MASKTECH

Security Target

COMMON CRITERIA DOCUMENTS | Version 1.2

MTCOS Smart Tachograph V2 / SLE78CFX4000P

Digital Tachograph – Tachograph Card

Certification-ID: BSI-DSZ-CC-1088

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 ST Introduction (ASE_INT.1)

This section provides overview information to enable a potential user of this Security Target (ST) to determine, whether the ST is of interest. [REG_2016/799, REG_2021/1228] Annex 1C requirements not included in this ST are not the subject of security certification.

1.1 ST Reference

Title	Security Target – MTCOS Smart Tachograph V2 / SLE78CFX4000P
Version number	1.2
Issue date	2022-04-06
Author	MaskTech International GmbH
Registration	BSI-DSZ-CC-1088
CC reference	3.1 (Revision 5)
Compliant to	Common Criteria Protection Profile: Digital Tachograph – Tachograph Card (TC PP) [CC_PP-0091]
Assurance level	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
TOE name	MTCOS Smart Tachograph V2 / SLE78CFX4000P
TOE hardware	Infineon Technologies AG, SLE78CFX4000P (M7892), contact-based Smartcard IC
TOE version	MTCOS Pro 2.5
Keywords:	Digital Tachograph, Tachograph Card

1.2 TOE Overview

MTCOS Smart Tachograph V2 / SLE78CFX4000P provides the Tachograph Card application according [REG_2016/799, REG_2018/502][1] (driver card, workshop card, company card and control card) based on the MTCOS Pro operating system. MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to [ISO_7816]. It provides public and secret key cryptography and supports also other applications like ePassports, e-purses, health insurance cards and access control. The operating system software is implemented

[1] Note that the consolidated [REG_2016/799] includes [REG_2018/502], thus the latter is not cited explicitly in the following.

on the SLE78CFX4000P (M7892) secure contact-based controller of Infineon Technologies AG (BSI-DSZ-CC-0782-V5 [IFX_ST-SLE78-B11]). Chip and cryptographic library are certified according to CC EAL6 augmented compliant to the Protection Profile BSI-CC-PP-0035-2007 [CC_PP-0035]. The TOE consists of software and hardware.

1.2.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) addressed by this ST is a second generation Tachograph Card in the sense of [REG_2016/799] 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. The TOE is a smart card that comprises:

a) The circuitry of the chip SLE78CFX4000P (M7892), including all IC dedicated software being active in the operational phase of the TOE (the integrated circuit, IC);
b) The IC Embedded Software (operating system);
c) The 2 tachograph applications (1st and 2nd generation);
d) The administration-scripts (configuration of card type); and
e) The associated guidance documentation [AGD].

The basic functions of the TOE 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.

The TOE 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 the card reader has the appropriate access rights.

Concerning write access, during the end-usage phase of a Tachograph Card life cycle (as described in section 1.2.4), only Vehicle Units may write user data to the card.

The functional requirements for a Tachograph Card are specified in [REG_2016/799, REG_2021/1228] 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

The Tachograph Card is viewed as unit of

the physical part in form of the chip embedded into a plastic card with visual readable data (depending on the card type) printed on the card.

the logical part as data stored according [REG_2016/799, REG_2021/1228] on the chip; security features and services provided are described in this section.

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 personalization 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.

Specifically the Tachograph Card aims to protect:

a) The data that is stored in such a way as to prevent unauthorized 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.

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 [REG_2016/799] Annex 1C, Appendix 11.

All cryptographic mechanisms, including algorithms and the length of corresponding keys, are implemented exactly as required and defined in [REG_2016/799] Annex 1C, Appendix 11, Part B for second generation mechanisms, and in [REG_2016/799] 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 to be downloaded to external media;
b) Workshop cards - PIN verification, verification of MACs over Remote Tachograph Monitoring data and decryption of such data, creation of signatures over data to be downloaded to external media 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.

Note 1: 1st generation VU (compliant with Annex I B [REG_2002/1360]) will not have to be replaced, following the application of the new [REG_2016/799] Annex 1C. They will continue to be used in the field, until their end of life. 2nd generation VU (compliant with [REG_2016/799] 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 [REG_2016/799].

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).

MTCOS Smart Tachograph V2 / SLE78CFX4000P is interoperable with both Digital Tachograph Systems. It contains 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 [REG_2016/799, REG_2021/1228] 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 the card information, the chip information 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 the card information, the chip information 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

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 [REG_2016/799, REG_2021/1228] 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: Organization, security and commands for interchange
   v) Part 8: Commands and mechanisms for security operations;

c) ISO/IEC 10373 Identification cards - Test methods.

1.2.4 TOE Life Cycle and Boundary

Because the lot sizes of workshop cards, company cards and control cards are significantly less that those of driver cards, the life cycle step of the driver card and of the workshop, company or control card differ with regard to the **initialization step**. For the driver card, it is performed in life cycle phase **development**. For workshop, company or control cards *administration scripts* to convert the driver card file system are provided that must be applied by the Administrator before the personalization step but after delivery, thus the initialization step is part of life cycle phase **operational use**. Table 1.1 gives an overview of the life cycle phases of the TOE. The steps are adapted from the typical smart card product life cycle as e.g. described in [CC_PP-0084].

TOE life cycle phase	Step	Description
Development	* Smart Card Embedded Software Development * IC Design and IC Dedicated Software Development * IC Manufacturing * IC Packaging and Testing * Smart Card Product Finishing Process (conditionally) * Personalization (initialization)	TOE development at Infineon Technologies AG and MASKTECH INTERNATIONAL GMBH and production at Infineon Technologies AG. TOE initialization (driver card) at Infineon Technologies AG.
Delivery	–	Delivery from Infineon Technologies AG to the issuing authority.
Operational use	* Smart Card Product Finishing Process (conditionally) * Personalization (initialization; conditionally) * Personalization (personalization) * End-usage	TOE initialization (workshop, company and control cards only) and personalization of the TOE. End-usage as Tachograph Card.

Table 1.1: Life cycle phases and steps.

Development In this phase the IC and the IC dedicated software are developed by Infineon Technologies AG, the embedded software (operating system) and the Tachograph Card application software are developed by MASKTECH INTERNATIONAL GMBH. This phase also includes the IC manufacturing, packaging and testing at Infineon Technologies AG.

The loading of dedicated, embedded and application software (driver card) is performed at Infineon Technologies AG and covered by the IC hardware evaluation (BSI-DSZ-CC-0782-V5 [IFX_ST-SLE78-B11]). The Flash Loader has been deactivated permanently before delivery.

Delivery The TOE is securely delivered as an initialized module from Infineon Technologies AG to the issuing authority or the party acting on behalf of it. Note that the embedding of the chip into the plastic card takes place after delivery and is beyond the scope of the certification.

Operational use

- Personalization: Conditionally, the application software is configured (workshop, company or control cards only) and the user identification data and cryptographic keys are written by the issuing authority or the party acting on behalf of it.
- End-usage: The personalized Tachograph Card is handed over to the end-user. Write access is restricted to the Vehicle Unit as specified in [REG_2016/799, REG_2021/1228].

1.2.5 Non-TOE Hardware/Software/Firmware

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

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

2 Conformance Claims (ASE_CCL.1)

2.1 CC Conformance Claim

This ST claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 [CC_Part1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 [CC_Part2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 [CC_Part3]

as follows

- Part 2 extended (with FCS_RNG.1 and FPT_EMS.1)
- Part 3 conformant (EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5)

2.2 PP Claim

This ST claims strict conformance to the Common Criteria Protection Profile “Digital Tachograph – Tachograph Card (TC PP)” [CC_PP-0091].

2.3 PP Additions

The personalization of the TOE is performed after delivery, thus the according SFRS had been added in addition to those included in [CC_PP-0091]. These can be taken from Table 6.1, page 25.

2.4 Package Claim

The assurance level for the TOE is CC EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 defined in [CC_Part3].

2.5 Conformance Claim Rationale

According section 2.2 this ST claims strict conformance to [CC_PP-0091]. Table 2.1 gives an overview of the components.

Assurance Component	See section	Corresponding section in [CC_PP-0091]
ASE_INT.1	1	Chapter 1; the TOE definition (section 1.2.1) complies to the definition of a tachograph card as described in section 1.2.1 of [CC_PP-0091]. For better readability, the TOE life cycle as it is implemented is described in the additional section 1.2.4.
ASE_CCL.1	2	Chapter 2; put for this ST according to section 2.5 of [CC_PP-0091]. Conformance to CC Parts in version 3.1, revision 5 is claimed (revision 4 in [CC_PP-0091])
ASE_SPD.1	3	Chapter 3; no significant changes
ASE_OBJ.2	4	Chapter 4; no significant changes
ASE_ECD.1	5	Chapter 5; no significant changes
ASE_REQ.2	6	Chapter 6; if required, SFRs have been iterated to address the different life cycle phases of the TOE, see Table 6.1. operations done for the SFRs are clearly indicated according to [CC_PP-0091].

Table 2.1: Conformance claim rationale.

3 Security Problem Definition (ASE_SPD.1)

Note 2: Although each of the Tachograph Card types (driver card, workshop card, control card or company card) is used for a different purpose, [CC_PP-0091] and this ST describe 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

The assets to be protected by the TOE and its environment within the **operational use** phase of the TOE's life cycle are the application data defined in the table below[1].

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 3.1: Primary assets to be protected by the TOE and its environment

[1]The security properties to be maintained for each asset are defined in [REG_2016/799, REG_2021/1228] Annex 1C, especially Appendices 2 and 11.

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 authorized 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 authorized 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).
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 personalization.

Table 3.2: Secondary assets to be protected by the TOE and its environment

All primary assets represent user data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF and TSF-data in the sense of the CC. Security data and user data, stored by the Tachograph Card, need to be protected against unauthorized 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

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

No.	Role	Definition
1	Administrator	Active only during operational use phase (initialization and personalization).
2	Vehicle Unit [2]	Vehicle Unit (authenticated[3]), to which the Tachograph Card is connected (S.VU).
3	Other Device[4]	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 [CC_PP-0091], 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 3.3: Subjects and external entities.

Note 3: This table defines the subjects in the sense of [CC_Part1] which can be recognized 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 TOE internal image (also called subject in [CC_Part1]). From this point of view, the TOE itself does not distinguish between "subjects" and "external entities".

3.2 Threats

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

The threats are defined in the following tables.

[2] Tachograph cards may be inserted in 1st generation or 2nd generation Vehicle Units.

[3] Authenticated to the Tachograph Card by the method specified in [REG_2016/799] Annex 1C, Appendix 11, Chapter 4 (for 1 st generation VU) and Chapter 10 (for 2nd generation VU).

[4] 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.

Label	Threat
T.Identification_Data	**Modification of Identification Data** - A successful modification of identification data held by the TOE (IDD, see sec. 3.1.1, 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. 3.1.1), 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. 3.1.1) 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. 3.1.1) 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 3.4: Threats addressed by the TOE.

3.3 Assumptions

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.

The assumptions are provided in the following table.

