security attributes							x
FDP_RIP.1	Subset residual information protection			x		x		
FDP_SDI.2	Stored data integrity monitoring and action	x	x				x	
FIA_AFL.1	Authentication failure handling (1:C)				x			
FIA_AFL.1	Authentication failure handling (2:WC)				x			
FIA_ATD.1	User attribute definition				x			
FIA_UAU.3	Unforgeable authentication				x	x	x	
FIA_UAU.4	Single-use authentication mechanism					x	x	
FIA_UID.2	User authentication before any action				x			
FIA_USB.1	User-subject binding				x			
FPR_UNO.1	Unobservability			x		x		
FPT_EMS.1	TOE emanation	x	x	x	x			
FPT_FLS.1	Failure with preservation of secure state	x	x		x			
FPT_PHP.3	Resistance to physical attack	x	x	x	x			x
FPT_TST.1	TSF testing	x	x		x			
FCS_CKM.1	Cryptographic key generation (1)					x	x	
FCS_CKM.2	Cryptographic key distribution (1)					x	x	

		ication_DataO.Card_	rageO.Card_Activity_	O.Protect_Secret	O.Data_Access	nunicationsO.Secure_	ImplementO.Crypto_	O.Software_Update
FCS_CKM.4	Cryptographic key destruction (1)					x	x	
FCS_COP.1	Cryptographic operation (1:AES)					x	x	
FCS_COP.1	Cryptographic operation (2:SHA-2)					x	x	
FCS_COP.1	Cryptographic operation (3:ECC)					x	x	
FCS_RNG.1	Random number generation					x	x	
FIA_UAU.1	Timing of authentication (1)				x			
FPT_TDC.1	Inter-TSF basic TSF data consistency (1)					x		
FTP_ITC.1	Inter-TSF trusted channel (1)					x		
FCS_CKM.1	Cryptographic key generation (2)					x	x	
FCS_CKM.2	Cryptographic key distribution (2)					x	x	
FCS_CKM.4	Cryptographic key destruction (2)					x	x	
FCS_COP.1	Cryptographic operation (4:TDES)					x	x	
FCS_COP.1	Cryptographic operation (5:RSA)					x	x	
FCS_COP.1	Cryptographic operation (6:SHA-1)					x	x	
FIA_UAU.1	Timing of authentication (2)				x			
FPT_TDC.1	Inter-TSF basic TSF data consistency (2)					x		
FTP_ITC.1	Inter-TSF trusted channel (2)					x		

Table 13 - Coverage of security objectives for the TOE by SFRs

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

Security Objective	SFR	Rationale
O.Card_Identification_Data	FAU_ARP.1 FAU_SAA.1	In the case of a detected integrity error the TOE will indicate the corresponding violation.
	FDP_ACC.2 FDP_ACF.1	Access to TSF data, especially to the identification data, is regulated by the security function policy defined in the

Security Objective	SFR	Rationale
		components FDP_ACC.2 and FDP_ACF.1, which explicitly denies write access to personalised identification data.
	FDP_SDI.2	Integrity of the stored data within the TOE, specifically the integrity of the identification data, is required by this component.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of identification data.
	FPT_FLS.1	Requires that any failure state should not expose identification data, or compromise its integrity.
	FPT_PHP.3	Requires the TOE to resist attempts to access identification data through manipulation or physical probing.
	FPT_TST.1	Requires tests to be carried out to assure that the integrity of the identification data has not been compromised.
O.Card_Activity_Storage	FAU_ARP.1 FAU_SAA.1	In the case of a detected integrity error the TOE will indicate the corresponding violation.
	FDP_ACC.2 FDP_ACF.1	Access to card activity data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units.
	FDP_SDI.2	Integrity of the stored data within the TOE, specifically the integrity of the card activity data, is required by this component.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of card activity data.
	FPT_FLS.1	Requires that any failure state should not expose card activity data, or compromise its integrity.
	FPT_PHP.3	Requires the TOE to resist attempts to access card activity data through manipulation or physical probing.
	FPT_TST.1	Requires tests to be carried out to assure that the integrity of card activity data has not been compromised.
O.Protect_Secret	FDP_ACC.2 FDP_ACF.1	Require that the TOE prevent access to secret keys other than for the TOE's cryptographic operations.
	FDP_RIP.1	Requires the secure management of storage resources within the TOE to prevent data leakage.
	FPR_UNO.1	This requirement safeguards the unobservability of secret keys used in cryptographic operations.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the confidentiality of the keys.
	FPT_PHP.3	Requires the TOE to resist attempts to gain access to the keys through manipulation or physical probing.
O.Data_Access	FDP_ACC.2 FDP_ACF.1	Access to user data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorised vehicle units.
	FIA_AFL.1(1:C) FIA_AFL.1(1:WC)	These components require that if authentication fails the TOE reacts with a warning to the connected entity, and the user is assumed not to be an authorised vehicle unit.