Label	Assumption
A.Personalization_Phase	**Personalization Phase Security** - All data structures and data on the card produced during the **operational use** phase (initialization and personalization), in particular during initialization and/or personalization are correct according to [REG_2016/799, REG_2021/1228] 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 Personalization Service Provider controls all materials, equipment and information, which is used for initialization and/or personalization of authentic smart cards, in order to prevent counterfeit of the TOE.

Table 3.5: Assumptions.

3.4 Organizational Security Policies

This section shows the organizational security policies that are to be enforced by the TOE, its operational environment, or a combination of the two. The organizational security policies are provided in the following table.

Label	Organizational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [REG_2016/799] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity, authenticity and/or non-repudiation need to be protected.

Table 3.6: Organizational security policies.

4 Security Objectives (ASE_OBJ.2)

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

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 [REG_2016/799, REG_2021/1228] and [REG_2002/1360].

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 personalization 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 [REG_2016/799] Annex 1C, Appendix 11.
O.Software_Update	**Software updates** - Where updates to TOE software are possible, the TOE must accept only those that are authorized. Note that this objective is only listed for completeness; it is not applicable, because no software updates are possible.

Table 4.1: Security objectives for the TOE.

4.2 Security Objectives for the Operational Environment

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.Personalization_Phase	**Secure Handling of Data in Personalization Phase** - All data structures and data on the card produced during the Personalization Phase, in particular during initialization and/or personalization must be correct according to [REG_2016/799, REG_2021/1228] Annex 1C, and must be handled so as to preserve the integrity and confidentiality of the data. The Personalization Service Provider must control all materials, equipment and information that are used for initialization and/or personalization of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalization process must be appropriately secured with the goal of data integrity and confidentiality.
OE.Crypto_Admin	**Implementation of Tachograph Components** - All requirements from [REG_2016/799] 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 4.2: Threats addressed by the operational environment.

5 Extended Components Definition (ASE_ECD.1)

For [CC_PP-0091] the security functional requirements in CC Part 2 have been extended to cover part of the TOE functionality that cannot otherwise clearly be expressed.

[CC_PP-0091] 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 [KiSch-RNG] Chapter 3.

5.1 Class FCS: Cryptographic Support

5.1.1 Generation of Random Numbers (FCS_RNG)

Rationale [CC_Part2] 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 coherent set of SFRs that include the generation of random numbers as a security service can be expressed.

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

Component leveling

FCS_RNG: Generation of random numbers——1

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 There are no management activities foreseen.

Audit: FCS_RNG.1 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: [assignment: *a defined quality metric*].

5.2 Class FPT: Protection of the TSF

5.2.1 TOE Emanation (FPT_EMS)

Rationale 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_Part2].

Family behavior 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

FPT_EMS: TOE emanation —— 1

FPT_EMS.1 TOE emanation requires that the TOE does not produce intelligible emissions that enable access to TSF data or user data.

Management: FPT_EMS.1 There are no management activities foreseen.

Audit: FPT_EMS.1 There are no actions defined to be auditable.

FPT_EMS.1	**TOE emanation**
Hierarchical to:	–
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 (ASE_REQ.2)

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.

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 [CC_Part1]. Each of these operations is used in this ST.

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~~.

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 and appear in square brackets. 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 *italicized*.

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 and appear in square brackets. 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 *italicized*. 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 italicized*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

Note that the denotation of [CC_PP-0091] has been changed for consistency and better readability. Table 6.1 gives an overview of the SFRS used in this ST and the corresponding SFRs from [CC_PP-0091]. SFRs addressing the personalization step have no explicit correspondance in the PP ("– " in columns 3 and 4 of table 6.1).

SFR	Component name	Corresponding SFR in [CC_PP-0091]	
FAU_ARP.1	Security alarms	FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis	FAU_SAA.1	Potential violation analysis

SFR	Component name	Corresponding SFR in [CC_PP-0091]	
FCO_NRO.1	Selective proof of origin	FCO_NRO.1	Selective proof of origin
FDP_ACC.2/Usage	Complete access control (usage)	FDP_ACC.2	Complete access control
FDP_ACF.1/Usage	Security attribute based access control (usage)	FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic data authentication	FDP_DAU.1	Basic data authentication
FDP_ETC.1	Export of user data without security attributes	FDP_ETC.1	Export of user data without security attributes
FDP_ETC.2	Export of user data with security attributes	FDP_ETC.2	Export of user data with security attributes
FDP_ITC.1	Import of user data without security attributes	FDP_ITC.1	Import of user data without security attributes
FDP_ITC.2	Import of user data with security attributes	FDP_ITC.2	Import of user data with security attributes
FDP_RIP.1	Subset residual information protection	FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action	FDP_SDI.2	Stored data integrity monitoring and action
FIA_AFL.1/C	Authentication failure handling (card)	FIA_AFL.1	Authentication failure handling (1:C)
FIA_AFL.1/WC	Authentication failure handling (workshop card)	FIA_AFL.1	Authentication failure handling (2:WC)
FIA_ATD.1/Usage	User attribute definition (usage)	FIA_ATD.1	User attribute definition
FIA_UAU.3	Unforgeable authentication	FIA_UAU.3	Unforgeable authentication
FIA_UAU.4	Single-use authentication mechanism	FIA_UAU.4	Single-use authentication mechanism
FIA_UID.2	User authentication before any action	FIA_UID.2	User authentication before any action
FIA_USB.1/Usage	User-subject binding (usage)	FIA_USB.1	User-subject binding
FPR_UNO.1	Unobservability	FPR_UNO.1	Unobservability
FPT_EMS.1	TOE emanation	FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state	FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack	FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing	FPT_TST.1	TSF testing
FCS_CKM.1/G2	Cryptographic key generation (generation 2)	FCS_CKM.1	Cryptographic key generation (1)
FCS_CKM.2/G2	Cryptographic key distribution (generation 2)	FCS_CKM.2	Cryptographic key distribution (1)

SFR	Component name	Corresponding SFR in [CC_PP-0091]	
FCS_CKM.4/G2	Cryptographic key destruction (generation 2)	FCS_CKM.4	Cryptographic key destruction (1)
FCS_COP.1/AES	Cryptographic operation (AES)	FCS_COP.1	Cryptographic operation (1:AES)
FCS_COP.1/SHA2	Cryptographic operation (SHA-2)	FCS_COP.1	Cryptographic operation (2:SHA-2)
FCS_COP.1/ECC	Cryptographic operation (ECC)	FCS_COP.1	Cryptographic operation (3:ECC)
FCS_RNG.1	Random number generation	FCS_RNG.1	Random number generation
FIA_UAU.1/G2	Timing of authentication (generation 2)	FIA_UAU.1	Timing of authentication (1)
FPT_TDC.1/G2	Inter-TSF basic TSF data consistency (generation 2)	FPT_TDC.1	Inter-TSF basic TSF data consistency (1)
FTP_ITC.1/G2	Inter-TSF trusted channel (generation 2)	FTP_ITC.1	Inter-TSF trusted channel (1)
FCS_CKM.1/G1	Cryptographic key generation (generation 1)	FCS_CKM.1	Cryptographic key generation (2)
FCS_CKM.2/G1	Cryptographic key distribution (generation 1)	FCS_CKM.2	Cryptographic key distribution (2)
FCS_CKM.4/G1	Cryptographic key destruction (generation 1)	FCS_CKM.4	Cryptographic key destruction (2)
FCS_COP.1/TDES	Cryptographic operation (TDES)	FCS_COP.1	Cryptographic operation (4:TDES)
FCS_COP.1/RSA	Cryptographic operation (RSA)	FCS_COP.1	Cryptographic operation (5:RSA)
FCS_COP.1/SHA1	Cryptographic operation (SHA-1)	FCS_COP.1	Cryptographic operation (6:SHA-1)
FIA_UAU.1/G1	Timing of authentication (generation 1)	FIA_UAU.1	Timing of authentication (2)
FPT_TDC.1/G1	Inter-TSF basic TSF data consistency (generation 1)	FPT_TDC.1	Inter-TSF basic TSF data consistency (2)
FTP_ITC.1/G1	Inter-TSF trusted channel (generation 1)	FTP_ITC.1	Inter-TSF trusted channel (2)
FCS_CKM.1/Perso	Cryptographic key generation (personalization)	–	–
FCS_CKM.4/Perso	Cryptographic key destruction (personalization)	–	–
FCS_COP.1/Perso	Cryptographic operation (personalization)	–	–
FDP_ACC.2/Perso	Complete access control (personalization)	–	–

SFR	Component name	Corresponding SFR in [CC_PP-0091]	
FDP_ACF.1/Perso	Security attribute based access control (personalization)	–	–
FIA_AFL.1/Perso	Authentication failure handling (personalization)	–	–
FIA_ATD.1/Perso	User attribute definition	–	–
FIA_USB.1/Perso	User-subject binding (personalization)	–	–

Table 6.1: SFR overview.

6.1 Security Functional Requirements for the TOE

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 [CC_PP-0091] 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. In addition to [CC_PP-0091], section 6.1.4 addresses the requirements for personalization.

6.1.1 Security Functional Requirements for the TC

6.1.1.1 Class FAU Security Audit

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 [REG_2016/799] 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.

Note 4: On user authentication failures and activity data input integrity errors status word SW1 SW2 `66 88` is returned, on self test errors and stored data integrity errors status word SW1 SW2 `6F 00` is returned.

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: *no other rules*].

Note 5: 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

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 [REG_2016/799] 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 [REG_2016/799] Appendix 11, sections 6.2 and 14.3].

Note 6: 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 [REG_2016/799] Appendix 11, sections 6 and 14.

6.1.1.3 Class FDP User Data Protection

FDP_ACC.2/Usage	**Complete access control (usage)**
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Access control functions
FDP_ACC.2.1/Usage	The TSF shall enforce the [AC SFP] on [• Subjects: – S.VU (a Vehicle Unit in the sense of [REG_2016/799] Annex 1C) – S.Non-VU (other card interface devices) • Objects: – User data * User Identification data * Activity data – Security data * Cryptographic keys (see Tables A.1, A.2, A.4 and A.5) * 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/Usage	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/Usage	**Security attribute based access control (usage)**
Hierarchical to:	–
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/Usage

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

- Subjects:
  - S.VU (in the sense of [REG_2016/799] Annex 1C)
  - S.Non-VU (other card interface devices)
- Objects:
  - User data:
    - User identification data
    - Activity data
  - Security data:
    - Cryptographic keys (see Tables A.1, A.2, A.4 and A.5)
    - PIN (for workshop card)
  - TOE application code
  - TOE file system (Attribute: access conditions)
  - Card identification data
  - Master file contents].

FDP_ACF.1.2/Usage

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

- GENERAL_READ
  - Driver card, workshop card: user data may be read from the TOE by any user
  - Control card, company card: user data may be read from the TOE by any user, except 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 personalization
  - 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: TOE application code may only be upgraded following successful authentication
- FILE_STRUCTURE
  - All card types: files structure and access conditions shall be created before personalization is completed and then locked from any future modification or deletion by any user without successful authentication by the party responsible for card initialization].

FDP_ACF.1.3/Usage

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

FDP_ACF.1.4/Usage	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 [REG_2016/799] Annex 1C, Appendix 2].

Note 7: Note that software upgrades in the end-usage phase of the card life cycle are not intended for the TOE.

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

FDP_ETC.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.

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.

[1] In the context of [CC_PP-0091] "validity" means integrity and authenticity.

FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [none].

FDP_ITC.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 initialization
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].

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.
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].

Note 8: The requirement for verified software updates is not applicable, because no software updates are possible.

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: *deallocation of the resource from*] the following objects: [assignment: *cryptographic keys, PINs*].

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
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: *integrity checked stored data*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [warn the entity connected].

Note 9: Integrity checked stored data include cryptographic keys, PINs, user identification data and activity data.

6.1.1.4 Class FIA Identification and Authentication

FIA_AFL.1/C	**Authentication failure handling (card)**
Hierarchical to:	–
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/C	The TSF shall detect when [1] unsuccessful authentication attempts occur related to [authentication of a card interface device].
FIA_AFL.1.2/C	When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [a) warn the entity connected, b) assume the user to be S.Non-VU].

FIA_AFL.1/WC	**Authentication failure handling (workshop card)**
Hierarchical to:	–
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/WC	The TSF shall detect when [5] unsuccessful authentication attempts occur related to [PIN verification of Workshop Card].
FIA_AFL.1.2/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].

FIA_ATD.1/Usage	**User attribute definition (usage)**
Hierarchical to:	–
Dependencies:	–
FIA_ATD.1.1/Usage	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)].

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.

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 [REG_2016/799] Appendix 11, Chapters 4 and 10].

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.

Note 10: The identification of the user is initiated following insertion of the card into a card reader and power-up of the card.

FIA_USB.1/Usage	**User-subject binding (usage)**
Hierarchical to:	–
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1/Usage	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/Usage	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: *none*].
FIA_USB.1.3/Usage	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *no changes permitted*].

6.1.1.5 Class FPR Privacy

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

FPT_EMS.1	**TOE emanation**
Hierarchical to:	–
Dependencies:	–
FPT_EMS.1.1	The TOE shall not emit [assignment: *information about IC power consumption and command execution time*] in excess of [assignment: *non-useful information*] enabling access to [private keys or session keys] and [assignment: *PINS (workshop card) and activity data*].

FPT_EMS.1.2	The TSF shall ensure [any users] are unable to use the following interface [smart card circuit contacts] to gain access to [private keys or session keys] and [assignment: *PINS (workshop card) and activity data*].

Note 11: FPT_EMS.1 applies to the end-usage phase of the card life cycle.

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	–
Dependencies:	–
FPT_FLS.1.1	The TSF shall preserve a secure state[2] 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)].

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.

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.

FPT_TST.1	**TSF testing**
Hierarchical to:	–
Dependencies:	–

[2] 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.

FPT_TST.1.1	The TSF shall run a suite of self tests [during initial start-up[3] 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)

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

FCS_CKM.1/G2	**Cryptographic key generation (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/G2	The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [REG_2016/799] 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 [REG_2016/799] Annex 1C, Appendix 11, Part B] that meet the following: [Reference [KiSch-RNG] predefined RNG class [selection: *PTG.3*], [REG_2016/799] Annex 1C, Appendix 11, Section 10].

Note 13: The AES algorithm as defined in [FIPS_197] with key lengths of 128, 192 and 256 bits is used. The cryptographic key derivation algorithms as defined in [BSI_TR-03111], sec. 4.3.3.2 (key derivation for AES) is used.

FCS_CKM.2/G2	**Cryptographic key distribution (generation 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

[3] During initial start-up means before other code is executed.

FCS_CKM.2.1/G2	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [secure messaging AES session key agreement as specified in [REG_2016/799] Annex 1C, Appendix 11, Part B] that meets the following [[REG_2016/799] Annex 1C, Appendix 11, Part B].

Note 14: FCS_CKM.1/G2 and FCS_CKM.2/G2 relate to session key agreement with the Vehicle Unit.

FCS_CKM.4/G2	**Cryptographic key destruction (generation 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/G2	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting cryptographic key value with random numbers*] that meets the following [• Requirements in Table A.5; • 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[4] • [assignment: *[ISO_19790]*]].

FCS_COP.1/AES	**Cryptographic operation (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 FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

[4] 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_COP.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_197], [REG_2016/799] Annex 1C, Appendix 11].

FCS_COP.1/SHA2	**Cryptographic operation (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/SHA2	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: [[FIPS_180-4], [REG_2016/799] Annex 1C, Appendix 11].

FCS_COP.1/ECC	**Cryptographic operation (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/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-repudiation of data downloaded from a Tachograph Card]

in accordance with a specified cryptographic algorithm [[REG_2016/799] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [REG_2016/799], Appendix 11, Part B] that meet the following: [[REG_2016/799] Annex 1C, Appendix 11, Part B; [FIPS_186-4]; [BSI_TR-03111], and the standardized domain parameters in the following table

Name	Size (bits)	Object identifier
NIST P-256	256	secp256r1
BrainpoolP256 r1	256	brainpoolP256r1
NIST P-384	384	secp384r1
BrainpoolP384 r1	384	brainpoolP384r1
BrainpoolP512 r1	512	brainpoolP512r1
NIST P-521	521	secp521r1

].

Note 15: The cryptographic algorithm ECDSA according [BSI_TR-03111], sec. 4.2.1 and [FIPS_186-4], sec. 6.4 and the cryptographic algorithm ECDH according [BSI_TR-03111], sec. 4.3.2 are used.

Note 16: 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 6.2 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 [CC_PP-0091].

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 6.2: Cipher suites.

FCS_RNG.1	Random number generation (Class PTG.3)
Hierarchical to:	–
Dependencies:	–
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*]. (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: *continuously*]. The online test is suitable for detecting nontolerable 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: *octets of bits*] 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[5] [assignment: *none*]. (PTG.3.8) The internal random numbers shall [selection: use PTRNG of class PTG.2 as random source for the postprocessing].

6.1.2.2 Class FIA Identification and Authentication

FIA_UAU.1/G2	Timing of authentication (generation 2)
Hierarchical to:	–
Dependencies:	FIA_UID.1 Timing of Identification

[5] See [KiSch-RNG] Section 2.4.4.

FIA_UAU.1.1/G2	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 [REG_2016/799], [REG_2021/1228] Annex 1C, Appendix 2; b) Control card, company card – export of user data without security attributes as allowed by the applicable access rules in [REG_2016/799], [REG_2021/1228] Annex 1C, Appendix 2] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/G2	The TSF shall require each user to be successfully authenticated **using the method described in [REG_2016/799] Annex 1C, Appendix 11, Chapter 10** before allowing any other TSF-mediated actions on behalf of that user.

Note 17: FIA_UAU.1.1/G2 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 [CC_PP-0091]. 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 [REG_2016/799, REG_2021/1228] Annex 1C, Appendix 2 access rules (see section 4, access rules = 'ALW').

Similarly, FIA_UAU.1.1/G2 b) allows "other devices" (without having performed any authentication) to access data from control and company cards, following [REG_2016/799, REG_2021/1228] Annex 1C, Appendix 2, Section 4 access rules.

6.1.2.3 Class FPT Protection of the TSF

FPT_TDC.1/G2	**Inter-TSF basic TSF data consistency (generation 2)**
Hierarchical to:	–
Dependencies:	–
FPT_TDC.1.1/G2	The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [REG_2016/799] Annex 1C, Appendix 11] when shared between the TSF and ~~another trusted IT product~~ **a Vehicle Unit**.
FPT_TDC.1.2/G2	The TSF shall use [the interpretation rules (communication protocols) as defined by [REG_2016/799] 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

FTP_ITC.1/G2	**Inter-TSF trusted channel (generation 2)**
Hierarchical to:	–
Dependencies:	–

FTP_ITC.1.1/G2	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/G2	The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3/G2	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].

Note 18: The requirements for establishing the trusted channel are given in [REG_2016/799] Appendix 11, Chapter 10 (for 2nd generation Vehicle Units).

6.1.3 Security Functional Requirements for External Communications (1st generation)

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

FCS_CKM.1/G1	**Cryptographic key generation (generation 1)**
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/G1	The TSF shall generate keys in accordance with a specified key generation algorithm [cryptographic key derivation algorithms specified in [REG_2016/799] 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 [REG_2016/799] Annex 1C, Appendix 11 Part A, Chapter 3].

Note 19: Two-key TDES keys as defined in [NIST_SP800-67] are used.

FCS_CKM.2/G1	**Cryptographic key distribution (generation 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/G1	The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [for triple DES session keys as specified in [REG_2016/799] Annex 1C, Appendix 11 Part A] that meets the following [[REG_2016/799] Annex 1C, Appendix 11 Part A, Chapter 3].

FCS_CKM.4/G1	**Cryptographic key destruction (generation 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/G1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting cryptographic key value with random numbers*] that meets the following [• Requirements in Tables A.1 and A.2; • 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[6] • [assignment: *[ISO_19790]*]].

FCS_COP.1/TDES	**Cryptographic operation (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/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: [[REG_2016/799] Annex 1C, Appendix 11 Part A, Chapter 3].

Note 20: Two-key TDES keys as defined in [NIST_SP800-67] (3DES) and [ISO_9797-1], algorithm 3 (Retail-MAC), are used.

[6] 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_COP.1/RSA	Cryptographic operation (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/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: [[REG_2016/799] Annex 1C, Appendix 11 Part A, Chapter 3].

Note 21: RSA keys as defined in[RFC_8017] are used.

FCS_COP.1/SHA1	Cryptographic operation (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/SHA1	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: [[FIPS_180-4]].

6.1.3.2 Class FIA Identification and Authentication

FIA_UAU.1/G1	Timing of authentication (generation 1)
Hierarchical to:	–
Dependencies:	FIA_UID.1 Timing of Identification
FIA_UAU.1.1/G1	The TSF shall allow [a) Driver card, workshop card - export of user data with security attributes (digital signature used in card data download function, see [REG_2016/799] Annex 1C, Appendix 11, Chapters 6 and 14)) and export of user data without security attributes as allowed by the applicable access rules in [REG_2016/799] Annex 1C, Appendix 2; b) Control card, company card - export of user data without security attributes as allowed by the applicable access rules in [REG_2016/799] Annex 1C, Appendix 2] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/G1	The TSF shall require each user to be successfully authenticated **using the method described in [REG_2016/799] 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

FPT_TDC.1/G1	**Inter-TSF basic TSF data consistency (generation 1)**
Hierarchical to:	–
Dependencies:	–
FPT_TDC.1.1/G1	The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [REG_2016/799] Annex 1C, Appendix 11 Chapter 5] when shared between the TSF and ~~another trusted IT product~~ **a Vehicle Unit**.
FPT_TDC.1.2/G1	The TSF shall use [the interpretation rules (communication protocols) as defined by [REG_2016/799] 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

FTP_ITC.1/G1	**Inter-TSF trusted channel (generation 1)**
Hierarchical to:	–
Dependencies:	–
FTP_ITC.1.1/G1	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/G1	The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3/G1	The TSF shall ~~initiate communication via~~ **use** the trusted channel for [data import from and export to a Vehicle Unit in accordance with [REG_2002/1360] Appendix 2].