Security Objective	SFR	Rationale
	FIA_ATD.1 FIA_USB.1	The definition of user security attributes supplies a distinction between vehicle units and other card interface devices.
	FIA_UAU.1(1&2) FIA_UID.2	These requirements ensure that write access to user data is not possible without a preceding successful authentication process.
	FIA.UAU.3	Prevents the use of forged credentials during the authentication process.
	FPT_EMS.1	Requires the TOE to limit emanations, thereby protecting the authentication process.
	FPT_FLS.1	Requires that any failure state should not allow unauthorised write access to the card.
	FPT_PHP.3	Requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.
	FPT_TST.1	Requires that tests be carried out to assure that the integrity of the TSF and identification data has not been compromised.
O.Secure_Communications	FAU_ARP.1 FAU_SAA.1	During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will provide a warning to the entity sending the data.
	FDP_ACC.2 FDP_ACF.1	The necessity for the use of a secure communication protocol as well as the access to the relevant card´s keys are defined within these requirements.
	FDP_ETC.1 FDP_ITC.1 FTP_ITC.1(1&2)	These requirements provide for a secure data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel. This includes assured identification of its end points and protection of the data transfer from modification and disclosure. By this means, both parties are capable of verifying the integrity and authenticity of received data. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device.
	FCO_NRO.1 FDP_DAU.1 FDP_ETC.2	Within the TOE's end-usage phase, the TOE offers a data download functionality with specific properties. The TOE provides the capability to generate an evidence of origin for the data downloaded to the external media, to verify this evidence of origin by the recipient of the data downloaded, and to download the data to external media in such a manner that the data integrity can be verified.
	FDP_RIP.1	Requires the secure management of storage resources within the TOE to prevent data leakage.
	FIA_UAU.3 FIA_UAU.4	These requirements support the security of the trusted channel, as the TOE prevents the use of forged authentication data, and as the TOE's input for the authentication tokens and for the session keys within the preceding authentication process is used only once.

Security Objective	SFR	Rationale
	FPR_UNO.1	This requirement safeguards the unobservability of the establishing process of the trusted channel, and the unobservability of the data exchange itself, both of which contribute to a secure data transfer.
	FCS_CKM.1(1&2) FCS_CKM.2(1&2) FCS_CKM.4(1&2) FCS_COP.1(all) FCS_RNG.1	The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys. FCS_COP.1 also realizes the securing of the data exchange itself. Random numbers are generated in support of cryptographic key generation for authentication.
	FPT_TDC.1(1&2)	Requires a consistent interpretation of the security related data shared between the TOE and the card interface device.
O.Crypto_Implement	FDP_DAU.1 FDP_SDI.2	Approved cryptographic algorithms are required for digital signatures in support of data authentication.
	FIA_UAU.3 FIA_UAU.4	Approved cryptographic algorithms are required to prevent the forgery, copying or reuse of authentication data.
	FCS_CKM.1(1&2) FCS_CKM.2(1&2) FCS_CKM.4(1&2) FCS_RNG.1	Key generation, distribution and destruction must be done using approved methods. Random numbers are generated in support of cryptographic key generation for authentication.
	FCS_COP.1(all)	Approved cryptographic algorithms are required for all cryptographic operations.
O.Software_Update[15]	FDP_ACC.2 FDP_ACF.1	Require that users cannot update TOE software.
	FDP_ITC.2	Provides verification of imported software updates.
	FPT_PHP.3	Requires the TOE to resist physical attacks that may be aimed at modifying software.

Table 14 - Suitability of the SFRs

7.2.3 Security assurance requirements rationale

79 The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [5] Annex 1C, Appendix 10.

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

15 Note that if software update is implemented for the TOE then the mapping provided here will need to be augmented appropriately.

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

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

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

84 The augmentation of EAL4 chosen comprises the following assurance components:

– ATE_DPT.2 and
– AVA_VAN.5.

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

Component	Dependencies required by CC Part 3	Dependency satisfied by
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 15 - SARs' dependencies (additional to EAL4 only)

7.2.4 Security requirements – internal consistency

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

a) SFRs

87 The dependency analysis in section 7.2.1 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

88 All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items. The current PP accurately reflects the requirements of

EU Parliament and Council Regulation 165/2014, Annex I C, which is assumed to be internally consistent.

b) SARs

89 The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the assurance components in section 7.2.3 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

90 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 7.2.1 and 7.2.3. Furthermore, as also discussed in section 7.2.3, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

8 Glossary and Acronyms

8.1 Glossary

Glossary Term	Definition
Activity data	Activity data include events data and faults data for all card types and specific data depending on card type, such as control activity data for control cards, driver activity, vehicles used and places for driver cards and company activity data for company cards. For a full definition, see [5] Annex 1C, Appendix 2 Activity data are part of User Data.
Application note	Informative part of the PP containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE.
Attacker	A person or a process trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained.
Authentication	A function intended to establish and verify a claimed identity.
Authentication data	Data used to support verification of the identity of an entity.
Authenticity	The property that information is coming from a party whose identity can be verified.
Calibration	Updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Member State) and vehicle characteristics (w, k, l, tyre size, speed limiting device setting (if applicable), current UTC time, current odometer value); during the calibration of a recording equipment, the types and identifiers of all type approval relevant seals in place shall also be stored in the data memory. Any update or confirmation of UTC time only, shall be considered as a time adjustment and not as a calibration. Calibration of a recording equipment requires the use of a workshop card.
Card identification data	The following elements stored on the TOE, as defined in [5] Annex 1C, Appendix 1 and Appendix 2: typeOfTachographCardId, cardIssuingMemberState, cardNumber, cardIssuingAuthorityName, cardIssueDate, cardValidityBegin, cardExpiryDate
Company card	A tachograph card issued by the authorities of a Member State to a transport undertaking needing to operate vehicles fitted with a tachograph, which identifies the transport undertaking, and allows for the displaying, downloading and printing of the data, stored in the tachograph, which have been locked by that transport undertaking.

Glossary Term	Definition
Control card	A tachograph card issued by the authorities of a Member State to a national competent control authority that identifies the control body and, optionally, the control officer. It allows access to the data stored in the data memory or in the driver cards and, optionally, in the workshop cards for reading, printing and/or downloading. It also gives access to the roadside calibration checking function, and to data on the remote early detection communication reader.
Data memory	An electronic data storage device built into the tachograph card.
Digital Signature	Data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data.
Downloading	The copying, together with the digital signature, of a part, or of a complete set, of data files recorded in the data memory of the vehicle unit or in the memory of a tachograph card, provided that this process does not alter or delete any stored data.
Driver card	A tachograph card, issued by the authorities of a Member State to a particular driver that identifies the driver and allows for the storage of driver activity data.
European Root Certification Authority (ERCA)	An organisation responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment (TP.360) Via E. Fermi, 1 I-21020 Ispra (VA)
Event	An abnormal operation detected by the smart tachograph that may result from a fraud attempt.
External GNSS Facility	A facility that contains the GNSS receiver when the vehicle unit is not a single unit as well as other components needed to protect the communication of position data to the rest of the vehicle unit.
Fault	An abnormal operation detected by the smart tachograph that may arise from an equipment malfunction or failure.
Human user	A legitimate user of the TOE, being a driver, controller, workshop or company. A user is in possession of a valid tachograph card.
Integrity	The property of accuracy and completeness of information.