Note 22: The requirements for establishing the trusted channel are given in [REG_2016/799] Appendix 11, Chapter 5 (for 1st generation Vehicle Units).

6.1.4 Security Functional Requirements for Personalization

The following requirements shall be met on personalization.

6.1.4.1 Class FCS Cryptographic Support

FCS_CKM.1/Perso	**Cryptographic key generation (personalization)**
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/Perso	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *AES*] and specified cryptographic key size [assignment: *256 bits*] that meet the following: [assignment: *[FIPS_197]*].

Note 23: SFR FCS_CKM.1/Perso has been added to address the session key generation to be used in personalization phase.

FCS_CKM.4/Perso	**Cryptographic key destruction (personalization)**
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/Perso	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting cryptographic key value with random numbers*] that meets the following [assignment: *[ISO_19790]*].

Note 24: SFR FCS_CKM.4/Perso has been added to address the destruction of session keys to be used in personalization phase.

FCS_COP.1/Perso	**Cryptographic operation (personalization)**
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/Perso	The TSF shall perform [assignment: *Secure Messaging – encryption/decryption/CMAC* in accordance with a specified cryptographic algorithm [assignment: *AES in CBC mode*] and cryptographic key sizes [assignment: *256 bits*] that meet the following: [assignment: *[FIPS_197], [ISO_10116]*] **and** a specified cryptographic algorithm [assignment: *CMAC-AES*] and cryptographic key sizes [assignment: *256 bits*] that meet the following: [assignment: *[FIPS_197], [NIST_SP800-38B]*].

Note 25: SFR FCS_COP.1/Perso has been added to address Secure Messaging to be used in personalization phase.

6.1.4.2 Class FDP User Data Protection

FDP_ACC.2/Perso	**Complete access control (personalization)**
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Access control functions
FDP_ACC.2.1/Perso	The TSF shall enforce the [assignment: *Personalization Access Control SFP*] on [assignment: • *Subjects:* – *Administrator (performing personalization)* – *other card interface devices* • *Objects:* – *User data* * *User Identification data* – *Security data* * *Cryptographic private keys* * *Cryptographic public keys* * *PIN (for Workshop card)* – *TOE file system* – *Card identification data*] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/Perso	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.

Note 26: SFR FDP_ACC.2/Perso has been added to address access control in personalization phase.

FDP_ACF.1/Perso	**Security attribute based access control (personalization)**
Hierarchical to:	–
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/Perso	The TSF shall enforce the [assignment: *Personalization Access Control SFP*] to objects based on the following: [assignment: • *Subjects:* – *Administrator (performing personalization)* – *other card interface devices* • *Objects:* – *User data:* * *User identification data* – *Security data:* * *Cryptographic private keys* * *Cryptographic public keys* * *PIN (for Workshop card)* – *TOE file system* – *Card identification data*].
FDP_ACF.1.2/Perso	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: • *Read access* – *All card types: user data may be read from the TOE by the Administrator* • *Write access* – *All card types: card identification data and user identification data may only be written by the Administrator* – *The administration of the files structure may only be performed after successful authentication by the Administrator*].
FDP_ACF.1.3/Perso	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *none*].
FDP_ACF.1.4/Perso	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *none*].

Note 27: SFR FDP_ACF.1/Perso has been added to address access control in personalization phase. Note that the administration of the file structure is restricted to the conversion of the card type including all access conditions associated with the specific card type.

6.1.4.3 Class FIA Identification and Authentication

FIA_AFL.1/Perso	**Authentication failure handling (personalization)**
Hierarchical to:	–
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/Perso	The TSF shall detect when [assignment: *10*] unsuccessful authentication attempts occur related to [assignment: *consecutive failed authentication attempts using the personalization key*].

FIA_AFL.1.2/Perso	When the defined number of unsuccessful authentication attempts has been [assignment: *met*], the TSF shall [assignment: *block the personalization key*].

Note 28: SFR FIA_AFL.1/Perso has been added to address the authentication failure handling in personalization phase.

FIA_ATD.1/Perso	**User attribute definition**
Hierarchical to:	–
Dependencies:	–
FIA_ATD.1.1/Perso	The TSF shall maintain the following list of security attributes belonging to individual users: [• *Administrator (performing personalization)* • *Non-administrator (other card interface devices)*]

Note 29: SFR FIA_ATD.1/Perso has been added to address the user attribute definition in personalization phase.

FIA_USB.1/Perso	**User-subject binding (personalization)**
Hierarchical to:	–
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1/Perso	The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [• *Administrator (performing personalization)* • *Non-administrator (other card interface devices)*]
FIA_USB.1.2/Perso	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: *usage of TOE's access rules mechanism*].
FIA_USB.1.3/Perso	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *no changes permitted*].

Note 30: SFR FIA_USB.1/Perso has been added to address the user-subject binding in personalization phase.

6.2 Security Assurance Requirements for the TOE

The assurance level for this Security Target is EAL4 augmented by the assurance components ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5, as defined in [CC_Part1]. These security assurance requirements are derived from [REG_2016/799] Annex 1C, Appendix 10 (SEC_006) and extended by ALC_DVS.2.

7 Rationale

7.1 Security Objectives Rationale

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.

Security objective / **Threat/assumption/OSP**	T.Identification_Data	T. Activity_Data	T.Application	T.Data_Exchange	T.Clone	A.Personalization_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.Personalization_Phase						x	
OE.Crypto_Admin	x	x		x		x	
OE.EOL			x		x		

Table 7.1: Security objectives rationale

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

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 personalization process. O.Crypto_Implement and OE.Crypto_Admin

require the implementation and management of strong cryptography to support this.

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.

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

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.

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.

A.Personalization_Phase is supported through the corresponding environment objective OE.Personalization_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.

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

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 I below*
FCO_NRO.1	FIA_UID.1	Satisfied by FIA_UID.2
FDP_ACC.2/Usage	FDP_ACF.1	Satisfied by FDP_ACF.1/Usage
FDP_ACF.1/Usage	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2/Usage, *see Note II below*
FDP_DAU.1	–	–

SFR	Dependencies	Rationale
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2/Usage
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.2/Usage
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2/Usage, *see Note II 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/G2 & FTP_ITC.1/G1 and FPT_TDC.1/G2 & FPT_TDC.1/G1
FDP_RIP.1	–	–
FDP_SDI.2	–	–
FIA_AFL.1/C	FIA_UAU.1	Satisfied by FIA_UAU.1/G2 & FIA_UAU.1/G1
FIA_AFL.1/WC	FIA_UAU.1	Satisfied by FIA_UAU.1/G2 & FIA_UAU.1/G1
FIA_ATD.1/Usage	–	–
FIA_UAU.3	–	–
FIA_UAU.4	–	–
FIA_UID.2	–	–
FIA_USB.1/Usage	FIA_ATD.1	Satisfied by FIA_ATD.1
FPR_UNO.1	–	–
FPT_EMS.1[1]	–	–
FPT_FLS.1	–	–
FPT_PHP.3	–	–
FPT_TST.1	–	–
2nd generation specific		
FCS_CKM.1/G2	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2/G2, FCS_COP.1/AES & FCS_COP.1/ECC and FCS_CKM.4/G2
FCS_CKM.2/G2	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/G2 and FCS_CKM.4/G2
FCS_CKM.4/G2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1/G2

[1] Extended component

SFR	Dependencies	Rationale
FCS_COP.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/G2 and FCS_CKM.4/G2
FCS_COP.1/SHA2	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/ECC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4/G2
FCS_RNG.1[2]	–	–
FIA_UAU.1/G2	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1/G2	–	–
FTP_ITC.1/G2	–	–
1st generation specific		
FCS_CKM.1/G1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2/G1, FCS_COP.1/TDES & FCS_COP.1/RSA and FCS_CKM.4/G1
FCS_CKM.2/G1	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/G1 FCS_CKM.4/G1
FCS_CKM.4/G1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1/G1
FCS_COP.1/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/G1 and FCS_CKM.4/G1
FCS_COP.1/RSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FDP_ITC.2 and FCS_CKM.4/G1
FCS_COP.1/SHA1	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/G1	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TDC.1/G1	–	–
FTP_ITC.1/G1	–	–

[2] Extended component

SFR	Dependencies	Rationale
Personalization specific		
FCS_CKM.1/Perso	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_COP.1/Perso and FCS_CKM.4/Perso
FCS_CKM.4/Perso	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1/Perso
FCS_COP.1/Perso	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/Perso and FCS_CKM.4/Perso
FDP_ACC.2/Perso	FDP_ACF.1	Satisfied by FDP_ACF.1/Perso
FDP_ACF.1/Perso	FDP_ACC.1, FMT_MSA.3	Partially satisfied by FDP_ACC.2/Perso, *see Note II below*
FIA_AFL.1/Perso	FIA_UAU.1	Satisfied by FIA_UAU.1/G2 & FIA_UAU.1/G1
FIA_ATD.1/Perso	–	–
FIA_USB.1/Perso	FIA_ATD.1	Satisfied by FIA_ATD.1/Perso

Table 7.2: SFRs' dependencies

Note I: 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 II: The access control TSF specified in FDP_ACF.1 uses security attributes that are defined during the personalization 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

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

SFR	Security objective	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	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		
FDP_ACC.2/Usage	Complete access control (usage)	x	x	x	x	x		x
FDP_ACF.1/Usage	Security attribute based access control (usage)	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/C	Authentication failure handling (card)				x			
FIA_AFL.1/WC	Authentication failure handling (workshop card)				x			
FIA_ATD.1/Usage	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/Usage	User-subject binding (usage)				x			
FPR_UNO.1	Unobservability			x		x		
FPT_EMS.1	TOE emanation	x	x	x	x			

SFR	Security objective	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
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/G2	Cryptographic key generation (generation 2)					x	x	
FCS_CKM.2/G2	Cryptographic key distribution (generation 2)					x	x	
FCS_CKM.4/G2	Cryptographic key destruction (generation 2)					x	x	
FCS_COP.1/AES	Cryptographic operation (AES)					x	x	
FCS_COP.1/SHA2	Cryptographic operation (SHA-2)					x	x	
FCS_COP.1/ECC	Cryptographic operation (ECC)					x	x	
FCS_RNG.1	Random number generation					x	x	
FIA_UAU.1/G2	Timing of authentication (generation 2)				x			
FPT_TDC.1/G2	Inter-TSF basic TSF data consistency (generation 2)					x		
FTP_ITC.1/G2	Inter-TSF trusted channel (generation 2)					x		
FCS_CKM.1/G1	Cryptographic key generation (generation 1)					x	x	
FCS_CKM.2/G1	Cryptographic key distribution (generation 1)					x	x	
FCS_CKM.4/G1	Cryptographic key destruction (generation 1)					x	x	
FCS_COP.1/TDES	Cryptographic operation (TDES)					x	x	
FCS_COP.1/RSA	Cryptographic operation (RSA)					x	x	
FCS_COP.1/SHA1	Cryptographic operation (SHA-1)					x	x	