Glossary Term	Definition
Intelligent Dedicated Equipment	Equipment used to download data from a Tachograph card to external storage media.
Interface	A facility between systems that provides the media through which they can connect and interact.
Interoperability	The capacity of systems and the underlying business processes to exchange data and to share information.
Manufacturer	The generic term for a manufacturer producing and completing the Tachograph Card as the TOE.
Member State Authority (MSA)	Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA). The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself. Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
Member State Certification Authority (MSCA)	An organisation established by a Member State Authority, responsible for implementation of the MSA policy and for signing certificates for public keys to be inserted into tachograph cards.
Motion Sensor	A part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled.
Personal Identification Number (PIN)	A secret password necessary for using a workshop card and only known to the approved workshop to which that card is issued.
Personalisation	The process by which the equipment-individual data are stored in and unambiguously, inseparably associated with the related equipment.
Registering member state	The Member State of the European Union in which the vehicle is registered. This is represented by a numeric code (see [5] Annex 1C, Appendix 1, Chapter 2.101).
Remote Early Detection Communication	Communication between the remote early detection communication facility and the remote early detection communication reader during targeted roadside checks with the aim of remotely detecting possible manipulation or misuse of recording equipment.

Glossary Term	Definition
Remote Communication Facility	The equipment of the vehicle unit that is used to perform targeted roadside checks.
Remote Early Detection Communication Reader	A system used by control officers for targeted roadside checks of vehicle units, using a DSRC connection.
Secret key	A symmetric or private asymmetric key.
Security Certification	Process to certify, by a Common Criteria certification body, that the tachograph card fulfils the security requirements defined in the relevant Protection Profile.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys and certificates). Security data includes the Sensor Installation Data on a workshop card, see [5] Annex 1C, Appendix 2.
Self Test	Tests run cyclically and automatically by the recording equipment to detect faults.
Smart Tachograph System	The recording equipment, tachograph cards and the set of all directly or indirectly interacting equipment during their construction, installation, use, testing and control, such as cards, remote early detection communication reader and any other equipment for data downloading, data analysis, calibration, generating, managing or introducing security elements, etc.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]). In the context of this PP, the term security data is also used.
User	A human user or connected IT entity.
User identification data	The following data elements stored on the TOE, as defined in Annex IC [5] Appendix 2 and Appendix 1: For driver cards: holderSurname, holderFirstNames, cardHolderBirthDate, cardHolderPreferredLanguage, drivingLicenceIssuingAuthority, drivingLicenceIssuingNation, drivingLicenceNumber. For workshop cards: workshopName, workshopAddress, holderSurname, holderFirstNames, cardHolderPreferredLanguage. For control cards: controlBodyName, controlBodyAddress, holderSurname, holderFirstNames, cardHolderPreferredLanguage. For company cards: companyName, companyAddress, cardHolderPreferredLanguage

Glossary Term	Definition
User Data	Any data, other than security data, recorded or stored by the Tachograph Card. User data include card identification data, user identification data and activity data. The CC gives 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 [1]). • 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 [2]).
Vehicle Unit	The tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of this Regulation; the vehicle unit includes, among other things, a processing unit, a data memory, a time measurement function, two smart card interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user's inputs.
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.
Workshop Card	A tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the user and allows for the testing, calibration and activation of tachographs, and/or downloading from them.

8.2 Acronyms

AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
CC	Common Criteria
DES	Data Encryption Standard (see FIPS PUB 46-3)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EGF	External GNSS Facility
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
GNSS	Global Navigation Satellite System
MAC	Message Authentication Code

MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
OSP	Organisational Security Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
TSF	TOE Security Functionality
VRN	Vehicle Registration Number
VU	Vehicle Unit

9 Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 4: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

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

Digital tachograph: directives and standards

[5] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

[6] Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex 1B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)

Other standards

[7] A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011

Protection profile

[8] Security IC Platform Protection Profile with Augmentation Packages, European Smart Card Industry Association (EUROSMART), Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014

10 Annex A – Key & Certificate Tables

91 This annex provides details of the cryptographic keys and certificates required by the tachograph cards during their lifetime, and to support communication with 1st and 2nd generation vehicle units.