SFR	Security objective	O.Card_Identification_Data	O.Card_Activity_Storage	O.Protect_Secret	O.Data_Access	O.Secure_Communications	O.Crypto_Implement	O.Software_Update
FIA_UAU.1/G1	Timing of authentication (generation 1)				x			
FPT_TDC.1/G1	Inter-TSF basic TSF data consistency (generation 1)					x		
FTP_ITC.1/G1	Inter-TSF trusted channel (generation 1)					x		
FCS_CKM.1/Perso	Cryptographic key generation (personalization)					x	x	
FCS_CKM.4/Perso	Cryptographic key destruction (personalization)					x	x	
FCS_COP.1/Perso	Cryptographic operation (personalization)					x	x	
FDP_ACC.2/Perso	Complete access control (personalization)	x	x	x	x	x		
FDP_ACF.1/Perso	Security attribute based access control (personalization)	x	x	x	x	x		
FIA_AFL.1/Perso	Authentication failure handling (personalization)				x			
FIA_ATD.1/Perso	User attribute definition (personalization)				x			
FIA_USB.1/Perso	User-subject binding (personalization)				x			

Table 7.3: Coverage of security objectives for the TOE by SFRs

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

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/Usage FDP_ACF.1/Usage FDP_ACC.2/Perso FDP_ACF.1/Perso	Access to TSF data, especially to the identification data, is regulated by the security function policy defined in the components FDP_ACC.2/Usage, FDP_ACF.1/Usage, FDP_ACC.2/Perso and FDP_ACF.1/Perso which explicitly denies write access to personalized 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/Usage FDP_ACF.1/Usage FDP_ACC.2/Perso FDP_ACF.1/Perso	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 authorized Vehicle Units or the Administrator, respectively.
	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.

Security Objective	SFR	Rationale
	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/Usage FDP_ACF.1/Usage FDP_ACC.2/Perso FDP_ACF.1/Perso	Access to user data is regulated by the security function policy defined in these components, which explicitly restricts write access of user data to authorized Vehicle Units.
	FIA_AFL.1/C FIA_AFL.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 authorized Vehicle Unit.
	FIA_AFL.1/Perso	This component requires that if authentication fails in personalization phase the TOE reacts with the blocking of the personalization key.
	FIA_ATD.1/Usage FIA_ATD.1/Perso FIA_USB.1/Usage FIA_USB.1/Perso	The definition of user security attributes supplies a distinction between Vehicle Units, Administrator and other card interface devices.
	FIA_UAU.1/G2 FIA_UAU.1/G1 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 unauthorized write access to the card.
	FPT_PHP.3	Requires the TOE to resist attempts to interfere with authentication through manipulation or physical probing.

Security Objective	SFR	Rationale
	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/Usage FDP_ACF.1/Usage FDP_ACC.2/Perso FDP_ACF.1/Perso	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/G2 FTP_ITC.1/G1	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.
	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.

Security Objective	SFR	Rationale
	FCS_CKM.1/G2 FCS_CKM.1/G1 FCS_CKM.1/Perso FCS_CKM.2/G2 FCS_CKM.2/G2 FCS_CKM.4/G2 FCS_CKM.4/G1 FCS_CKM.4/Perso 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/G2 FPT_TDC.1/G1	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/G2 FCS_CKM.1/G1 FCS_CKM.1/Perso FCS_CKM.2/G2 FCS_CKM.2/G2 FCS_CKM.4/G2 FCS_CKM.4/G1 FCS_CKM.4/Perso 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[3]	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 7.4: Suitability of the SFRs.

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

7.2.3 Security Assurance Requirements Rationale

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 [REG_2016/799] Annex 1C, Appendix 10.

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.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the TOE's development and manufacturing environment.

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

The selection of the component AVA_VAN.5 provides a higher assurance than the predefined 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 3.3: 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 [CC_PP-0091].

The set of *assurance* requirements being part of EAL4 fulfills all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance components:

- ALC_DVS.2,
- ATE_DPT.2 and
- AVA_VAN.5.

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

Component	Dependencies required by [CC_Part3]	Dependency satisfied by
ALC_DVS.2	no dependencies	–
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 7.5: SARs' dependencies (additional to EAL4 only).

7.2.4 Security Requirements – Internal Consistency

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
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, including the requirements defined for the personalization step, is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately explained. All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior of these 'shared' items. [CC_PP-0091] accurately reflects the requirements of [REG_2016/799, REG_2021/1228], Annex I C, which is assumed to be internally consistent.

b) SARs
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.

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 TOE Summary Specification (ASE_TSS.1)

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

8.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

8.1.1 TOE Security Functions from Hardware (IC) and Cryptographic Library

8.1.1.1 F.IC_CL: Security Functions of the Hardware (IC) and Cryptographic Library

This security function covers the security functions of the hardware (IC) as well as of the cryptographic library. The Security Target of the hardware [IFX_ST-SLE78-B11] defines the following security features:

SF_DPM Device phase management

SF_PS Protection against snooping

SF_PMA Protection against modification attacks

SF_PLA Protection against logical attacks

SF_CS Cryptographic support including the components

- Triple DES (only hardware-implemented Triple DES used by the TOE)
- AES (only hardware-implemented AES used by the TOE)
- RSA (encryption, decryption, signature generation and verification; asymmetric key generation; cryptographic library function used by the TOE)
- EC (signature generation and verification; asymmetric key generation; asymmetric key agreement; cryptographic library function used by the TOE)
- SHA-2 (not used by the TOE)
- PTRNG respectively TRNG (PTRNG is not used by the TOE)

8.1.2 TOE Security Functions from Embedded Software (ES) – Operating system

8.1.2.1 F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects (any file) and security attributes.
2. No access control policy allows reading of secret keys.
3. Any access not explicitly allowed is denied.

8.1.2.2 F.Identification_Authentication

This function provides identification and authentication in **operational use** phase of the user roles

- Administrator (performing initialization and personalization)
- Vehicle Unit (end-usage)

by the methods:

1. **Initialization** step (workshop, company and control cards only):
   - Symmetric authentication [FIPS_197, NIST_SP800-38B] with following properties:
     - It uses a challenge from the TOE.
     - On error (wrong challenge) the user role is not identified/authenticated.
     - After **ten** consecutive failed authentication attempts the authentication method is irreversibly blocked and the key is no longer usable (retry counter with a value of **10**). Upon a successful authentication, the retry counter is reset to ten unless the key is blocked.
     - A usage counter of 50.000 prevents the unlimited usage of the key. The counter cannot be reset. After the limit is reached, the key is irreversibly blocked.
   - Secure Messaging with following properties:
     - A static key with a usage counter of 500 used (permitting one successful reconfiguration of the card type). The counter cannot be reset. After the limit of the usage counter is reached, the key is blocked.
     - After **three** consecutive not successfully executed APDUs, the key is irreversibly blocked (retry counter with a value of **3**). Upon a successfully executed APDU the retry counter is reset to three unless the key is blocked.
     - The cryptographic method for confidentiality is AES-256/CBC provided by F.Crypto.
     - The cryptographic method for authenticity is CMAC provided by F.Crypto.
     - A chained initialization vector for AES encryption and CMAC is used.
2. **Personalization** step:
   - Symmetric authentication [FIPS_197, NIST_SP800-38B] with following properties:

  - It uses a challenge from the TOE.
  - The cryptographic method for confidentiality is AES-256/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
  - After **ten** consecutive failed authentication attempts the authentication method is irreversibly blocked and the key is no longer usable (retry counter with a value of **10**). Upon a successful authentication, the retry counter is reset to ten unless the key is blocked.
  - A usage counter of 50.000 prevents the unlimited usage of the key. The counter cannot be reset. After the limit is reached, the key is irreversibly blocked.
  - On success the session keys are created and stored for Secure Messaging.
  - Keys and data in transient memory are overwritten after usage.
- Secure Messaging with following properties:
  - The cryptographic method for confidentiality is AES-256/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - The initialization vector is an encrypted Send Sequence Counter (SSC) for encryption and MAC.
  - A session key is used.
  - Upon any command that is not protected correctly with the session keys these are overwritten according to [ISO_19790] and a new authentication is required.
  - Keys and data in transient memory are overwritten after usage.

3. **End-usage** step:

   2nd generation:
   - Certificate chain verification according to [REG_2016/799] using ECDSA from F.IC_CL.
   - VU authentication with following properties:
     - PIN verification (workshop card only); the PIN has a length of 8 bytes; it is stored on the card in a SHA-256 hash representation; the authentication method is irreversibly blocked after **five** failed authentications (retry counter of **5**). Upon a successful authentication, the retry counter is reset to five unless the PIN is blocked.
     - Verification of the signature (of a random number generated by the card) sent by the Vehicle Unit according to [BSI_TR-03111].
   - Chip Authentication according to [REG_2016/799] with following properties:
     - Key agreement using ECDH according [BSI_TR-03111] provided by F.IC_CL.
     - Session keys are created and stored for Secure Messaging.
   - Secure Messaging with following properties:
     - Session keys are used.

  - The cryptographic method for confidentiality is AES/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - The key lengths are depending on the chosen cipher suite (see Table 6.2).
  - Depending on the access conditions of the according files Secure Messaging is in authentication-only mode or in encrypt-then-authenticate mode.
  - The Secure Messaging session is limited by a Secure Messaging counter of 240 APDUs.
  - The initialization vector is an encrypted Send Sequence Counter (SSC) for AES encryption and CMAC.
  - On any command that is not protected correctly with the session keys these are overwritten according to [ISO_19790] and a new authentication is required.
  - Keys and data in transient memory are overwritten after usage.
- The authenticity of **downloaded** data files is ensured using digital signature (ECDSA according [BSI_TR-03111], for key lengths see Table 6.2; control cards only).
- The authenticity of data files **to be downloaded** is ensured using digital signature (ECDSA according [BSI_TR-03111], for key lengths see Table 6.2; driver and workshop cards only).
- The authenticity and integrity of data sent over a remote channel from a Vehicle Unit is ensured using AES according [FIPS_197] (control and workshop cards only). For workshop cards, a usage counter of 13.000 (3.250 for a specific VU) prevents the unlimited usage of the DSRC master key. The counter cannot be reset. After the limit is reached, the key is irreversibly blocked.

1st generation:

- Certificate chain verification according to [REG_2016/799] using RSA from F.IC_CL.
- Mutual authentication:
  - PIN verification (workshop card only); the PIN has a length of 8 bytes; it is stored on the card in a SHA-256 hash representation; the authentication method is ireeversibly blocked after **five** failed authentications (retry counter of **5**). Upon a successful authentication, the retry counter is reset to five unless the PIN is blocked.
  - Internal authentication according to [REG_2016/799] using RSA from F.IC_CL.
  - Verification of the signature (of a random number generated by the card) sent by the Vehicle Unit.
  - Session keys are created and stored for Secure Messaging.
- Secure Messaging with following properties:
  - Session keys are used.
  - The cryptographic method for confidentiality is 3DES/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is DES/Retail-MAC provided

by F.Crypto.
  - Depending on the access conditions of the according files Secure Messaging is in authentication-only mode or in encrypt-then-authenticate mode.
  - The Secure Messaging session is limited by a Secure Messaging counter of 240 APDUs.
  - The initialization vector is an encrypted Send Sequence Counter (SSC) for 3DES encryption and Retail-MAC.
  - On any command that is not protected correctly with the session keys these are overwritten according to [ISO_19790] and a new authentication is required.
  - Keys and data in transient memory are overwritten after usage.
- The authenticity of downloaded data files is ensured using digital signature (RSA with 1024 bit key length according to [RFC_8017]; driver and workshop cards only).

8.1.2.3 F.Management

Development phase The Manufacturer applies the operating system and application software to the chip. The application software includes the configuration and the file layout for the driver card.

Operational use phase the Administrator performs the following steps:

- Configuration of the file layout, if a workshop, control or company card is required (initialization step).
- Formatting of all data to be stored in the TOE.
- Writing of all the required data to the appropriate files.
- Changing the TOE into the end-usage mode.

8.1.2.4 F.Crypto

This function provides the implementation or, if the functionality of the cryptographic library (F.IC_CL) is used, the high level interface to

- DES
- AES
- CMAC
- 3DES/CBC
- DES/Retail MAC
- HMAC
- ECC (supplied by F.IC_CL)
- RSA (supplied by F.IC_CL)

This function implements the hash algorithms according to [FIPS_180-4]

- SHA-1

- SHA-256
- SHA-384
- SHA-512

This function implements the post-processing of the random number generator

- RNG (PTG.3, supplied by F.IC_CL)

8.1.2.5 F.Verification

TOE internal functions ensures correct operation.

8.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 are given in table 8.1.

Measure	Description
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.2	Testing: security enforcing modules
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 8.1: Assurance Measures

8.3 TOE Summary Specification Rationale

Table 8.2 shows the coverage of the SFRs by TSFs.

SFR	TSFs	Justification
FAU_ARP.1	F.Access_Control, F.Verification	The TSFs provide the means to indicate the corresponding violation, if user authentication failures (realized by F.Access_Control), self test errors and integrity errors on stored and activity data (realized by F.Verification) occur.
FAU_SAA.1	F.Access_Control, F.Verification	The TSFs provide the means to detect and monitor potential security violations, if user authentication failures (realized by F.Access_Control), self test errors and integrity errors on stored and activity data (realized by F.Verification) occur.
FCO_NRO.1	F.Identification_Authentication	The TSF provides the means to generate and verify evidence of origin for transmitted data (digital signature) and ensure the integrity of transmitted data (MAC).
FDP_ACC.2/Usage	F.Access_Control	The TSF provides the means to enforce access control policy in operational use phase.
FDP_ACF.1/Usage	F.Access_Control	The TSF provides the means to enforce access control policy on objects in operational use phase.
FDP_DAU.1	F.Crypto, F.Identification_Authentication	The TSFs provide the functionality to generate and verify evidence of origin for activity data.
FDP_ETC.1	F.Identification_Authentication	The TSF provides the means to enforce access control policy for exporting user data without security attributes.
FDP_ETC.2	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to enforce access control policy for exporting user data with security attributes.

SFR	TSFs	Justification
FDP_ITC.1	F.Identification_Authentication	The TSF provides the means to enforce access control policy for importing user data without security attributes.
FDP_ITC.2	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to enforce access control policy for importing user data with security attributes.
FDP_RIP.1	F.Identification_Authentication, F.Management	The TSFs provide the means to ensure the protection of residual information.
FDP_SDI.2	F.Management, F.Verification	The TSF provides the means to monitor the integrity of user data stored in containers and to warn the entity connected in the case of an integrity error.
FIA_AFL.1/C	F.Identification_Authentication	The TSF provides the means to detect unsuccessful authentications and warn the entity connected.
FIA_AFL.1/WC	F.Identification_Authentication	The TSF provides the means to detect unsuccessful authentications, block the PIN check procedure and indicate subsequent users the reason for the blocking.
FIA_ATD.1/Usage	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to maintain lists of security attributes belonging to user groups and user IDs in operational use phase.
FIA_UAU.3	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to prevent the use of forged or copied authentication data.
FIA_UAU.4	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to prevent the re-use of authentication data.
FIA_UID.2	F.Access_Control	The TSF provides the means to successfully identify the user before allowing any TSF-mediated action.
FIA_USB.1/Usage	F.Identification_Authentication	The TSF provides the means to associate security attributes with user groups and user IDs in operational use phase.

SFR	TSFs	Justification
FPR_UNO.1	F.IC_CL	The TSF provides the means to ensure the unobservability of authentication and cryptographic operations.
FPT_EMS.1	F.IC_CL	The TSF provides the means to ensure the limitation of emanations.
FPT_FLS.1	F.IC_CL	The TSF provides the means to preserve a secure state in the case of failures.
FPT_PHP.3	F.IC_CL	The TSF provides the means to resist physical manipulation and probing.
FPT_TST.1	F.IC_CL, F.Verification	The TSF provides the means to test for correct operation and to enable the user to verity the integrity of the TSF and TSF-data.
FCS_CKM.1/G2	F.IC_CL, F.Crypto	The TSFs provide the AES algorithm.
FCS_CKM.2/G2	F.IC_CL, F.Crypto	The TSFs provide the AES algorithm.
FCS_CKM.4/G2	F.Identification_Authentication	The TSF provides the means to destroy cryptographic keys.
FCS_COP.1/AES	F.IC_CL, F.Crypto	The TSFs provide the AES algorithm.
FCS_COP.1/SHA2	F.Crypto	The TSF provides the SHA implementation.
FCS_COP.1/ECC	F.IC_CL, F.Crypto	The TSFs provide the ECDH and ECDSA algorithms.
FCS_RNG.1	F.IC_CL, F.Crypto	The TSFs provide random numbers.
FIA_UAU.1/G2	F.Identification_Authentication	The TSF provides the means to successfully authenticate the user before allowing any TSF-mediated action.
FPT_TDC.1/G2	F.IC_CL, F.Crypto	The TSF provides the means to consistently interpret security related data shared between the TOE and the card interface device.
FTP_ITC.1/G2	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to provide and use a trusted channel.
FCS_CKM.1/G1	F.IC_CL, F.Crypto	The TSFs provide the two key TDES algorithm.

SFR	TSFs	Justification
FCS_CKM.2/G1	F.IC_CL, F.Crypto	The TSFs provide the two key TDES algorithm.
FCS_CKM.4/G1	F.Identification_Authentication	The TSF provides the means to destroy cryptographic keys.
FCS_COP.1/TDES	F.IC_CL, F.Crypto	The TSFs provide the two key TDES algorithm.
FCS_COP.1/RSA	F.IC_CL, F.Crypto	The TSFs provide the RSA algorithm.
FCS_COP.1/SHA1	F.Crypto	The TSF provides the SHA implementation.
FIA_UAU.1/G1	F.Identification_Authentication	The TSF provides the means to successfully authenticate the user before allowing any TSF-mediated action.
FPT_TDC.1/G1	F.IC_CL, F.Crypto	The TSF provides the means to consistently interpret security related data shared between the TOE and the card interface device.
FTP_ITC.1/G1	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to provide and use a trusted channel.
FCS_CKM.1/Perso	F.IC_CL, F.Crypto	The TSFs provide the AES algorithm.
FCS_CKM.4/Perso	F.Identification_Authentication	The TSF provides the means to destroy cryptographic keys.
FCS_COP.1/Perso	F.IC_CL, F.Crypto	The TSFs provide the AES algorithm.
FDP_ACC.2/Perso	F.Access_Control	The TSF provides the means to enforce access control policy in personalization phase.
FDP_ACF.1/Perso	F.Access_Control	The TSF provides the means to enforce access control policy on objects in personalization phase.
FIA_AFL.1/Perso	F.Identification_Authentication	The TSF provides the means to detect unsuccessful authentications and block the block the personalization key.
FIA_ATD.1/Perso	F.Access_Control, F.Identification_Authentication	The TSFs provide the means to maintain lists of security attributes belonging to user groups and user IDs in personalization phase.

SFR	TSFs	Justification
FIA_USB.1/Perso	F.Identification_Authentication	The TSF provides the means to associate security attributes with user groups and user IDs in personalization phase.

Table 8.2: Coverage of SFRs for the TOE by TSFs.

8.4 Statement of Compatibility

This section addresses the compatibility between this composite ST and the ST of SLE78CFX4000P (M7892) [IFX_ST-SLE78-B11]. No conflict between both Security Targets can be found.

8.4.1 Relevance of Hardware TSFs

Table 8.3 shows the relevance of the hardware security functions for the composite Security Target.

HW-TSFs	Description	Relevant	Not relevant
SF_DPM	Device phase management	x	
SF_PS	Protection against snooping	x	
SF_PMA	Protection against modification attacks	x	
SF_PLA	Protection against logical attacks	x	
SF_CS (TDES)*	Cryptographic support	x	
SF_CS (AES)*	Cryptographic support	x	
SF_CS (RSA)	Cryptographic support	x	
SF_CS (EC)	Cryptographic support	x	
SF_CS (SHA-2)	Cryptographic support		x
SF_CS (TRNG)	Cryptographic support	x	

* only the hardware-implementation is used by the TOE

Table 8.3: Relevance of hardware TSFs for composite ST

8.4.1.1 Security Objectives

Table 8.4 gives a mapping of the hardware security objectives to those of the composite ST.

HW objective	Matches TOE objective	Remarks
O.Phys-Manipulation (protection against physical manipulation)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret	
O.Phys-Probing (protection against physical probing)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret	
O.Malfunction (protection against malfunctions)	O.Card_Activity_Storage O.Protect_Secret	
O.Leak-Inherent (protection against inherent information leakage)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret	
O.Leak-Forced (protection against forced information leakage)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret	
O.Abuse-Func (protection against abuse of functionality)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret	
O.Identification (TOE identification)	O.Card_Identification_Data	
O.RND (random numbers)	O.Crypto_Implement	
O.Add-Functions (additional specific security functionality)	O.Crypto_Implement	
O.Mem-Access (area based memory access control)	–	used implicitly
OE.Plat-Appl (usage of hardware platform)	O.Protect_Secret O.Secure_Communications	
OE.Resp-Appl (treatment of user data)	O.Card_Activity_Storage O.Card_Identification_Data O.Protect_Secret O.Data_Access O.Secure_Communications	

HW objective	Matches TOE objective	Remarks
OE.Process-Sec-IC (protection during packaging, finishing and personalization)	–	protection in personalization phase is ensured by the AGD assurance class

Table 8.4: Mapping of hardware to TOE security objectives including those of the environment.

8.4.1.2 Security Requirements

Table 8.5 addresses the platform security requirements and their relevance for the TOE. Neither the SFRs that can be mapped to the platform SFRs nor those that are application specific (and thus not listed in the table) show any conflicts with the platform SFRs.