Table 16	- First-generation asymmetric keys generated, used or stored by tachograph cards
Table 17	- First-generation symmetric keys generated, used or stored by tachograph cards
Table 18	- First-generation certificates used or stored by tachograph cards
Table 19	– Second-generation asymmetric keys generated, used or stored by tachograph cards
Table 20	- Second-generation symmetric keys generated, used or stored by tachograph cards
Table 21	- Second-generation certificates used or stored by tachograph cards

92 In general, a tachograph card will not be able to know when it has reached end of life. This is because it is not powered and has no internal clock. Thus, the card will not be able to make permanent secret keys unavailable as indicated in the following tables. Therefore, doing so, if feasible, is a matter of organisational policy

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
Card.SK	Card private key	Used by the card to perform card authentication towards vehicle units and for signing downloaded data files	RSA	Generated by card or card manufacturer at the end of the manufacturing phase	See section 6.1.2.1.1 if done by card. Otherwise, not in scope of this PP.	Made unavailable when the card has reached end of life	Card non-volatile memory
EUR.PK	Public key of ERCA	Used by card to perform verification of MS certificates presented by (foreign) VUs during mutual authentication. See also notes for EUR.KID in Table 18.	RSA	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for this PP	Not applicable	Card non-volatile memory
VU.PK (conditional, possibly multiple)	VU public key	Used by card to perform VU authentication; see also notes for VU.C contents in Table 18.	RSA	Generated by VU or VU manufacturer; obtained by card in VU certificate during mutual authentication	Out of scope for this PP	Not applicable	Card non-volatile memory
MS.PK (conditional, possibly multiple)	Public key of an MSCA other than the MSCA responsible for signing the card certificate	Used by card to perform verification of VU certificates signed by this (foreign) MSCA. See also notes for MS.C contents in Table 18.	RSA	Generated by (foreign) MSCA; obtained by card in MS certificate presented by a VU during mutual authentication	Out of scope for this PP	Not applicable	Card non-volatile memory

Table 16 - First-generation asymmetric keys generated, used or stored by tachograph cards

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
	Secure Messaging	Session key for data protection between card and a VU during a	TDES	Agreed between card and VU during mutual authentication	See section 6.1.3.1.1	Made unavailable when the Secure Messaging	Not permanently

	session key	Secure Messaging session				session is aborted	stored
K_{M-WC} (workshop cards only)	Motion sensor master key – workshop card part	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU	TDES	Generated by ERCA; inserted in card by card manufacturer. Note: See [5] Annex 1C, Appendix 11, CSM_105.	Out of scope for this PP	Made unavailable when the card has reached end of life	Card non-volatile memory

Table 17 - First-generation symmetric keys generated, used or stored by tachograph cards

Certificate Symbol	Description	Purpose	Source	Stored in	Note
Card.C	Card certificate for signing and Mutual Authentication	Used by VUs or IDE to obtain and verify the Card.PK they will subsequently use to perform card authentication or verification of signatures created by the card	Created and signed by MSCA based on card manufacturer input; inserted by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	
MS.C	Certificate of MSCA responsible for signing card certificate	Used by VUs or IDE to obtain and verify the MS.PK they will subsequently use to verify the Card.C	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	
VU.C contents (conditional, possibly multiple)	CHR and other VU certificate contents	If a card has verified a VU certificate before, it may store the public key (see Table 16), the CHR and possibly the validity period and other data in order to authenticate that VU again in the future	Created and signed by MSCA based on VU manufacturer input; inserted in VU by VU manufacturer; obtained and stored by card during a previous successful VU authentication.	Card general non-volatile memory	Presence in card is conditional; only if card is designed to store VU certificate contents for future reference and has encountered VUs in the past. The card may store the contents of multiple VU.C.
MS.C contents (conditional, possibly multiple)	CHR and other MS certificate contents	If a VU has verified a MS certificate before, it may store the public key (see Table 16), the CHR and possibly the validity period and other data in order to verify card certificates based on that MS certificate in the future	Created and signed by ERCA based on MSCA input, inserted in VU by VU manufacturer; obtained and stored by card after successful verification during a previous mutual authentication process with a	Card general non-volatile memory	Presence in card is conditional; only if card is designed to store MS certificate contents for future reference and has encountered VUs containing a foreign MS certificate in the past. The

			(foreign) VU.		card may store the contents of multiple MS.C.
EUR.KID	Key Identifier for public key of ERCA	This identifier will be used by VUs to reference the European root public key	Inserted in card by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	

Table 18 - First-generation certificates used or stored by tachograph cards

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
Card_MA.SK	Card private key for Mutual Authentication and session key agreement	Used by the card to perform card authentication towards VUs and perform session key agreement	ECC	Generated by card or card manufacturer at the end of the manufacturing phase	See section 6.1.2.1.1 if done by card. Otherwise, not in scope of this PP.	Made unavailable when the card has reached end of life	Card non-volatile memory
Card_Sign.SK (driver cards and workshop cards only)	Card private key for signing	Used by the card to sign downloaded data files.	ECC	Generated by card or card manufacturer at the end of the manufacturing phase	See section 6.1.2.1.1 if done by card. Otherwise, not in scope of this PP.	Made unavailable when the card has reached end of life	Card non-volatile memory
EUR.PK (current)	The current public key of ERCA (at the time of issuing of card)	Used by the card for the verification of MSCA certificates issued under the current ERCA root certificate. See also notes for EUR.C (current) contents in Table 21.	ECC	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for this PP	Not applicable	Card non-volatile memory
EUR.PK (previous) (conditional; only present if existing at time of card	The previous public key of ERCA (at the time of issuing of card)	Used by the card to verify MSCA certificates issued under the previous ERCA root certificate. See also notes for EUR.C	ECC	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for this PP	Not applicable	Card non-volatile memory

issuance)		(previous) contents in Table 21.					
EUR.Link.PK (conditional; only if the card has successfully authenticated a next-generation VU)	The public key of ERCA following the public key that was current at the time of issuing of the card	Used by the card to verify MSCA certificates issued under the next ERCA root certificate. Note that EUR.Link.PK is the same as the next EUR.PK. See also Application note 19: and notes for EUR.Link.C contents in Table 21.	ECC	Generated by ERCA; inserted by manufacturer in a VU issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by card during mutual authentication towards such a VU.	Out of scope for this PP	Not applicable	Card non-volatile memory
VU_MA.PK (conditional, possibly multiple)	VU public key for Mutual Authentication	Used by card to perform VU authentication and session key agreement. See also notes for VU_MA.C contents in Table 21	ECC	Generated by VU or VU manufacturer; obtained by card in VU_MA certificate during mutual authentication	Out of scope for this PP	Not applicable	Card non-volatile memory
MSCA_VU-EGF.PK (conditional, possibly multiple)	Public key of MSCA responsible for signing VU certificates	Used by card to verify the certificate of a VU signed by this (foreign) MSCA. See also notes for MSCA_VU-EGF.C contents in Table 21	ECC	Generated by MSCA ; obtained by card in MSCA_VU-EGF certificate during mutual authentication	Out of scope for this PP	Not applicable	Card non-volatile memory

Table 19 – Second-generation asymmetric keys generated, used or stored by tachograph cards

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and time	Stored in
$K_{M\text{-}WC}$ (workshop cards only)	Motion sensor master key – workshop card part	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU	AES	Generated by ERCA; inserted in card by card manufacturer. Note: as explained in [5] Annex 1C, Appendix 11, section 12.2, a workshop card may contain up to three keys	Out of scope for this PP	Made unavailable when the card has reached end of life	Card non-volatile memory