HW SFRs	Matches TOE SFr	Remarks
FAU_SAS.1 (audit storage)	–	used implicitly
FMT_LIM.1 (limited capabilities)	–	used implicitly
FMT_LIM.2 (limited availability)	–	used implicitly
FDP_ACC.1 (subset access control)	–	used implicitly
FDP_ACF.1 (security attribute based access control)	–	used implicitly
FPT_PHP.3 (resistance to physical attack)	FPT_PHP.3	
FDP_ITT.1 (basic internal transfer protection)	FPR_UNO.1 FPT_EMS.1	
FDP_SDI.1 (stored data integrity monitoring)	FDP_SDI.2	
FDP_SDI.2 (stored data integrity monitoring and action)	FDP_SDI.2	
FDP_IFC.1 (subset information flow control)	FPR_UNO.1 FPT_EMS.1	

HW SFRs	Matches TOE SFr	Remarks
FMT_MSA.1 (management of security attributes)	–	used implicitly
FMT_MSA.3 (static attribute initialization)	–	used implicitly
FMT_SMF.1 (specification of management functions)	–	used implicitly
FRU_FLT.2 (limited fault tolerance)	FPT_PHP.3	
FPT_ITT.1 (basic internal TSF data transfer protection)	FPR_UNO.1 FPT_EMS.1	
FPT_TST.2 (subset TOE testing)	FPT_TST.1	
FPT_FLS.1 (failure with preservation of secure state)	FPT_FLS.1	
FCS_RNG.1 (generation of random numbers)	FCS_RNG.1	
FCS_COP.1/TDES (cryptographic operation - TDES)	FCS_COP.1/TDES FCS_COP.1/Perso	
FCS_CKM.4/TDES (cryptographic key destruction - TDES)	FCS_CKM.4/G1	
FCS_COP.1/AES (cryptographic operation - AES)	FCS_COP.1/AES FCS_COP.1/Perso	
FCS_CKM.4/AES (cryptographic key destruction - AES)	FCS_CKM.4/G2 FCS_CKM.4/Perso	
FCS_COP.1/SHA (cryptographic operation (SHA-1, SHA-224 and SHA-256))	–	not applicable (functionality not used by the TOE)
FCS_COP.1/RSA-v1.02.013 (cryptographic operation (RSA))	–	not applicable (library not used by the TOE)
FCS_COP.1/RSA-v2.07.003 (cryptographic operation (RSA))	FCS_COP.1/RSA	
FCS_CKM.1/RSA-v2.07.003 (cryptographic key generation (RSA))	–	not applicable (function not used by the TOE)

HW SFRs	Matches TOE SFr	Remarks
FCS_COP.1/ECDSA-v1.02.013 (cryptographic operation (ECDSA))	–	not applicable (library not used by the TOE)
FCS_COP.1/ECDSA-v2.07.003 (cryptographic operation (ECDSA))	FCS_COP.1/ECC	
FCS_COP.1/ECDH-v1.02.013 (cryptographic operation (ECDH))	–	not applicable (library not used by the TOE)
FCS_COP.1/ECDH-v2.07.003 (cryptographic operation (ECDH))	FCS_COP.1/ECC	
FCS_CKM.1/EC-v1.02.013 (cryptographic key generation (EC))	–	not applicable (library not used by the TOE)
FCS_CKM.1/ECv2.07.003 (cryptographic key generation (EC))	–	not applicable (function not used by the TOE)
FCS_COP.1/TDES_SCL (cryptographic operation - TDES - SCL)	–	not applicable (functionality not used by the TOE)
FCS_CKM.4/TDES_SCL (cryptographic key destruction - TDES - SCL)	–	not applicable (functionality not used by the TOE)
FCS_COP.1/AES_SCL (cryptographic operation - AES - SCL)	–	not applicable (functionality not used by the TOE)
FCS_CKM.4/AES_SCL (cryptographic key destruction - AES - SCL)	–	not applicable (functionality not used by the TOE)

Table 8.5: Mapping of hardware to TOE SFRs.

8.4.1.3 Assurance Requirements

The level of assurance of the

- TOE is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
- Hardware is EAL6 augmented with ALC_FLR.1

This shows that the assurance requirements of the TOE is matched or exceeded by the assurance requirements of the hardware. There are no conflicts.

9 Glossary and Acronyms

9.1 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 [REG_2016/799, REG_2021/1228] Annex 1C, Appendix 2. Activity data are part of User Data.
Application note	Informative part of [CC_PP-0091] containing supporting information that is relevant or useful for the construction, evaluation or use of the TOE (relevant applications notes from the PP are adopted as consecutively numbered 'Note:' by this ST).
Attacker	A person or a process trying to undermine the security policy defined by [CC_PP-0091], 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.

Glossary Term	Definition
Card identification data	The following elements stored on the TOE, as defined in [REG_2016/799] 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.
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 organization 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.

Glossary Term	Definition
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.
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 personalization service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalizers 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 organization 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 traveled.
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.
Personalization	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 [REG_2016/799] 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 fulfills 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 [REG_2016/799] 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_Part1]). In the context of [CC_PP-0091], 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 [REG_2016/799] 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_Part1]). • 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_Part2]).
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.

9.2 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
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EGF	External GNSS Facility
ERCA	European Root Certification Authority (see Administrative Agreement 1739800-12 (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 1739800-12 (DG-TREN))
OSP	Organizational 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
TOE	Target of Evaluation
TSF	TOE Security Functionality
VRN	Vehicle Registration Number
VU	Vehicle Unit

10 Bibliography

[AGD] User Guidance – MTCOS Smart Tachograph V2 / SLE78CFX4000P, MaskTech International GmbH, Version 1.3, 2022-04-06.

[BSI_AIS31] Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, AIS 31, Version 3, 2013-05-15.

[BSI_TR-03111] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, BSI, Version 2.1, 2018-06-01.

[BSI_TR-03116-2] TR-03116-2, Technische Richtlinie – Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2 – Hoheitliche und eID-Dokumente, BSI, Stand 2022, 2021-11-30.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PP-0035] BSI-CC-PP-0035-2007, Security IC Platform Protection Profile, BSI, Version 1.0, 2007-06-15.

[CC_PP-0084] BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, EUROSMART, Version 1.0, 2014-01-13.

[CC_PP-0091] BSI-CC-PP-0091-2017, Common Criteria Protection Profile / Digital Tachograph – Tachograph Card (TC PP), European Commission Joint Research Centre, Version 1.0, 2017-05-09.

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), National Institute of Standards and Technology, 2015-08.

[FIPS_186-4] FIPS PUB 186-4, DIGITAL SIGNATURE STANDARD (DSS), National Institute of Standards and Technology, 2013-07.

[FIPS_197] FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), National Institute of Standards and Technology, 2001-11.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2021.

[IFX_ST-SLE78-B11] BSI-DSZ-CC-0782-V5-2020, Infineon Technologies AG, Security Target Lite 'M7892 B11', Version 4.1, 2020-10-21.

[ISO_10116] ISO/IEC 10116-2017, Information technology – Security techniques - Modes of operation for an n-bit block cipher, ISO/IEC, 2017-07.

[ISO_18013-3] ISO/IEC 18013-3:2017, Information technology – Personal identification – ISO-compliant driving license – Part 3: Access control, authentication and integrity validation, ISO/IEC, 2017-04.

[ISO_19790] ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules, ISO/IEC, 2012.

[ISO_7816] ISO/IEC 7816, Identification cards – Integrated circuit cards – Multipart Standard, ISO/IEC, 2008.

[ISO_9796-2] ISO/IEC 9796-2:2010, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO/IEC, 2010-12.

[ISO_9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 2011.

[KiSch-RNG] Version 2.0, A proposal for: Functionality classes for random number generators, W. Killmann and W. Schindler, 2011-09-18.

[NIST_SP800-38B] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2016-10.

[NIST_SP800-67] NIST SP 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017-11.

[NIST_SP800-90A] NIST SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, 2015-06.

[REG_2002/1360] 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, European Parliament, 2002.

[REG_2016/799] 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, European Parliament, 2016 (consolidated version of 2020-02-26).

[REG_2018/502] COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, European Parliament, 2018.

[REG_2021/1228] COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components, European Parliament, 2021.

[RFC_5480] RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, 2009.

[RFC_5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter and J. Merkle, 2010.

[RFC_5869] RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF), H. Krawczyk and P. Eronen, 2010.

[RFC_8017] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, K. Moriarty (Ed.), B. Kaliski, J. Johnson, and A. Rusch, 2016-11.

11 Revision History

Version	Date	Name	Changes
1.0	2021-11-15	Gudrun Schürer	Initial version based on v0.8 of the confidential Security Target
1.1	2022-01-17	Gudrun Schürer	Amended SFR FCS_COP.1/Perso in section 6.1.4.1, added footnote in section 1.2
1.2	2022-04-06	Gudrun Schürer	Update to Tachograph Generation 2 Version 2

12 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de

A Annex A - Key & Certificate Tables

N The information given in this section is only informative and provided for the convenience of the reader. The tables are taken from [CC_PP-0091] and describe a generic tachograph card.

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	Content
Table A.1	First-generation asymmetric keys generated, used or stored by Tachograph Cards
Table A.2	First-generation symmetric keys generated, used or stored by Tachograph Cards
Table A.3	First-generation certificates used or stored by Tachograph Cards
Table A.4	Second-generation asymmetric keys generated, used or stored by Tachograph Cards
Table A.5	Second-generation symmetric keys generated, used or stored by Tachograph Cards
Table A.6	Second-generation certificates used or stored by Tachograph Cards

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 organizational 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 6.1.3.1 (FCS_CKM.1/G1) if done by card. Otherwise, not in scope of [CC_PP-0091].	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 A.3.	RSA	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for [CC_PP-0091]	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 A.3.	RSA	Generated by VU or VU manufacturer; obtained by card in VU certificate during mutual authentication	Out of scope for [CC_PP-0091]	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 A.3.	RSA	Generated by (foreign) MSCA; obtained by card in MS certificate presented by a VU during mutual authentication	Out of scope for [CC_PP-0091]	Not applicable	Card non-volatile memory

Table A.1: 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	Session key for data protection between card and a VU during a Secure Messaging session	TDES	Agreed between card and VU during mutual authentication	See section 6.1.3.1 (FCS_CKM.1/G1)	Made unavailable when the Secure Messaging session is aborted	Not permanently 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 [REG_2016/799] Annex 1C, Appendix 11, CSM_105.	Out of scope for [CC_PP-0091]	Made unavailable when the card has reached end of life	Card non-volatile memory

Table A.2: 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 nonvolatile 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 nonvolatile 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 A.1), 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 nonvolatile 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 A.1), 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 (foreign) VU.	Card general nonvolatile 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 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 nonvolatile memory	

Table A.3: 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 (FCS_CKM.1/G2) if done by card. Otherwise, not in scope of [CC_PP-0091]	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 (FCS_CKM.1/G2) if done by card. Otherwise, not in scope of [CC_PP-0091]	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 A.6.	ECC	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for [CC_PP-0091]	Not applicable	Card non-volatile memory
EUR.PK (previous) (conditional; only present if existing at time of card issuance)	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 (previous) contents in Table A.6.	ECC	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Out of scope for [CC_PP-0091]	Not applicable	Card non-volatile memory

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
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 31: and notes for EUR.Link.C contents in Table A.6.	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 [CC_PP-0091]	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 A.6	ECC	Generated by VU or VU manufacturer; obtained by card in VU_MA certificate during mutual authentication	Out of scope for [CC_PP-0091]	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 A.6	ECC	Generated by MSCA; obtained by card in MSCA_VU-EGF certificate during mutual authentication	Out of scope for [CC_PP-0091]	Not applicable	Card non-volatile memory

Table A.4: 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-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 [REG_2016/799] Annex 1C, Appendix 11, section 12.2, a workshop card may contain up to three keys K_{M-WC} (of consecutive key generations).	Out of scope for [CC_PP-0091]	Made unavailable when the card has reached end of life	Card non-volatile memory
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 (FCS_CKM.2/G2)	Made unavailable when the Secure Messaging session is aborted[1]	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 (FCS_CKM.2/G2)	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 [CC_PP-0091]	Made unavailable when the card has reached end of life	Card non-volatile memory (control and workshop cards only)

Table A.5: Second-generation symmetric keys generated, used or stored by Tachograph Cards.