				K_{M-WC} (of consecutive key generations).			
K_{MAC}	Secure Messaging session key for authenticity	Session key for authenticity between card and a VU during a Secure Messaging session	AES	Agreed between card and VU during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted[16]	Not permanently stored
K_{ENC}	Secure Messaging session key for confidentiality	Session key for confidentiality between card and a VU during a Secure Messaging session	AES	Agreed between card and VU during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored
KM_{DSRC}	DSRC Master key	Master key to derive keys to protect confidentiality and authenticity of data sent from a VU to a control authority over a DSRC channel	AES	Generated by ERCA Note: Workshop and control cards may contain up to 3 KM_{DSRC} keys	Out of scope for this PP	Made unavailable when the card has reached end of life	Card non-volatile memory (control and workshop cards only)

Table 20 - Second-generation symmetric keys generated, used or stored by tachograph cards

Certificate Symbol	Description	Purpose	Source	Stored in	Note
Card_MA.C	Card certificate for Mutual Authentication and session key agreement	Used by VU to obtain and verify the Card_MA.PK they will subsequently use to perform card authentication.	Created and signed by MSCA based on card manufacturer input; inserted by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	
Card_Sign.C (driver cards and workshop	Card certificate for signing	Used by IDE to obtain and verify the Card_Sign.PK they will subsequently use to verify the	Created and signed by MSCA based on card manufacturer input; inserted by manufacturer	Card general non-volatile memory	

16 See [5], Annex 1C, Appendix 11, Section 10.5.3 for details of secure messaging session abortion.

cards only)		signature over a data file signed by the card.	at the end of the manufacturing phase		
MSCA_Card.C	Certificate of MSCA responsible for signing the Card_MA and Card_Sign certificates	Used by a VU or IDE to obtain and verify the MSCA_Card.PK they will subsequently use to verify the Card_MA or Card_Sign certificate.	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	
EUR.Link.C	Link certificate signed by previous EUR.SK (see Application note 19:)	Used by a VU, EGF or IDE issued under the previous ERCA root certificate to obtain and verify the current EUR.PK they will subsequently use to verify the MSCA_Card certificate.	Created and signed by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	Presence in card is conditional; only if a previous ERCA root certificate existed at the moment of card manufacturing
EUR.C (current) contents	CHR and other contents of current European root certificate	This CHR will be referenced by VUs issued under the current European root public key (see Table 19). The card may store the validity period and other certificate data as well.	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	
EUR.C (previous) contents	CHR and other contents of previous European root certificate	This CHR will be referenced by cards and EGFs issued under the previous European root public key (see Table 19). The card may store the validity period and other certificate data as well.	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Card general non-volatile memory	Presence in card is conditional; only if a previous ERCA root certificate existed at the moment of card manufacturing
EUR.Link.C contents	CHR and other contents of next European root certificate	This CHR will be referenced by VUs issued under the next European root public key (see). The card may store the validity period and other certificate data as well.	Generated by ERCA; inserted by manufacturer in a VU issued under the next generation of EUR.C as part of the EUR.Link.C; obtained and stored by card during mutual authentication towards such VU	Card general non-volatile memory	Presence in card is conditional; only if the card has successfully authenticated a next-generation VU
VU_MA.C contents	CHR and other contents of VU	If a card has verified a VU_MA certificate before, it may store the	Created and signed by MSCA based on VU manufacturer	Card general non-volatile memory	Presence in card is conditional; only if card is designed to store

	certificate for Mutual Authentication	public key (see Table 19), the CHR and possibly the validity period and other data in order to authenticate that VU again in the future	input; inserted in VU by VU manufacturer; obtained and stored by card during mutual authentication after successful verification.		VU certificate contents for future reference and has encountered VUs in the past. The card may store the contents of multiple VU_MA.C.
MSCA_VU-EGF.C contents	CHR and other contents of certificate of MSCA responsible for signing VU certificates	If a card has verified a MSCA certificate before, it may store the public key (see Table 19), the CHR and possibly the validity period and other data in order to verify VU certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in VU by VU manufacturer; obtained and stored by card after successful verification during a previous mutual authentication process with a VU.	Card general non-volatile memory	Presence in card is conditional; only if card is designed to store VU certificate contents for future reference and has encountered VUs in the past. The card may store the contents of multiple MSCA_VU.C, e.g. different MSCAs and/or generations.

Table 21 - Second-generation certificates used or stored by tachograph cards

Application note 19: During its lifetime, a tachograph card can be confronted with two different link certificates:

- If at the time of issuance of the card, there are VUs in the field that are issued under a previous EUR.C, then the card shall be issued with both the previous EUR.C and an EUR.Link.C signed with the previous EUR.SK. The card will need the first one to check the authenticity of the old VUs. The card will need the second one to prove its authenticity towards old VUs.
- If, after the issuance of the card, a new EUR.C is generated and VUs are issued under this new root certificate, then such a new VU will present the card with an EUR.Link.C signed by the current EUR.SK to prove its authenticity. The card can check this certificate with its current EUR.PK. If correct, the card may store the EUR.Link.PK as a new trust point.

11 Annex B – Operations for FCS_RNG.1

93 This annex provides further information on the use of FCS_RNG.1 and FCS_CKM.1(1) in compliant security targets. The security target author should select one of these classes, as appropriate to the TOE, to complete the selection in FCS_CKM.1(1), and should complete the operations in FCS_RNG.1 correspondingly. Further information on the application of these classes can be found in [7].

11.1 Class PTG.2

94 Functional security requirements of the class PTG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.2)

FCS_RNG.1.1 The TSF shall provide a [physical] random number generator that implements:

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [*selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered [*selection: externally, at regular intervals, continuously, applied upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2 The TSF shall provide [*selection: bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet:

(PTG.2.6) Test procedure A[17] [*assignment: additional standard test suites*] does not distinguish the internal random numbers from output sequences of an ideal RNG.

17 See [7] Section 2.4.4.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

11.2 Class PTG.3

95 Functional security requirements of the class PTG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.3)

FCS_RNG.1.1 The TSF shall provide a [hybrid physical] random number generator that implements:

(PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [*selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered [*selection: externally, at regular intervals, continuously, upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

FCS_RNG.1.2 The TSF shall provide [*selection: bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet:

(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A[13] [*assignment: additional test suites*].

(PTG.3.8) The internal random numbers shall [*selection: use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work*]].

11.3 Class DRG.2

96 Functional security requirements of the class DRG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.2)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

(DRG.2.1) If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].

(DRG.2.2) The RNG provides forward secrecy.

(DRG.2.3) The RNG provides backward secrecy.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.2.4) The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.2.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[13] [*assignment: additional test suites*].

11.4 Class DRG.3

97 Functional security requirements of the class DRG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.3)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

(DRG.3.1) If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[13] [*assignment: additional test suites*].

11.5 Class DRG.4

98 Functional security requirements of the class DRG.4 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.4)

FCS_RNG.1.1 The TSF shall provide a [hybrid deterministic] random number generator that implements:

(DRG.4.1) The internal state of the RNG shall [*selection: use PTRNG of class PTG.2 as random source, have [assignment: work factor], require [assignment: guess work]*].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy [*selection: on demand, on condition [assignment: condition], after [assignment: time]*].

(DRG.4.5) The internal state of the RNG is seeded by an [*selection: internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3, [other selection]*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.4.6) The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[13] [*assignment: additional test suites*].

11.6 Class NTG.1

99 Functional security requirements of the class NTG.1 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class NTG.1)

FCS_RNG.1.1 The TSF shall provide a [non-physical true] random number generator that implements:

(NTG.1.1) The RNG shall test the external input data provided by a non-physical entropy source in order to estimate the entropy and to detect non-tolerable statistical defects under the condition [*assignment: requirements for NPTRNG operation*].

(NTG.1.2) The internal state of the RNG shall have at least [*assignment: Min-entropy*]. The RNG shall prevent any output of random numbers until the conditions for seeding are fulfilled.

(NTG.1.3) The RNG provides backward secrecy even if the current internal state and the previously used data for reseeding, resp. for seed-update, are known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

NTG.1.4) The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(NTG.1.5) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A[13] [*assignment: additional test suites*].

(NTG.1.6) The average Shannon entropy per internal random bit exceeds 0.997.