[1] See [REG_2016/799], Annex 1C, Appendix 11, Section 10.5.3 for details of secure messaging session abortion.

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 nonvolatile memory	
Card_Sign.C (driver cards and workshop cards only)	Card certificate for signing	Used by IDE to obtain and verify the Card_Sign.PK they will subsequently use to verify the signature over a data file signed 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 nonvolatile memory	
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 nonvolatile memory	
EUR.Link.C	Link certificate signed by previous EUR.SK (see 31)	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.	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Card general nonvolatile 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 A.4). 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 nonvolatile 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 A.4). The card may store the validity period and other certificate data as well.	Created and signed by ERCA; inserted in card by manufacturer at the end of the manufacturing phase	Card general nonvolatile memory	Presence in card is conditional; only if a previous ERCA root certificate existed at the moment of card manufacturing

Certificate Symbol	Description	Purpose	Source	Stored in	Note
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 nonvolatile 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 certificate for Mutual Authentication	If a card has verified a VU_MA certificate before, it may store public key (see Table A.4), 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 mutual authentication after successful verification.	Card general nonvolatile 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_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 A.4), 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 nonvolatile 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 A.6: Second-generation certificates used or stored by Tachograph Cards.

Note 31: 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.

B Overview Cryptographic Algorithms

The following cryptographic algorithms are used by the TOE to enforce its security policy:

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
1	Authenticity	RSA signature generation (RSASSA-PKCS1v1_5 using SHA-1) (generation 1)	[REG_2016/799], app. 11, sec. 6.1 [RFC_8017][1], sec. 8.2 [FIPS_180-4][2], sec. 6.1	1024	[REG_2016/799]	FCS_COP.1/RSA, FDP_DAU.1, FDP_SDI.2, FPT_TDC.1/G1, FCO_NRO.1, FIA_UAU.3
2	Authenticity	ECDSA signature generation using SHA-[256, 384, 512] (generation 2)	[REG_2016/799], app. 11, sec. 14.2 [FIPS_186-4], sec.6.4 [BSI_TR-03111][3], sec. 5.2 (signature format) [RFC_5480] (NIST curves) [RFC_5639] (Brainpool curves) [FIPS_180-4], sec. 6.2, 6.4, 6.5	acc. to used elliptic curve: brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 secp256r1 secp384r1 secp521r1	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/ECC, FDP_DAU.1, FDP_SDI.2, FPT_TDC.1/G2, FCO_NRO.1, FIA_UAU.3
3	Authenticity	RSA signature verification (RSASSA-PKCS1v1_5 using SHA-1) (generation 1, control card)	[REG_2016/799], app. 11, sec. 6.2 [RFC_8017][1], sec. 8.2 [FIPS_180-4][2], sec. 6.1	1024	[REG_2016/799]	FCS_COP.1/RSA, FDP_DAU.1, FDP_SDI.2, FPT_TDC.1/G1, FCO_NRO.1, FIA_UAU.3
4	Authenticity	ECDSA signature verification using SHA-[256, 384, 512] (generation 2, control card)	[REG_2016/799], app. 11, sec. 14.3 [FIPS_186-4], sec.6 [BSI_TR-03111][3], sec. 5.2 (signature format) [RFC_5480] (NIST curves) [RFC_5639] (Brainpool curves) [FIPS_180-4], sec. 6.2, 6.4, 6.5	acc. to used elliptic curve: brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 secp256r1 secp384r1 secp521r1	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/ECC, FDP_DAU.1, FDP_SDI.2, FPT_TDC.1/G2, FCO_NRO.1, FIA_UAU.3

[1] Compliant to the outdated PKCS #1 version 2.0 standard referenced in [REG_2016/799].
[2] Compliant to the outdated FIPS 180-1 standard referenced in [REG_2016/799].
[3] Compliant to the BSI-03111 version 2.0 standard referenced in [REG_2016/799].

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
5	Authenticated Key Agreement	Mutual Authentication VU-TC using elliptic curve and SHA-[256, 384, 512 (generation 2)	[REG_2016/799], app. 11, sec. 10 [FIPS_186-4], sec.6 [BSI_TR-03111][3], sec. 4.3.2.2 (key agreement), sec. 4.2.1 (ECDSA), sec. 5.2 (signature format) [RFC_5480] (NIST curves) [RFC_5639] (Brainpool curves) also cf. line 8	acc. to used elliptic curve: brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 secp256r1 secp384r1 secp521r1 AES: 128, 192, 256	[REG_2016/799] [REG_2021/1228]	FCS_CKM.1/G2, FCS_COP.1/ECC, FIA_AFL.1/C, FIA_AFL.1/WC, FIA_UAU.1/G2, FIA_UAU.4
6	Authenticated Key Agreement	Mutual Authentication VU-TC using RSA and SHA-1 (generation 1)	[REG_2016/799], app. 11, sec. 4 [RFC_8017][1], sec. 5.2 [ISO_9796-2][4], sec. 9 also cf. line 20	RSA: 1024 3DES: 112	[REG_2016/799]	FCS_CKM.1/G1, FCS_COP.1/RSA, FIA_AFL.1/C, FIA_AFL.1/WC, FIA_UAU.1/G1, FIA_UAU.4
7	Authenticated Key Agreement	BAC, Symmetric Authentication, based on AES in CBC mode, conforming to BAP standard (basic access protection, driving license) using SHA-256.	[FIPS_197] (AES) [ISO_10116] sec. 7 (CBC) [ISO_18013-3] Annex B [ICAO_9303] also cf. line 10	256	[ISO_18013-3] Annex B [ICAO_9303]	FCS_COP.1/Perso, FIA_AFL.1/Perso
8	Key Derivation	Cryptographic key generation (generation 2 using SHA-[256, 384, 512])	[REG_2016/799], app. 11, sec. 10.4 [BSI_TR-03111][3], sec. 4.3.3.2 [FIPS_180-4], sec. 6.2, 6.4, 6.5	128, 192, 256	[REG_2016/799] [REG_2021/1228]	FCS_CKM.1/G2, FCS_CKM.2/G2
9	Key Derivation	Cryptographic key generation (generation 1)	[REG_2016/799], app. 11, sec. 4	112	[REG_2016/799]	FCS_CKM.1/G1, FCS_CKM.2/G1
10	Key Derivation	Cryptographic key generation (personalization using SHA-256)	[FIPS_197] [ISO_18013-3] Annex B [FIPS_180-4], sec. 6.2	256	[ISO_18013-3] Annex B [ICAO_9303]	FCS_CKM.1/Perso
11	Confidentiality	AES in CBC mode for Secure Messaging and DSRC (generation 2)	[REG_2016/799], app. 11, sec. 10.5 [FIPS_197] (AES) [ISO_10116], sec. 7 (CBC)	128, 192, 256	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/AES, FCS_CKM.2/G2
12	Confidentiality	3DES in CBC mode for Secure Messaging (generation 1)	[REG_2016/799], app. 11, sec. 5 [NIST_SP800-67][5] (3DES) [ISO_10116][6] , sec. 7 (CBC)	112	[REG_2016/799]	FCS_COP.1/TDES, FCS_CKM.2/G1
13	Confidentiality	AES in CBC mode for Secure Messaging (personalization)	[FIPS_197] (AES) [ISO_10116], sec. 7 (CBC)	256	[ISO_18013-3] Annex B [ICAO_9303]	FCS_COP.1/Perso
14	Integrity	CMAC-AES for Secure Messaging and DSRC (generation 2)	[REG_2016/799], app. 11, sec. 10.5 [FIPS_197] (AES) [NIST_SP800-38B], sec. 6 (CMAC)	128, 192, 256	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/AES

[4]Compliant to the outdated ISO/IEC 9796-2 first edition standard referenced in [REG_2016/799].
[5]Compliant to the outdated FIPS 46-3 standard referenced in [REG_2016/799].
[6]Compliant to the older ANSI X9.52 standard referenced in [REG_2016/799].

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
15	Integrity	Secure Messaging 3DES/Retail-MAC (generation 1)	[REG_2016/799], app. 11, sec. 5.1 [NIST_SP800-67][5] (3DES) [ISO_9797-1][7], algorithm 3	112	[REG_2016/799]	FCS_COP.1/TDES
16	Integrity	CMAC-AES for Secure Messaging (personalization)	[FIPS_197] (AES) [NIST_SP800-38B], sec. 6 (CMAC)	256	[ISO_18013-3] Annex B [ICAO_9303]	FCS_COP.1/Perso
17	Trusted Channel	Secure Messaging in authentication-only mode or encrypt-then-authenticate mode (generation 2)	[REG_2016/799], app. 11, sec. 10.5 also cf. lines 8, 11, 14	–	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/AES, FTP_ITC.1/G2
18	Trusted Channel	Secure Messaging in authentication-only mode or encrypt-then-authenticate mode (generation 1)	[REG_2016/799], app. 11, sec. 5 also cf. lines 9, 12, 15	–	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/TDES, FTP_ITC.1/G1
19	Cryptographic Primitive	PTG.3 Random number generator (PTG.2 and cryptographic post-processing)	[BSI_AIS31] [NIST_SP800-90A] sec. 10.2, 10.3.2	–	[BSI_TR-03116-2]	FCS_RNG.1
20	Cryptographic Primitive	SHA-[1, 256 384, 512]	[REG_2016/799], app. 11, sec. 2.2.2 and sec. 8.2.3 [FIPS_180-4][8], sec. 6	–	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/SHA1, FCS_COP.1/SHA2
21	Cryptographic Primitive	HMAC using SHA-2 (generation 2, workshop and control card)	[REG_2016/799], app. 11, sec. 9.2.2.1 [RFC_5869] [FIPS_180-4], sec. 6.2, 6.4, 6.5	128, 192, 256 (keying material)	[REG_2016/799] [REG_2021/1228]	FCS_COP.1/AES

Table B.1: Overview Cryptographic Algorithms

[7] Compliant to the outdated ANSI X9.19 standard referenced in [REG_2016/799].

[8] Compliant to the outdated FIPS 180-1 standard referenced in [REG_2016/799] for generation 1.